Protokollverifikation in Temporallogik:
Fallstudie:
Alternating-Bit Protokoll

Wolfgang May

Fallstudie zur Diplomarbeit
am
Institut für Logik, Komplexität und Deduktionssysteme
Universität Karlsruhe

Zusammenfassung

Diese Fallstudie zur Diplomarbeit „Protokollverifikation in Temporallogik: Evolving Algebras und ein Tableaukalkül“ [May95] wendet das dort beschriebene Verfahren auf das Alternating-Bit-Protokoll an.

Die Beschreibung des Alternating-Bit-Protokolls als Evolving Algebra sowie die Aufteilung des Beweises in Einzelschritte basiert auf [Hu94b], wo die Korrektheit durch einen in mathematisch-argumentativem Stil geführten Beweis gezeigt wird. Auf dieser Grundlage wird die Korrektheit formal mit dem in [May95] beschriebenen Tableaukalkül nachgewiesen.

Inhaltsverzeichnis

1 Überblick

Die Zielsetzung dieser – primär als Testumgebung für den entwickelten Tableaukalkül durchgeführten – Fallstudie war folgende:

- Zeigen, daß es grundsätzlich möglich ist, mit dem angegebenen Kalkül ein – wenn auch einfaches – Protokoll aufgrund dessen Entwurfsüberlegungen zu verifizieren,
- Dabei entstehende Probleme erkennen und wenn möglich beseitigen, und die Beweisführung optimieren.

Da die Fallstudie parallel zu der theoretischen Entwicklung des Kalküls durchgeführt wurde, also gewissermaßen die Basis zu ihrer eigenen Optimierung bildete, werden auch die daraus entwickelten Optimierungen erst ab Abschnitt 17 eingesetzt. Aus diesem Grund stellt sie in vielen Punkten nicht die beste und eleganteste, aber eine mögliche Lösung dar.

In Kapitel 1 wird die Modellierung der operationalen Semantik als Evolving Algebra $\mathcal{ABP}$ basierend auf [Hu94b] beschrieben.

Kapitel 2 enthält die Axiomatisierung der gemäß [May95], Kap. 2 aus der Evolving Algebra erhaltenen Kripke-Struktur $\boldsymbol{K}^{\mathcal{ABP}}$ in CTL sowie die Formulierung der Fairnessvoraussetzungen in CTL*.

Kapitel 3 enthält als Vorbereitung zum eigentlichen Beweis einige Tableaux, die in den Induktionsbeweisen häufig benötigte elementare Beweisschritte enthalten.

Ab Kapitel 4 wird auf der Grundlage des argumentativen Beweises aus [Hu94b] der formale Korrektheitsbeweis schrittweise durchgeführt. Die Einzelschritte spiegeln die einzelnen bei der Entwicklung des Protokolls zugrundeliegenden Überlegungen wider.

Der Gesamtbeweis gliedert sich dabei in zwei Hauptteile:

Lemma 1 bis Korollar 5:
In erster Linie müssen induktiv über die Zustandsfolge prädikatenlogische Invarianten gezeigt werden. Dabei werden in jedem Beweis zwei Pfadbezeichner p, q und drei Präfixe $0, a, b$ verwendet, wobei b und a unmittelbare Nachfolgezustände beschreiben. Dieses läßt sich bei geeigneter Codierung auch prädikatenlogisch durchführen.

Ab Lemma 7:
Erst zum Nachweis von Persistenz- und Erreichbarkeitsaussagen, aus denen die nach außen sichtbare Korrektheit und Terminierung des Protokolls folgt, ist eine auf Temporallogik basierende Beweisführung notwendig. Dabei müssen zusätzlich Fairnessannahmen verarbeitet werden. Auf dieser Stufe werden in jedem Beweis viele Präfixe und viele – auch längere – Pfadabschnitte betrachtet und somit die Möglichkeiten des Kalküls erst ausgenutzt. Ab Lemma 7 werden die in [May95], Abschnitt 9 genannten Optimierungen eingesetzt.

Der Beweis lehnt sich in der Numerierung und Aussage der Lemmata an [Hu94b] an.

Abschließend werden die aus der Fallstudie gewonnenen Erkenntnisse zusammengestellt.

2 Operationale Semantik: Die Evolving Algebra $\mathcal{ABP}$

Das Kommunikationssystem, das die Umgebung des Alternating-Bit-Protokolls bildet, besteht aus den Instanzen „Sender“ und „Empfänger“ als Dienstnehmer sowie einem Medium als Dienstgeber. Entsprechend werden Sender und Empfänger durch Algorithmen beschrieben, sie besitzen eigene Datenstrukturen. Das Medium tritt nur durch sein – unkontrollierbares – Verhalten in Erscheinung.

In [Hu94b] wird vorausgesetzt daß in einem Schritt jeweils nur eine Regel angewendet werden kann („only sequential runs“). Mit dieser Vorgehensweise können – speziell auf höherer Abstraktionsebene – Spezifikationsfehler bezüglich ggs. Ausschluß nicht festgestellt werden.
Dagegen wird in [Hu94a], S. 2 und [Gu92], S. 9 angenommen, daß *alle* anwendbaren Regeln angewendet werden („all the necessary updates“). Falls sich dabei einige Regeln widersprechen, wird indeterministisch „durch einen Dämonen“ eine (maximale?) Teilmenge ausgewählt und angewendet. Damit läßt sich durch die Interpretation der Regeln als Menge Parallelität modellieren. Zur Modellierung verteilter Systeme werden in [Gu92], S. 23 entsprechend mehrere Dämonen – für jede Instanz einer – vorgesehen, die eventuell mit verschiedenen Geschwindigkeiten arbeiten. Dies ist somit die allgemeinste Annahme, die Parallelität zuläßt, aber nicht vorschreibt. Ihr folgt die Ausarbeitung des Beweises in der vorliegenden Arbeit. Sie subsumiert bezüglich Aussagen über alle Berechnungsfolgen die beiden vorgenannten Annahmen (rein sequentiell und maximal parallel).

Da eine indeterministische Anwendung der Regeln angenommen wird, mußte die Vorbedingung für *AcknowledgeMessage* gegenüber [Hu94b] verstärkt werden: *AcknowledgeMessage* ist nur möglich, wenn $\mathsf{ReceiverBit} \neq \mathsf{Bit}(\mathsf{ReceiverInMessage})$ ist. Dies entspricht der Situation, daß die ankommende Information bereits verarbeitet ist. Ohne Verstärkung der Vorbedingung führt eine alleinige Anwendung von *AcknowledgeMessage* dazu, daß eine Nachricht als empfangen bestätigt wird, ohne durch *AcceptDatum* verarbeitet worden zu sein.

Der Artikel [Hu94b] ist in sich an mehreren Stellen inkonsistent. Im Beweis von Lemma 2 wird („then rule *AcceptDatum* must also fire“) implizit angenommen, daß eine anwendbare Regel auch angewendet wird. Im Widerspruch dazu wird in den Induktionsbeweisen andererseits – ebenso implizit – angenommen, daß in jedem Schritt nur jeweils eine Regel angewendet wird. Diese Annahme führt zu Problemen im Zusammenhang mit Fairness und den Regeln *SenderLose*/*ReceiverLose*: Wenn diese jedesmal, wenn sie anwendbar sind, auch ausgeführt werden, wird jede Datenübertragung unmöglich.

In der vorliegenden Arbeit werden Einschränkungen der Nebenläufigkeit nur insofern gemacht, daß nicht zwei Regeln gleichzeitig Veränderungen an einem Datum vornehmen. Dies entspricht einem exklusiven Schreibzugriff auf die Datenstrukturen, wobei als Schreibzugriff auch das Entfernen eines Elementes gilt. Ein Schreibzugriff schließt einen Lesezugriff nicht aus. In diesem Fall erhält der Leser den ursprünglichen Wert (die Auswirkungen des Schreibzugriffs sind erst im nächsten Zustand sichtbar).

Damit entspricht diese Modellierung immer noch nicht ganz der realen Ausführung des Alternating Bit-Protokolls, bei dem Senden einer Nachricht auf das Medium und Empfangen und Entfernen der ersten Nachricht gleichzeitig möglich ist. Ebenso ist in der Realität ein Datenverlust im Medium gleichzeitig mit Senden oder Empfangen möglich.

Auf die Axiomatisierung bezogen betrifft dies genau diejenigen Regeln, die gemeinsam in einer Invarianzformel (A unless $R_1 \wedge \ldots \wedge R_n$) auftreten, d.h. verändernd auf einen Bezeichner zugreifen.

Auf höheren Abstraktionsebenen wird es solche Situationen häufig geben, so daß i.a. weitere Regeln für kombinierte Anwendung einzelner Regeln eventuell unterschiedlicher Instanzen vorzusehen sind.

[Hu94b] nimmt an, daß unendlich viele Daten übertragen werden sollen, eine Terminierung des Protokolls ist damit nicht relevant. In dieser Arbeit wird dagegen angenommen, daß nur endlich viele Daten übertragen werden sollen. Damit ergeben sich zusätzliche Aussagen über die Terminierung sowie die dann vorliegende Situation. Aus diesem Grund wurde in die Regel *ProcessAcknowledge* eine Fallunterscheidung, ob das Ende des zu übertragenden Files bereits erreicht ist, eingebaut.

2.1 Die Evolving Algebra

Datenstrukturen:

Die verwendeten Datentypen werden durch eine algebraische Spezifikation angegeben:

Bit:

$$\begin{aligned} \mathrm{O} &: \quad \to \mathit{Bit} \\ \mathrm{L} &: \quad \to \mathit{Bit} \\ \mathit{flip} &: \mathit{Bit} \to \mathit{Bit} \end{aligned}$$

$$\begin{aligned} \mathit{flip}(\mathrm{O}) &= \mathrm{L} \\ \mathit{flip}(\mathrm{L}) &= \mathrm{O} \end{aligned}$$

Data: beliebige Menge, interne Spezifikation irrelevant.

Integer:

$$\begin{aligned} 0 &: \quad \to \mathit{Integer} \\ \mathrm{s} &: \mathit{Integer} \to \mathit{Integer} \\ \mathrm{p} &: \mathit{Integer} \to \mathit{Integer} \end{aligned}$$

Message:

$$\begin{aligned} \bot &: \quad \to \mathit{Message} \\ \mathit{msg} &: \mathit{Data} \times \mathit{Bit} \to \mathit{Message} \end{aligned}$$

Queue: *Queue* $\supset$ *Message*

$$\begin{aligned} \varepsilon &: \quad \to \mathit{Queue} \\ \mathit{msg} &: \mathit{Data} \times \mathit{Bit} \to \mathit{Queue} \\ | &: \mathit{Queue} \times \mathit{Queue} \to \mathit{Queue} \end{aligned}$$

$$\begin{aligned} Q_1|Q_2|Q_3 &= (Q_1|Q_2)|Q_3 \\ Q_1|Q_2|Q_3 &= Q_1|(Q_2|Q_3) \\ Q|\varepsilon &= Q \\ \varepsilon|Q &= Q \end{aligned}$$

File: Array [*Integer*] of *Data*.

Die Konstruktoren und Modifikatoren O, L, flip, 0, s, p, $\bot$, msg, ε (alle injektiv) und | (assoziativ, nicht injektiv) werden als zustandsunabhängig interpretierte Funktionen in den zustandsunabhängig interpretierten Anteil Σ^c der Signatur Σ der Evolving Algebra $\mathcal{ABP}$ übernommen. Das Superuniversum $\mathcal{S}$ der Evolving Algebra ist

$$\mathcal{S} = \{\mathit{true}, \mathit{false}, \mathit{undef}\} \cup \mathit{Data} \cup \mathit{Bit} \cup \mathit{Integer} \cup \mathit{Message} \cup \mathit{Queue} \quad .$$

Damit werden die o.g. zustandsunabhängig interpretierten Funktionen durch die Auswertung $\mathcal{ABP} = (ABP, \mathcal{S})$ wie folgt interpretiert:

$$\begin{array}{llll}
ABP(\mathrm{O}) = \mathrm{O} & , \; ABP(\mathrm{L}) = \mathrm{L} & , \; ABP(\mathsf{flip}) = \mathit{flip} & , \\
ABP(0) = 0 & , \; ABP(s(n)) = ABP(n) + 1 & , \; ABP(p(n)) = ABP(n) - 1 & , \\
ABP(\perp) = \perp & , \; ABP(\mathsf{msg}) = \mathit{msg} & , & \\
ABP(\varepsilon) = \varepsilon & , \; ABP(|) = | & . &
\end{array}$$

Den einzelnen Datentypen werden entsprechende Universen bzw. deren charakteristische Funktionen als zustandsunabhängig interpretierte Bezeichner in die Evolving Algebra $\mathcal{ABP}$ aufgenommen:

Für alle $X \in \mathsf{Term}_\Sigma$ gilt:
$ABP(\mathsf{Bit}(X)) = \mathit{true} \;\Leftrightarrow\; ABP(X) \in \{\mathrm{O}, \mathrm{L}\}$
$ABP(\mathit{Integer}(X)) = \mathit{true} \;\Leftrightarrow\; ABP(X) \in \mathbb{N}$
$ABP(\mathsf{Message}(X)) = \mathit{true} \;\Leftrightarrow\; X = \perp$ oder
es gibt D, B mit $X = \mathsf{msg}(D, B)$ und $ABP(\mathsf{Data}(D)) = \mathit{true}$ und $ABP(\mathsf{Bit}(B)) = \mathit{true}$.
$ABP(\mathsf{Queue}(X)) = \mathit{true} \;\Leftrightarrow$
$X = \varepsilon$ oder $ABP(\mathsf{Message}(X)) = \mathit{true}$ oder
es gibt Q_1, Q_2 mit $X = Q_1|Q_2$ und $ABP(\mathsf{Queue}(Q_1)) = \mathit{true}$ und $ABP(\mathsf{Queue}(Q_2)) = \mathit{true}$.

Der Datentyp *File*: Array [*Integer*] of *Data* wird als Funktion $\mathit{Integer} \to \mathit{Data}$ dargestellt.

Die zustandsabhängig interpretierten Bezeichner der Evolving Algebra sind von folgenden Typen:

Sender:	SenderFile: *File* ,	SenderNo: *Integer* ,
	SenderBit: *Bit* ,	SenderInMsg: *Message* ,
Empfänger:	ReceiverFile: *File* ,	ReceiverNo: *Integer* ,
	ReceiverBit: *Bit* ,	ReceiverInMsg: *Message* ,
Medium:	SenderQueue: *Queue* ,	ReceiverQueue: *Queue* .

Im folgenden werden für die Bezeichner Abkürzungen verwendet.

Startzustand:

$\mathsf{SNo} = \mathsf{RNo} = 0 \quad , \quad \forall x : \mathsf{RFile}(x) = \mathit{undef} \quad ,$
$\mathsf{SIM} = \mathsf{RIM} = \perp \quad , \quad \mathsf{SQ} = \mathsf{RQ} = \varepsilon \quad , \quad \mathsf{SBit} = \mathsf{RBit} \; .$

Regeln:

Sender:

Regel: *SendCom*

$$\begin{array}{ll} \textsf{if SIM} = \bot \textsf{ and SQ} = \textsf{msg}(D,B)|Q & \\ \textsf{then} & \textsf{SIM} := \textsf{msg}(D,B) \\ & \textsf{SQ} := Q \\ \textsf{endif} & \end{array}$$

Regel: *ReTrans*

$$\begin{array}{ll} \textsf{if true} & \\ \textsf{then} & \textsf{RQ} := \textsf{RQ}|\textsf{msg}(\textsf{SFile}(\textsf{SNo}),\textsf{SBit}) \\ \textsf{endif} & \end{array}$$

Regel: *ProcAck*

$$\begin{array}{ll} \textsf{if SIM} = \textsf{msg}(D,\textsf{SBit}) \textsf{ and SFile}(s(\textsf{SNo}) \neq \bot & \\ \textsf{then} & \textsf{RQ} := \textsf{RQ}|\textsf{msg}(\textsf{SFile}(s(\textsf{SNo})),\textsf{flip}(\textsf{SBit})) \\ & \textsf{SBit} := \textsf{flip}(\textsf{SBit}) \\ & \textsf{SNo} := s(\textsf{SNo}) \\ & \textsf{ready} := \textsf{false} \\ \textsf{elsif SIM} = \textsf{msg}(D,\textsf{SBit}) \textsf{ and SFile}(s(\textsf{SNo}) = \bot & \\ \textsf{then} & \textsf{RQ} := \textsf{RQ} \\ & \textsf{SBit} := \textsf{SBit} \\ & \textsf{SNo} := \textsf{SNo} \\ & \textsf{ready} := \textsf{true} \\ \textsf{endif} & \end{array}$$

Regel: *ClMsg*

$$\begin{array}{ll} \textsf{if SIM} = \textsf{msg}(D,B) & \\ \textsf{then} & \textsf{SIM} := \bot \\ \textsf{endif} & \end{array}$$

Empfänger:

Regel: *RecCom*

$$\begin{array}{ll} \textsf{if RIM} = \bot \textsf{ and RQ} = \textsf{msg}(D,B)|Q & \\ \textsf{then} & \textsf{RIM} := \textsf{msg}(D,B) \\ & \textsf{RQ} := Q \\ \textsf{endif} & \end{array}$$

Regel: *AccDat*

$$\begin{array}{ll} \textsf{if RIM} = \textsf{msg}(D,\textsf{RBit}) & \\ \textsf{then} & \textsf{RFile}(\textsf{RNo}) := D \\ & \textsf{RNo} := s(\textsf{RNo}) \\ & \textsf{RBit} := \textsf{flip}(\textsf{RBit}) \\ \textsf{endif} & \end{array}$$

Regel: *AckMsg*

$$\begin{array}{ll} \textsf{if RIM} = \textsf{msg}(D,\textsf{flip}(\textsf{RBit})) & \\ \textsf{then} & \textsf{SQ} := \textsf{SQ}|\textsf{msg}(\lambda,\textsf{flip}(\textsf{RBit})) \\ & \textsf{RIM} := \bot \\ \textsf{endif} & \end{array}$$

Medium:

Regel: *SLose*

$$\begin{array}{ll} \textsf{if SQ} = Q_1|\textsf{msg}(D,B)|Q_2 & \\ \textsf{then} & \textsf{SQ} := Q_1|Q_2 \\ \textsf{endif} & \end{array}$$

Regel: *RLose*

$$\begin{array}{ll} \textsf{if RQ} = Q_1|\textsf{msg}(D,B)|Q_2 & \\ \textsf{then} & \textsf{RQ} := Q_1|Q_2 \\ \textsf{endif} & \end{array}$$

In einem ersten Beweisschritt wäre zu überprüfen, ob der Startzustand und die angegebenen Regeln zu den Datenstrukturspezifikationen typverträglich sind.

Die Namen der Regeln werden als zustandsabhängig interpretierte Konstanten in die Signatur der Evolving Algebra aufgenommen:

$$\mathsf{SendCom},\ \mathsf{RecCom},\ \mathsf{SLose},\ \mathsf{RLose},\ \mathsf{ReTrans},\ \mathsf{ProcAck},\ \mathsf{ClMsg},\ \mathsf{AccDat},\ \mathsf{AckMsg} \quad .$$

3 Axiomatisierung der Evolving Algebra $\mathcal{ABP}$

Damit bieten sich verschiedene Möglichkeiten, die genannten Zusammenhänge zu axiomatisieren. Im folgenden wird eine ad-hoc-Axiomatisierung angegeben, mit der der Beweis durchgeführt wird. In Abschnitt 23 wird – mit den aus der Fallstudie gewonnenen Erkenntnissen – eine bessere Axiomatisierung aufgestellt.

Existenzaxiome

EA1: $\mathsf{A}\Box\exists Q : \mathsf{SQ} = Q$
EA2: $\mathsf{A}\Box\exists Q : \mathsf{RQ} = Q$
EA3: $\mathsf{A}\Box\exists M : \mathsf{SIM} = M$
EA4: $\mathsf{A}\Box\exists M : \mathsf{RIM} = M$
$\vdots$

Gleichheitsaxiome

Gleichheitsaxiome:
E1: $\mathsf{true} \neq \mathsf{false}$
E2: $\forall M, D, Q, Q' : \varepsilon \neq Q|\mathsf{msg}(D, B)|Q'$
E3: $\forall D, B : \bot \neq \mathsf{msg}(D, B)$
E4: $\forall B : B \neq \mathsf{flip}(B)$
E5: $\forall B : B = \mathsf{flip}(\mathsf{flip}(B))$
E6: $\forall N : 0 \neq s(N)$

Datenstrukturaxiome:

F1S:	$\mathsf{SQ} = \varepsilon \lor (\exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)\vert Q \land \exists D', B', Q' : \mathsf{SQ} = Q'\vert\mathsf{msg}(D', B'))$
F1R:	$\mathsf{RQ} = \varepsilon \lor (\exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)\vert Q \land \exists D', B', Q' : \mathsf{RQ} = Q'\vert\mathsf{msg}(D', B'))$
Q1:	$\forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)\vert Q') \to Q' = \varepsilon \lor (\exists D', B', Q'' : Q' = \mathsf{msg}(D', B')\vert Q'')$
Q2:	$\forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)\vert Q') \to Q' = \varepsilon \lor (\exists D', B', Q'' : Q' = Q''\vert\mathsf{msg}(D', B'))$
Q3:	$\forall Q, Q' : (\exists D, B : Q = Q'\vert\mathsf{msg}(D, B)) \to Q' = \varepsilon \lor (\exists D', B', Q'' : Q' = Q''\vert\mathsf{msg}(D', B'))$
Q4:	$\forall Q, Q' : (\exists D, B : Q = Q'\vert\mathsf{msg}(D, B)) \to Q' = \varepsilon \lor (\exists D', B', Q'' : Q' = \mathsf{msg}(D', B')\vert Q'')$
BS:	$\forall B : \mathsf{SBit} = B \to (\mathsf{RBit} = B \lor \mathsf{RBit} = \mathsf{flip}(B))$
BR:	$\forall B : \mathsf{RBit} = B \to (\mathsf{SBit} = B \lor \mathsf{SBit} = \mathsf{flip}(B))$
oder B':	$\mathsf{RBit} = \mathsf{SBit} \lor \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})$
NZ:	$\forall N : (\mathsf{SNo} = N \lor \mathsf{RNo} = N) \to \neg(N = s(N))$
Bool:	$\mathsf{ready} = \mathsf{true} \lor \mathsf{ready} = \mathsf{false}$
F2S:	$\mathsf{SIM} = \bot \lor \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)$
F2R:	$\mathsf{RIM} = \bot \lor \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B)$
F3S:	$\forall N : \mathsf{SFile}(N) = \bot \lor \exists D : \mathsf{SFile}(N) = D$
F3R:	$\forall N : \mathsf{RFile}(N) = \bot \lor \exists D : \mathsf{RFile}(N) = D$
F4S:	$\forall N : \mathsf{SFile}(N) = \bot \to \mathsf{SFile}(s(N)) = \bot$
F5:	$\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \to D \neq \bot$

Startzustand:

$$\begin{aligned} &\mathsf{SIM} = \bot, \quad \mathsf{SQ} = \varepsilon, \quad \mathsf{SNo} = 0, \\ &\mathsf{RIM} = \bot, \quad \mathsf{RQ} = \varepsilon, \quad \mathsf{RNo} = 0, \quad \mathsf{RFile}(0) = \bot \\ &\mathsf{ready} = \mathsf{false} \quad . \end{aligned}$$

Als Kurzform dient

$$\mathrm{Start} \equiv \mathsf{SIM} = \bot \land \mathsf{RIM} = \bot \land \mathsf{SQ} = \varepsilon \land \mathsf{RQ} = \varepsilon \land \mathsf{SNo} = 0 \land \mathsf{RNo} = 0 \quad .$$

Anwendbarkeit:

SC1:	$(\mathsf{SIM} = \bot \land \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)\vert Q) \leftrightarrow \mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})$
RC1:	$(\mathsf{RIM} = \bot \land \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)\vert Q) \leftrightarrow \mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})$
SL1:	$\mathsf{SQ} \neq \varepsilon \leftrightarrow \mathsf{E}\circ(\mathsf{SLose} = \mathsf{true})$
RL1:	$\mathsf{RQ} \neq \varepsilon \leftrightarrow \mathsf{E}\circ(\mathsf{RLose} = \mathsf{true})$
RT1:	$\mathsf{E}\circ(\mathsf{ReTrans} = \mathsf{true})$
PA1:	$(\exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B) \land \mathsf{SBit} = B) \leftrightarrow \mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true})$
CM1:	$(\exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)) \leftrightarrow \mathsf{E}\circ(\mathsf{ClMsg} = \mathsf{true})$
AD1:	$(\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \land \mathsf{RBit} = B) \leftrightarrow \mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})$
bzw.	$(\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit})) \leftrightarrow \mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})$
AM1:	$(\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{flip}(\mathsf{RBit}))) \leftrightarrow \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})$

Einschränkungen der Nebenläufigkeit:

SLE: $\mathsf{SLose} = \mathsf{true} \to \neg(\mathsf{SendCom} = \mathsf{true}) \wedge \neg(\mathsf{AckMsg} = \mathsf{true})$

RLE: $\mathsf{RLose} = \mathsf{true} \to \neg(\mathsf{RecCom} = \mathsf{true}) \wedge \neg(\mathsf{ReTrans} = \mathsf{true}) \wedge \neg(\mathsf{ProcAck} = \mathsf{true})$

SQE: $\neg(\mathsf{SendCom} = \mathsf{true} \wedge \mathsf{AckMsg} = \mathsf{true})$

RQE: $\neg(\mathsf{RecCom} = \mathsf{true} \wedge (\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true}))$

Fairness:

$$\mathsf{R}((\Box\Diamond\mathsf{E}\circ\langle name\rangle) \to (\Diamond\langle name\rangle))$$

Auswirkungen der Regeln:

SC2: $\forall D, B, Q: \ \mathsf{SQ} = \mathsf{msg}(D, B)|Q \to$
$\quad \mathsf{A}\circ(\mathsf{SendCom} = \mathsf{true} \to \mathsf{SQ} = Q \wedge \mathsf{SIM} = \mathsf{msg}(D, B))$

RC2: $\forall D, B, Q: \ \mathsf{RQ} = \mathsf{msg}(D, B)|Q \to$
$\quad \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \to \mathsf{RQ} = Q \wedge \mathsf{RIM} = \mathsf{msg}(D, B))$

SL2: $\forall Q: \ \mathsf{SQ} = Q \to$
$\quad \mathsf{A}\circ(\mathsf{SLose} = \mathsf{true} \to (\exists Q^0, D, B, Q^1 : Q = Q^0|\mathsf{msg}(D, B)|Q^1 \wedge \mathsf{SQ} = Q^0|Q^1))$

RL2: $\forall Q: \ \mathsf{RQ} = Q \to$
$\quad \mathsf{A}\circ(\mathsf{RLose} = \mathsf{true} \to (\exists Q^0, D, B, Q^1 : Q = Q^0|\mathsf{msg}(D, B)|Q^1 \wedge \mathsf{RQ} = Q^0|Q^1 \ ))$

RT2: $\forall Q: \ \mathsf{RQ} = Q \to \mathsf{A}\circ(\mathsf{ReTrans} = \mathsf{true} \to \mathsf{RQ} = Q|\mathsf{msg}(\mathsf{SFile}(\mathsf{SNo}), \mathsf{SBit}))$

PA2: $\forall Q, D, B, N: \ \mathsf{SIM} = \mathsf{msg}(D, B) \wedge \mathsf{SBit} = B \wedge \mathsf{RQ} = Q \wedge \mathsf{SNo} = N \to$

$$\begin{aligned}
&\mathsf{A}\circ(\mathsf{ProcAck} = \mathsf{true} \to \\
&\quad (\mathsf{SFile}(s(N)) \neq \bot \to \ \mathsf{RQ} = Q|\mathsf{msg}(\mathsf{SFile}(s(N)), \mathsf{flip}(B)) \\
&\qquad\qquad \wedge\ \mathsf{SNo} = s(N) \wedge \mathsf{SBit} = \mathsf{flip}(B) \\
&\qquad\qquad \wedge\ \mathsf{ready} = \mathsf{false}) \\
&\quad \wedge\ (\mathsf{SFile}(s(N)) = \bot \to \ \mathsf{RQ} = Q \wedge \mathsf{SNo} = N \wedge \mathsf{SBit} = B \\
&\qquad\qquad \wedge\ \mathsf{ready} = \mathsf{true}))
\end{aligned}$$

CM2: $\mathsf{ClMsg} = \mathsf{true} \to \mathsf{SIM} = \bot$

AD2: $\forall D, B, N: \ (\mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RNo} = N \wedge \mathsf{RBit} = B \to$
$\quad \mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \to \mathsf{RFile}(N) = D \wedge \mathsf{RNo} = s(N) \wedge \mathsf{RBit} = \mathsf{flip}(B)))$

AM2: $\forall D, B, Q: \ (\mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{SQ} = Q \to$
$\quad \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \to \mathsf{SQ} = Q|\mathsf{msg}(\lambda, B) \wedge \mathsf{RIM} = \bot))$

Dabei erwiesen sich SL2 und RL2 als praktisch unbrauchbar, da sie genau diejenige Nachricht genauer beschreiben, die im Folgezustand fehlt. Um Aussagen über Nachrichten in SQ bzw. RQ im Nachfolgezustand zu machen benötigt man so immer eine Fallunterscheidung, ob diese im Anfangs- oder Endstück liegen.

Mit entsprechender Gleichheitsbehandlung kann man die folgenden Lemmata zeigen, in denen SL2 und RL2 „rückblickend“ formuliert werden:

$$\begin{array}{lll}
\mathrm{SL2}_1: & \forall D, B: & (\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge (\exists Q, Q' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|Q'))) \\
& & \to (\exists R, R' : \mathsf{SQ} = R|\mathsf{msg}(D,B)|R') \\
\mathrm{RL2}_1: & \forall D, B: & (\mathsf{E}\circ(\mathsf{RLose} = \mathsf{true} \wedge (\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q'))) \\
& & \to (\exists R, R' : \mathsf{RQ} = R|\mathsf{msg}(D,B)|R') \\
\mathrm{SL2}_2: & \forall D, D', B, B': & (\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge (\exists Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q''))) \\
& & \to (\exists R, R', R'' : \mathsf{SQ} = R|\mathsf{msg}(D,B)|R'|\mathsf{msg}(D',B')|R'') \\
\mathrm{RL2}_2: & \forall D, D', B, B': & (\mathsf{E}\circ(\mathsf{RLose} = \mathsf{true} \wedge (\exists Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q''))) \\
& & \to (\exists R, R', R'' : \mathsf{RQ} = R|\mathsf{msg}(D,B)|R'|\mathsf{msg}(D',B')|R'') \\
\mathrm{SL2}_3: & \forall D, B, Q: & (\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge \mathsf{SQ} = \mathsf{msg}(D,B)|Q)) \to \\
& & \to ((\exists Q' : \mathsf{SQ} = \mathsf{msg}(D,B)|Q') \vee (\exists D', B' : \mathsf{SQ} = \mathsf{msg}(D',B')|\mathsf{msg}(D,B)|Q)) \\
\mathrm{RL2}_3: & \forall D, B, Q: & (\mathsf{E}\circ(\mathsf{RLose} = \mathsf{true} \wedge \mathsf{RQ} = \mathsf{msg}(D,B)|Q)) \to \\
& & \to ((\exists Q' : \mathsf{RQ} = \mathsf{msg}(D,B)|Q') \vee (\exists D', B' : \mathsf{RQ} = \mathsf{msg}(D',B')|\mathsf{msg}(D,B)|Q)) \\
\mathrm{SL2}_4: & \forall D, B, Q: & (\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge \mathsf{SQ} = Q|\mathsf{msg}(D,B))) \to \\
& & \to ((\exists Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D,B)) \vee (\exists D', B' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|\mathsf{msg}(D',B'))) \\
\mathrm{RL2}_4: & \forall D, B, Q: & (\mathsf{E}\circ(\mathsf{RLose} = \mathsf{true} \wedge \mathsf{RQ} = Q|\mathsf{msg}(D,B))) \to \\
& & \to ((\exists Q' : \mathsf{RQ} = Q'|\mathsf{msg}(D,B)) \vee (\exists D', B' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|\mathsf{msg}(D',B')))
\end{array}$$

Invarianzaxiome:

$$\begin{array}{ll}
\mathrm{SIM}: & \forall M : \mathsf{SIM} = M \to \mathsf{A}(\mathsf{SIM} = M \ \mathsf{unless}^+ \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true}) \\
\mathrm{RIM}: & \forall M : \mathsf{RIM} = M \to \mathsf{A}(\mathsf{RIM} = M \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}) \\
\mathrm{SQ}: & \forall Q : \mathsf{SQ} = Q \to \mathsf{A}(\mathsf{SQ} = Q \ \mathsf{unless}^+ \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}) \\
\mathrm{RQ}: & \forall Q : \mathsf{RQ} = Q \to \mathsf{A}(\mathsf{RQ} = Q \ \mathsf{unless}^+ \ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \\
& \qquad\qquad\qquad\qquad\qquad\qquad \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}) \\
\mathrm{SBit}: & \forall B : \mathsf{SBit} = B \to \mathsf{A}(\mathsf{SBit} = B \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \\
\mathrm{RBit}: & \forall B : \mathsf{RBit} = B \to \mathsf{A}(\mathsf{RBit} = B \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \\
\mathrm{SFile}: & \forall F : \mathsf{SFile} = F \to \mathsf{A}\Box(\mathsf{SFile} = F) \\
\mathrm{RFile}: & \forall F : \mathsf{RFile} = F \to \mathsf{A}(\mathsf{RFile} = F \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \\
\mathrm{SNo}: & \forall N : \mathsf{SNo} = N \to \mathsf{A}(\mathsf{SNo} = N \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \\
\mathrm{RNo}: & \forall N : \mathsf{RNo} = N \to \mathsf{A}(\mathsf{RNo} = N \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \\
\mathrm{ready}: & \forall T : \mathsf{ready} = T \to \mathsf{A}(\mathsf{ready} = T \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true})
\end{array}$$

Diese Invarianzen lassen sich direkt aus den Regeln generieren.

Per Induktion über die Zustandsfolge lassen sich die beiden folgenden Aussagen beweisen:

$$\begin{array}{ll}
\mathrm{SData}: & \forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\Box(\mathsf{SFile}(N) = D) \\
\mathrm{RData}: & \forall D, N : \mathsf{RFile}(N) = D \to \mathsf{A}(\mathsf{RFile}(N) = D \ \mathsf{unless}^+ \ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(N)))
\end{array}$$

4 Vorbereitung des Korrektheitsbeweises

In dem gesamten Beweis wird von den in [May95], Abschnitt 9.4 genannten Optimierungen

- Einschränkung der Substitution freier Variablen auf nicht-universelle Auftreten,
- Lemmagenerierung bei Auflösung von Implikationen

Gebrauch gemacht.

Bevor mit dem eigentlichen Beweis begonnen wird, werden einige Lemma-Tableaux angegeben, die – als Schemata zu verstehen – in den folgenden Beweisen häufig verwendet werden.

Die ersten dieser Lemma-Tableaux beschreiben für jede Regel name die bei ihrer Anwendung bestehende Umgebung. In ihnen werden die jeweils unter name1 und name2 beschriebenen Axiome verwendet. Die $\boxed{\text{umrandeten}}$ Formeln sind jeweils in das umgebende Tableau zu übernehmen.

$\vdots$

$$\boxed{\begin{array}{c} p : [\ldots, \sigma, \circ, \tau, \ldots] \quad [\mathrm{P}] \\ \tau : \ \mathsf{SendCom} = \mathsf{true} \quad [\mathrm{A}] \end{array}}$$

aus SC1: $\sigma : \ \mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}) \rightarrow (\mathsf{SIM} = \bot \wedge \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \quad [*1*]$

$\sigma : \ \neg\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}) \quad [*2*]$

$\sigma : \ (\mathsf{A})\neg\circ(\mathsf{SendCom} = \mathsf{true}) \quad [*3*]$

$[*3*]$ auf p:

$\tau : \ \neg(\mathsf{SendCom} = \mathsf{true}) \quad [*4*]$

$\square \ (\mathrm{A}, *4*)$

$\sigma : \ \mathsf{SIM} = \bot \wedge \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q \quad [*5*]$

$$\boxed{\sigma : \ \mathsf{SIM} = \bot \quad [*6*]}$$

$\sigma : \ \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q \quad [*7*]$

$$\boxed{\sigma : \ \mathsf{SQ} = \mathsf{msg}(d_1, b_1)|q_1 \quad [*8*]}$$

aus SC2:

$$\sigma : \ \forall D, B, Q : \ \mathsf{SQ} = \mathsf{msg}(D, B)|Q \rightarrow \mathsf{A}\circ(\mathsf{SendCom} = \mathsf{true} \rightarrow \mathsf{SQ} = Q \wedge \mathsf{SIM} = \mathsf{msg}(D, B)) \quad [*9*]$$

$$\sigma : \ \mathsf{SQ} = \mathsf{msg}(D_2, B_2)|Q_2 \rightarrow \mathsf{A}\circ(\mathsf{SendCom} = \mathsf{true} \rightarrow \mathsf{SQ} = Q_2 \wedge \mathsf{SIM} = \mathsf{msg}(D_2, B_2)) \quad [*10*]$$

$\sigma : \ \neg\mathsf{SQ} = \mathsf{msg}(D_2, B_2)|Q_2 \quad [*11*]$

$\square \ \{D_2 \leftarrow d_1, B_2 \leftarrow b_1, Q_2 \leftarrow q_1\}(*8*, *11*)$

D_2, B_2, Q_2 einsetzen:

$$\sigma : \ \mathsf{A}\circ(\mathsf{SendCom} = \mathsf{true} \rightarrow \mathsf{SQ} = q_1 \wedge \mathsf{SIM} = \mathsf{msg}(d_1, b_1)) \quad [*12*]$$

$\sigma : \ (\mathsf{A})\circ(\mathsf{SendCom} = \mathsf{true} \rightarrow \mathsf{SQ} = q_1 \wedge \mathsf{SIM} = \mathsf{msg}(d_1, b_1)) \quad [*13*]$

$[*13*]$ auf p:

$\tau : \ \mathsf{SendCom} = \mathsf{true} \rightarrow \mathsf{SQ} = q_1 \wedge \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [*14*]$

$\tau : \ \neg\mathsf{SendCom} = \mathsf{true} \quad [*15*]$

$\square \ (\mathrm{A}, *15*)$

$\tau : \ \mathsf{SQ} = q_1 \wedge \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [*16*]$

$$\boxed{\begin{array}{c} \tau : \ \mathsf{SQ} = q_1 \quad [*17*] \\ \tau : \ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [*18*] \end{array}}$$

$\vdots$

Tab. 0.1: Umgebung einer Anwendung von SendCom.

$$\vdots$$

$$\boxed{\begin{array}{l} p : [\ldots, \sigma, \circ, \tau, \ldots] \quad [\mathrm{P}] \\ \tau : \ \mathsf{RecCom} = \mathsf{true} \quad [\mathrm{A}] \end{array}}$$

aus RC1: $\sigma : \ \mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}) \rightarrow (\mathsf{RIM} = \perp \wedge \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q) \quad [*1*]$

$$\sigma : \ \neg\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}) \quad [*2*]$$

$$\sigma : \ (\mathsf{A})\neg\circ(\mathsf{RecCom} = \mathsf{true}) \quad [*3*]$$

$[*3*]$ auf p:

$$\tau : \ \neg(\mathsf{RecCom} = \mathsf{true}) \quad [*4*]$$

$$\Box \ (\mathrm{A}, *4*)$$

$$\sigma : \ \mathsf{RIM} = \perp \wedge \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q \quad [*5*]$$

$$\boxed{\sigma : \ \mathsf{RIM} = \perp \quad [*6*]}$$

$$\sigma : \ \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q \quad [*7*]$$

$$\boxed{\sigma : \ \mathsf{RQ} = \mathsf{msg}(d_1, b_1)|q_1 \quad [*8*]}$$

aus RC2:

$$\begin{array}{ll} \sigma : \ \forall D, B, Q : \ \mathsf{RQ} = \mathsf{msg}(D, B)|Q \rightarrow & [*9*] \\ \qquad \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = Q \wedge \mathsf{RIM} = \mathsf{msg}(D, B)) & \end{array}$$

$$\begin{array}{ll} \sigma : \ \mathsf{RQ} = \mathsf{msg}(D_2, B_2)|Q_2 \rightarrow & [*10*] \\ \qquad \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = Q_2 \wedge \mathsf{RIM} = \mathsf{msg}(D_2, B_2)) & \end{array}$$

$$\sigma : \ \neg\mathsf{RQ} = \mathsf{msg}(D_2, B_2)|Q_2 \quad [*11*]$$

$$\Box \ \{D_2 \leftarrow d_1, B_2 \leftarrow b_1, Q_2 \leftarrow q_1\}(*8*, *11*)$$

D_2, B_2, Q_2 einsetzen:

$$\begin{array}{ll} \sigma : \ \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow & [*12*] \\ \qquad \mathsf{RQ} = q_1 \wedge \mathsf{RIM} = \mathsf{msg}(d_1, b_1)) & \end{array}$$

$$\sigma : \ (\mathsf{A})\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = q_1 \wedge \mathsf{RIM} = \mathsf{msg}(d_1, b_1)) \quad [*13*]$$

$[*13*]$ auf p:

$$\tau : \ \mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = q_1 \wedge \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [*14*]$$

$$\tau : \ \neg\mathsf{RecCom} = \mathsf{true} \quad [*15*]$$

$$\Box \ (\mathrm{A}, *15*)$$

$$\tau : \ \mathsf{RQ} = q_1 \wedge \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [*16*]$$

$$\boxed{\begin{array}{l} \tau : \ \mathsf{RQ} = q_1 \quad [*17*] \\ \tau : \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [*18*] \end{array}}$$

$$\vdots$$

Tab. 0.2: Umgebung einer Anwendung von RecCom.

$$\vdots$$

$$\boxed{\begin{array}{c} p : [\ldots, \sigma, \circ, \tau, \ldots] \quad [\mathrm{P}] \\ \tau :\ \mathsf{SLose} = \mathsf{true} \quad [\mathrm{A}] \end{array}}$$

aus SL1: $\sigma :\ \mathsf{E}\circ(\mathsf{SLose} = \mathsf{true}) \rightarrow \mathsf{SQ} \neq \varepsilon \quad [*1*]$

$\sigma :\ \neg\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true}) \quad [*2*]$

$\sigma :\ (\mathsf{A})\neg\circ(\mathsf{SLose} = \mathsf{true}) \quad [*3*]$

$[*3*]$ auf p:

$\tau :\ \neg(\mathsf{SLose} = \mathsf{true}) \quad [*4*]$

$\Box\ (\mathrm{A}, *4*)$

$\boxed{\sigma :\ \mathsf{SQ} \neq \varepsilon \quad [*5*]}$

$\vdots$

Für SLose gibt es – wie auf Seite 8 beschrieben – mehrere Möglichkeiten, die Auswirkungen zu formulieren:

$$\vdots$$

von $[*5*]$:

aus SL2:

$$\sigma :\ \forall Q : \mathsf{SQ} = Q \rightarrow (\mathsf{A}\circ(\mathsf{SLose} = \mathsf{true} \rightarrow (\exists Q^0, D, B, Q^1 : Q = Q^0|\mathsf{msg}(D,B)|Q^1 \wedge \mathsf{SQ} = Q^0|Q^1))) \quad [*6*]$$

$$\sigma :\ \mathsf{SQ} = Q_2 \rightarrow (\mathsf{A}\circ(\mathsf{SLose} = \mathsf{true} \rightarrow (\exists Q^0, D, B, Q^1 : Q_2 = Q^0|\mathsf{msg}(D,B)|Q^1 \wedge \mathsf{SQ} = Q^0|Q^1))) \quad [*7*]$$

$\sigma :\ \neg\mathsf{SQ} = Q_2 \quad [*8*]$

aus EA:

$\sigma :\ \exists Q : \mathsf{SQ} = Q \quad [*11*]$

$\sigma :\ \mathsf{SQ} = q_3 \quad [*12*]$

$\Box\ \{Q_2 \leftarrow q_3\}(*8*, *12*)$

Q_2 einsetzen:

$\boxed{\mathrm{LG} :\ \sigma :\ \mathsf{SQ} = q_3 \quad [*9*]}$

$$\sigma :\ \mathsf{A}\circ(\mathsf{SLose} = \mathsf{true} \rightarrow (\exists Q^0, D, B, Q^1 : q_3 = Q^0|\mathsf{msg}(D,B)|Q^1 \wedge \mathsf{SQ} = Q^0|Q^1)) \quad [*10*]$$

$$\sigma :\ (\mathsf{A})\circ(\mathsf{SLose} = \mathsf{true} \rightarrow (\exists Q^0, D, B, Q^1 : q_3 = Q^0|\mathsf{msg}(D,B)|Q^1 \wedge \mathsf{SQ} = Q^0|Q^1)) \quad [*13*]$$

$[*13*]$ auf p:

$$\tau :\ \exists Q^0, D, B, Q^1 : q_3 = Q^0|\mathsf{msg}(D,B)|Q^1 \wedge \mathsf{SQ} = Q^0|Q^1 \quad [*14*]$$

$$\boxed{\tau :\ q_3 = q_2^0|\mathsf{msg}(d_2, b_2)|q_2^1 \wedge \mathsf{SQ} = q_2^0|q_2^1 \quad [*15*]}$$

$$\vdots$$

$$\vdots$$

von [∗5∗]:

aus SL2':

$$\sigma: \ \forall D, D', B, B': \ \ (\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge (\exists Q, Q', Q'': \mathsf{SQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q''))) \quad [*16*]$$
$$\rightarrow (\exists R, R', R'': \mathsf{SQ} = R|\mathsf{msg}(D,B)|R'|\mathsf{msg}(D',B')|R''))$$

$$\sigma: \ (\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge (\exists Q, Q', Q'': \mathsf{SQ} = Q|\mathsf{msg}(D_4,B_4)|Q'|\mathsf{msg}(D'_4,B'_4)|Q''))) \quad [*17*]$$
$$\rightarrow (\exists R, R', R'': \mathsf{SQ} = R|\mathsf{msg}(D_4,B_4)|R'|\mathsf{msg}(D'_4,B'_4)|R'')$$

$$\sigma: \ \exists R, R', R'': \mathsf{SQ} = R|\mathsf{msg}(D_4,B_4)|R'|\mathsf{msg}(D'_4,B'_4)|R'' \quad [*19*]$$
$$\boxed{\sigma: \ \mathsf{SQ} = r_4|\mathsf{msg}(D_4,B_4)|r'_4|\mathsf{msg}(D'_4,B'_4)|r''_4 \quad [*25*]}$$
$$\vdots$$

$$\sigma: \ \neg(\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge (\exists Q, Q', Q'': \mathsf{SQ} = Q|\mathsf{msg}(D_4,B_4)|Q'|\mathsf{msg}(D'_4,B'_4)|Q''))) \quad [*18*]$$
$$\sigma: \ (\mathsf{A})\circ(\neg(\mathsf{SLose} = \mathsf{true} \wedge (\exists Q, Q', Q'': \mathsf{SQ} = Q|\mathsf{msg}(D_4,B_4)|Q'|\mathsf{msg}(D'_4,B'_4)|Q''))) \quad [*20*]$$

[∗20∗] auf p:

$$\tau: \ \neg(\mathsf{SLose} = \mathsf{true} \wedge (\exists Q, Q', Q'': \mathsf{SQ} = Q|\mathsf{msg}(D_4,B_4)|Q'|\mathsf{msg}(D'_4,B'_4)|Q'')) \quad [*21*]$$

$$\tau: \ \neg(\mathsf{SLose} = \mathsf{true}) \quad [*22*]$$
$$\Box \ (\mathrm{A}, *22*)$$

$$\tau: \ \neg(\exists Q, Q', Q'': \mathsf{SQ} = Q|\mathsf{msg}(D_4,B_4)|Q'|\mathsf{msg}(D'_4,B'_4)|Q'') \quad [*23*]$$
$$\boxed{\tau: \ \neg(\mathsf{SQ} = Q_4|\mathsf{msg}(D_4,B_4)|Q'_4|\mathsf{msg}(D'_4,B'_4)|Q''_4) \quad [*24*]}$$
$$\vdots$$

Analog für nur eine Nachricht:

$$\vdots$$

von [∗5∗]:

$$\boxed{\tau: \ \neg(\mathsf{SQ} = Q_4|\mathsf{msg}(D_4,B_4)|Q'_4)} \qquad \boxed{\sigma: \ \mathsf{SQ} = r_4|\mathsf{msg}(D_4,B_4)|r'_4}$$
$$\vdots \qquad\qquad \vdots$$

Andere Möglichkeit, bei [∗5∗] weiterzumachen:

$$\vdots$$

von [∗5∗]:

aus SL2”:

$$\sigma: \ \forall D,B,Q: \ (\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge \mathsf{SQ} = \mathsf{msg}(D,B)|Q)) \rightarrow \qquad [*26*]$$
$$((\exists Q' : \mathsf{SQ} = \mathsf{msg}(D,B)|Q') \vee (\exists D',B' : \mathsf{SQ} = \mathsf{msg}(D',B')|\mathsf{msg}(D,B)|Q))$$

$$\sigma: \ (\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge \mathsf{SQ} = \mathsf{msg}(D_5,B_5)|Q_5)) \rightarrow \qquad [*27*]$$
$$((\exists Q' : \mathsf{SQ} = \mathsf{msg}(D_5,B_5)|Q') \vee (\exists D',B' : \mathsf{SQ} = \mathsf{msg}(D',B')|\mathsf{msg}(D_5,B_5)|Q_5))$$

$$\sigma: \ \neg(\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge \mathsf{SQ} = \mathsf{msg}(D_5,B_5)|Q_5)) \quad [*28*]$$
$$\sigma: \ (\mathsf{A})\circ(\neg(\mathsf{SLose} = \mathsf{true} \wedge \mathsf{SQ} = \mathsf{msg}(D_5,B_5)|Q_5)) \quad [*30*]$$

[∗30∗] auf p:

$$\tau: \ \neg(\mathsf{SLose} = \mathsf{true} \wedge \mathsf{SQ} = \mathsf{msg}(D_5,B_5)|Q_5) \quad [*31*]$$

$$\tau: \ \neg(\mathsf{SLose} = \mathsf{true}) \quad [*32*]$$
$$\Box \ (\mathrm{A}, *32*)$$

$$\boxed{\tau: \ \neg(\mathsf{SQ} = \mathsf{msg}(D_5,B_5)|Q_5) \quad [*33*]}$$
$$\vdots$$

$$\sigma: \ \exists Q' : \mathsf{SQ} = \mathsf{msg}(D_5,B_5)|Q') \vee (\exists D',B' : \mathsf{SQ} = \mathsf{msg}(D',B')|\mathsf{msg}(D_5,B_5)|Q_5) \quad [*29*]$$
$$\sigma: \ (\exists Q' : \mathsf{SQ} = \mathsf{msg}(D_5,B_5)|Q') \vee (\exists D',B' : \mathsf{SQ} = \mathsf{msg}(D',B')|\mathsf{msg}(D_5,B_5)|Q) \quad [*34*]$$

$$\sigma: \ \exists Q' : \mathsf{SQ} = \mathsf{msg}(D_5,B_5)|Q' \quad [*35*]$$
$$\boxed{\sigma: \ \mathsf{SQ} = \mathsf{msg}(D_5,B_5)|q'_5 \quad [*37*]}$$
$$\vdots$$

$$\sigma: \ \exists D',B' : \mathsf{SQ} = \mathsf{msg}(D,B)|\mathsf{msg}(D_5,B_5)|Q_5 \quad [*36*]$$
$$\boxed{\sigma: \ \mathsf{SQ} = \mathsf{msg}(d'_5,b'_5)|\mathsf{msg}(D_5,B_5)|Q_5 \quad [*38*]}$$
$$\vdots$$

Eine analoge Umgebung für die letzte Nachricht erhält man aus SL2”’:

$$\sigma: \ \forall D,B,Q: \ (\mathsf{E}\circ(\mathsf{SLose} = \mathsf{true} \wedge \mathsf{SQ} = Q|\mathsf{msg}(D,B))) \rightarrow$$
$$\rightarrow ((\exists Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D,B)) \vee (\exists D',B' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|\mathsf{msg}(D',B')))$$

$$\boxed{\tau: \ \neg(\mathsf{SQ} = Q_6|\mathsf{msg}(D_6,B_6))} \qquad \boxed{\sigma: \ \mathsf{SQ} = q'_6|\mathsf{msg}(D_6,B_6)} \qquad \boxed{\sigma: \ \mathsf{SQ} = Q_6|\mathsf{msg}(D_6,B_6)|\mathsf{msg}(d'_6,b'_6)}$$
$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

Tab. 0.3: Umgebungen einer Anwendung von SLose.

Tab. 0.4: Die entsprechenden Umgebungen für RLose lauten analog.

$\vdots$

$\boxed{\begin{array}{l} p : [\ldots, \sigma, \circ, \tau, \ldots] \quad [\mathrm{P}] \\ \tau :\ \mathsf{ReTrans} = \mathsf{true} \quad [\mathrm{A}] \end{array}}$

aus RT2:

$\sigma :\ \forall Q, N, B :\ \mathsf{RQ} = Q \wedge \mathsf{SNo} = N \wedge \mathsf{SFile}(\mathsf{SNo}) \neq \lambda \wedge \mathsf{SBit} = B \rightarrow \quad [*1*]$

$\mathsf{A}\circ(\mathsf{ReTrans} = \mathsf{true} \rightarrow \mathsf{RQ} = Q|\mathsf{msg}(\mathsf{SFile}(N), B))$

$\sigma :\ \mathsf{RQ} = Q_1 \wedge \mathsf{SNo} = N_1 \wedge \mathsf{SFile}(\mathsf{SNo}) \neq \lambda \wedge \mathsf{SBit} = B_1 \rightarrow \quad [*2*]$

$\mathsf{A}\circ(\mathsf{ReTrans} = \mathsf{true} \rightarrow \mathsf{RQ} = Q_1|\mathsf{msg}(\mathsf{SFile}(N_1), B_1))$

$\sigma :\ \neg(\mathsf{RQ} = Q_1 \wedge \mathsf{SNo} = N_1 \wedge \mathsf{SFile}(\mathsf{SNo}) \neq \lambda \wedge \mathsf{SBit} = B_1) \quad [*3*]$

$\Box\ \{\mathrm{EA}\text{: } Q_1 \leftarrow q_1, N_1 \leftarrow n_1, B_1 \leftarrow b_1\}$

Q_1, N_1, B_1 einsetzen:

$\boxed{\mathrm{LG} :\ \sigma :\ \mathsf{RQ} = q_1 \wedge \mathsf{SNo} = n_1 \wedge \mathsf{SFile}(\mathsf{SNo}) \neq \lambda \wedge \mathsf{SBit} = b_1 \quad [*4*]}$

$\sigma :\ \mathsf{A}\circ(\mathsf{ReTrans} = \mathsf{true} \rightarrow \mathsf{RQ} = q_1|\mathsf{msg}(\mathsf{SFile}(n_1), b_1)) \quad [*5*]$

[*5*] auf p:

$\tau :\ \mathsf{ReTrans} = \mathsf{true} \rightarrow \mathsf{RQ} = q_1|\mathsf{msg}(\mathsf{SFile}(n_1), b_1) \quad [*6*]$

$\tau :\ \neg\mathsf{ReTrans} = \mathsf{true} \quad [*7*]$

$\Box\ (\mathrm{A}, *7*)$

$\boxed{\tau :\ \mathsf{RQ} = q_1|\mathsf{msg}(\mathsf{SFile}(n_1), b_1) \quad [*8*]}$

$\vdots$

Tab. 0.6: Umgebung einer Anwendung von $\mathsf{ReTrans}$.

$$\vdots$$

$$\boxed{\begin{array}{l} p : [\ldots, \sigma, \circ, \tau, \ldots] \quad [\mathrm{P}] \\ \tau : \ \mathsf{ProcAck} = \mathsf{true} \quad [\mathrm{A}] \end{array}}$$

$$\text{aus PA1:} \quad \sigma : \ \mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}) \rightarrow (\exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B) \wedge \mathsf{SBit} = B) \quad [*1*]$$

$$\sigma : \ \neg\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}) \quad [*2*]$$
$$\sigma : \ (\mathsf{A})\neg\circ(\mathsf{ProcAck} = \mathsf{true}) \quad [*3*]$$
$$[*3*] \text{ auf } p\text{:}$$
$$\tau : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [*4*]$$
$$\Box \ (\mathrm{A}, *4*)$$

$$\sigma : \ \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B) \wedge \mathsf{SBit} = B \quad [*5*]$$
$$\sigma : \ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \wedge \mathsf{SBit} = b_1 \quad [*6*]$$
$$\boxed{\begin{array}{c} \sigma : \ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [*7*] \\ \sigma : \ \mathsf{SBit} = b_1 \quad [*8*] \end{array}}$$
$$\text{aus PA2:}$$

$$\begin{array}{lll} \sigma : \ \forall Q, D, B, N : \mathsf{SIM} = \mathsf{msg}(D, B) \wedge \mathsf{SBit} = B \wedge \mathsf{RQ} = Q \wedge \mathsf{SNo} = N \rightarrow & & [*9*] \\ \quad \mathsf{A}\circ(\mathsf{ProcAck} = \mathsf{true} \rightarrow (\mathsf{SFile}(s(N)) \neq \bot \rightarrow & \mathsf{RQ} = Q|\mathsf{msg}(\mathsf{SFile}(s(N)), \mathsf{flip}(B)) & \\ & \wedge\ \mathsf{SNo} = s(N) \wedge \mathsf{SBit} = \mathsf{flip}(B) & \\ & \wedge\ \mathsf{ready} = \mathsf{false}) & \\ \qquad \wedge\ (\mathsf{SFile}(s(N)) = \bot \rightarrow & \mathsf{RQ} = Q \wedge \mathsf{SNo} = N \wedge \mathsf{SBit} = B & \\ & \wedge\ \mathsf{ready} = \mathsf{true})) & \end{array}$$

$$\begin{array}{lll} \sigma : \ \mathsf{SIM} = \mathsf{msg}(D_2, B_2) \wedge \mathsf{SBit} = B_2 \wedge \mathsf{RQ} = Q_2 \wedge \mathsf{SNo} = N_2 \rightarrow & & [*10*] \\ \quad \mathsf{A}\circ(\mathsf{ProcAck} = \mathsf{true} \rightarrow \quad (\mathsf{SFile}(s(N_2)) \neq \bot \rightarrow & \mathsf{RQ} = Q_2|\mathsf{msg}(\mathsf{SFile}(s(N_2)), \mathsf{flip}(B_2)) & \\ & \wedge\ \mathsf{SNo} = s(N_2) \wedge \mathsf{SBit} = \mathsf{flip}(B_2) & \\ & \wedge\ \mathsf{ready} = \mathsf{false}) & \\ \qquad \wedge\ (\mathsf{SFile}(s(N_2)) = \bot \rightarrow & \mathsf{RQ} = Q_2 \wedge \mathsf{SNo} = N_2 \wedge \mathsf{SBit} = B_2 & \\ & \wedge\ \mathsf{ready} = \mathsf{true})) & \end{array}$$

$$\sigma : \ \neg(\mathsf{SIM} = \mathsf{msg}(D_2, B_2) \wedge \mathsf{SBit} = B_2 \wedge \mathsf{RQ} = Q_2 \wedge \mathsf{SNo} = N_2) \quad [*11*]$$

$$\sigma : \ \neg(\mathsf{SIM} = \mathsf{msg}(D_2, B_2) \wedge \mathsf{SBit} = B_2) \quad [*14*]$$
$$\Box^* \ \{D_2 \leftarrow d_1, B_2 \leftarrow b_1\}(7, 8, 14)$$

$$\sigma : \ \neg(\mathsf{RQ} = Q_2 \wedge \mathsf{SNo} = N_2) \quad [*15*]$$
$$\Box \ (\text{aus EA:}) \ \{Q_2 \leftarrow q_2, N_2 \leftarrow n_2\}$$

$$D_2,\ B_2,\ Q_2,\ N_2 \text{ einsetzen:}$$

$$\boxed{\text{LG} : \ \sigma : \ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \wedge \mathsf{SBit} = b_1 \wedge \mathsf{RQ} = q_2 \wedge \mathsf{SNo} = n_2 \quad [*12*]}$$

$$\begin{array}{lll} \sigma : \ \mathsf{A}\circ(\mathsf{ProcAck} = \mathsf{true} \rightarrow (\mathsf{SFile}(s(n_2)) \neq \bot \rightarrow & \mathsf{RQ} = q_2|\mathsf{msg}(\mathsf{SFile}(s(n_2)), \mathsf{flip}(b_1)) & [*13*] \\ & \wedge\ \mathsf{SNo} = s(n_2) \wedge \mathsf{SBit} = \mathsf{flip}(b_1) \wedge \mathsf{ready} = \mathsf{false}) & \\ \qquad \wedge\ (\mathsf{SFile}(s(n_2)) = \bot \rightarrow & \mathsf{RQ} = q_2 \wedge \mathsf{SNo} = n_2 \wedge \mathsf{SBit} = b_1 \wedge \mathsf{ready} = \mathsf{true})) & \end{array}$$

$$\hookrightarrow$$

$$\vdots$$

von [∗13∗]:

$$\sigma: \ \mathsf{A}\circ(\mathsf{ProcAck} = \mathsf{true} \rightarrow (\mathsf{SFile}(s(n_2)) \neq \bot \rightarrow \ \mathsf{RQ} = q_2|\mathsf{msg}(\mathsf{SFile}(s(n_2)), \mathsf{flip}(b_1)) \qquad [*13*]$$
$$\wedge\ \mathsf{SNo} = s(n_2) \wedge \mathsf{SBit} = \mathsf{flip}(b_1) \wedge \mathsf{ready} = \mathsf{false})$$
$$\wedge\ (\mathsf{SFile}(s(n_2)) = \bot \rightarrow \ \mathsf{RQ} = q_2 \wedge \mathsf{SNo} = n_2 \wedge \mathsf{SBit} = b_1 \wedge \mathsf{ready} = \mathsf{true}))$$

$$|$$

$$\sigma: \ (\mathsf{A})\circ(\mathsf{ProcAck} = \mathsf{true} \rightarrow \quad (\mathsf{SFile}(s(n_2)) \neq \bot \rightarrow \ \mathsf{RQ} = q_2|\mathsf{msg}(\mathsf{SFile}(s(n_2)), \mathsf{flip}(b_1)) \qquad [*16*]$$
$$\wedge\ \mathsf{SNo} = s(n_2) \wedge \mathsf{SBit} = \mathsf{flip}(b_1)$$
$$\wedge\ \mathsf{ready} = \mathsf{false})$$
$$\wedge\ (\mathsf{SFile}(s(n_2)) = \bot \rightarrow \ \mathsf{RQ} = q_2 \wedge \mathsf{SNo} = n_2 \wedge \mathsf{SBit} = b_1$$
$$\wedge\ \mathsf{ready} = \mathsf{true}))$$

$$|$$

[16] auf p:

$$\tau: \ \mathsf{ProcAck} = \mathsf{true} \rightarrow \quad (\mathsf{SFile}(s(n_2)) \neq \bot \rightarrow \ \mathsf{RQ} = q_2|\mathsf{msg}(\mathsf{SFile}(s(n_2)), \mathsf{flip}(b_1)) \qquad [*17*]$$
$$\wedge\ \mathsf{SNo} = s(n_2) \wedge \mathsf{SBit} = \mathsf{flip}(b_1)$$
$$\wedge\ \mathsf{ready} = \mathsf{false})$$
$$\wedge\ (\mathsf{SFile}(s(n_2)) = \bot \rightarrow \ \mathsf{RQ} = q_2 \wedge \mathsf{SNo} = n_2 \wedge \mathsf{SBit} = b_1$$
$$\wedge\ \mathsf{ready} = \mathsf{true})$$

$$\tau: \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [*18*]$$
$$\square\ (\mathrm{A}, *18*)$$

$$\tau: \ (\mathsf{SFile}(s(n_2)) \neq \bot \rightarrow \ \mathsf{RQ} = q_2|\mathsf{msg}(\mathsf{SFile}(s(n_2)), \mathsf{flip}(b_1)) \qquad [*19*]$$
$$\wedge\ \mathsf{SNo} = s(n_2) \wedge \mathsf{SBit} = \mathsf{flip}(b_1) \wedge \mathsf{ready} = \mathsf{false})$$
$$\wedge\ (\mathsf{SFile}(s(n_2)) = \bot \rightarrow \ \mathsf{RQ} = q_2 \wedge \mathsf{SNo} = n_2 \wedge \mathsf{SBit} = b_1 \wedge \mathsf{ready} = \mathsf{true})$$

$$|$$

$$\tau: \ \forall N : \mathsf{SFile}(N) = \bot \vee \exists D : \mathsf{SFile}(N) = d \quad [*20*]$$

$$\vdots$$

$\tau: \ (\mathsf{SFile}(s(n_2)) = d_3 \quad [*21*]$	$\tau: \ \mathsf{SFile}(s(n_2)) = \bot \quad [*26*]$
$\tau: \ \mathsf{RQ} = q_2\|\mathsf{msg}(\mathsf{SFile}(s(n_2)), \mathsf{flip}(b_1)) \quad [*22*]$	$\tau: \ \mathsf{RQ} = q_2 \quad [*27*]$
$\tau: \ \mathsf{SNo} = s(n_2) \quad [*23*]$	$\tau: \ \mathsf{SNo} = n_2 \quad [*28*]$
$\tau: \ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [*24*]$	$\tau: \ \mathsf{SBit} = b_1 \quad [*29*]$
$\tau: \ \mathsf{ready} = \mathsf{false} \quad [*25*]$	$\tau: \ \mathsf{ready} = \mathsf{true} \quad [*30*]$
$\vdots$	$\vdots$

Tab. 0.7: Umgebung einer Anwendung von ProcAck.

$\vdots$

$\boxed{\begin{array}{c} p : [\ldots, \sigma, \circ, \tau, \ldots] \quad [\mathrm{P}] \\ \tau : \ \mathsf{CIMsg} = \mathsf{true} \quad [\mathrm{A}] \end{array}}$

aus CM1: $\sigma : \ \mathsf{E}\circ(\mathsf{CIMsg} = \mathsf{true}) \rightarrow (\exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)) \quad [*1*]$

$\sigma : \ \neg\mathsf{E}\circ(\mathsf{CIMsg} = \mathsf{true}) \quad [*2*]$

$\sigma : \ (\mathsf{A})\neg\circ(\mathsf{CIMsg} = \mathsf{true}) \quad [*3*]$

$[*3*]$ auf p:

$\tau : \ \neg(\mathsf{CIMsg} = \mathsf{true}) \quad [*4*]$

$\Box$ (A, $*4*$)

$\sigma : \ \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B) \quad [*5*]$

$\boxed{\sigma : \ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [*6*]}$

aus CM2:

$\tau : \ \mathsf{CIMsg} = \mathsf{true} \rightarrow \mathsf{SIM} = \perp \quad [*7*]$

$\tau : \ \neg\mathsf{CIMsg} = \mathsf{true} \quad [*8*]$

$\Box$ (A, $*8*$)

$\boxed{\tau : \ \mathsf{SIM} = \perp \quad [*9*]}$

$\vdots$

Tab. 0.8: Umgebung einer Anwendung von CIMsg.

$\vdots$

$\boxed{\begin{array}{c} p : [\ldots, \sigma, \circ, \tau, \ldots] \quad [\mathrm{P}] \\ \tau : \ \mathsf{AccDat} = \mathsf{true} \quad [\mathrm{A}] \end{array}}$

aus AD1: $\sigma : \ \mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}) \rightarrow (\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = B) \quad [*1*]$

$\sigma : \ \neg\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}) \quad [*2*]$

$\sigma : \ (\mathsf{A})\neg\circ(\mathsf{AccDat} = \mathsf{true}) \quad [*3*]$

$[*3*]$ auf p:

$\tau : \ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [*4*]$

$\square$ (A, $*4*$)

$\sigma : \ \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = B \quad [*5*]$

$\sigma : \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \wedge \mathsf{RBit} = b_1 \quad [*6*]$

$\boxed{\begin{array}{c} \sigma : \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [*7*] \\ \sigma : \ \mathsf{RBit} = b_1 \quad [*8*] \end{array}}$

aus AD2:

$\sigma : \ \forall D, B, N : \ (\mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RNo} = N \wedge \mathsf{RBit} = B \rightarrow \quad [*9*]$
$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(N) = D \wedge \mathsf{RNo} = s(N) \wedge \mathsf{RBit} = \mathsf{flip}(B)))$

$\sigma : \ (\mathsf{RIM} = \mathsf{msg}(D_2, B_2) \wedge \mathsf{RNo} = N_2 \wedge \mathsf{RBit} = B_2 \rightarrow \quad [*10*]$
$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(N_2) = D_2 \wedge \mathsf{RNo} = s(N_2) \wedge \mathsf{RBit} = \mathsf{flip}(B_2)))$

$\sigma : \ \neg(\mathsf{RIM} = \mathsf{msg}(D_2, B_2) \wedge \mathsf{RNo} = N_2 \wedge \mathsf{RBit} = B_2) \quad [*11*]$

$\sigma : \ \neg(\mathsf{RIM} = \mathsf{msg}(D_2, B_2) \quad [*14*]$

$\square$ $\{D_2 \leftarrow d_1, B_2 \leftarrow b_1\}$

$(*7*, *14*)$

$\sigma : \ \neg(\mathsf{RNo} = N_2) \quad [*15*]$

$\square$ (EA: $\{N_2 \leftarrow n_2\}$)

$\sigma : \ \neg(\mathsf{RBit} = b_1) \quad [*16*]$

$\square$ $(*8*, *16*)$

D_2, B_2, N_2 einsetzen:

LG : $\sigma : \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \wedge \mathsf{RNo} = n_2 \wedge \mathsf{RBit} = b_1 \quad [*12*]$

$\sigma : \ \mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(n_2) = d_1 \wedge \mathsf{RNo} = s(n_2) \wedge \mathsf{RBit} = \mathsf{flip}(b_1))) \quad [*13*]$

$\boxed{\sigma : \ \mathsf{RNo} = n_2 \quad [*17*]}$

$\sigma : \ (\mathsf{A})\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(n_2) = d_1 \wedge \mathsf{RNo} = s(n_2) \wedge \mathsf{RBit} = \mathsf{flip}(b_1))) \quad [*18*]$

$[*18*]$ auf p:

$\tau : \ \mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(n_2) = d_1 \wedge \mathsf{RNo} = s(n_2) \wedge \mathsf{RBit} = \mathsf{flip}(b_1)) \quad [*19*]$

$\tau : \ \neg\mathsf{AccDat} = \mathsf{true} \quad [*20*]$

$\square$ (A, $*20*$)

$\tau : \ \mathsf{RFile}(n_2) = d_1 \wedge \mathsf{RNo} = s(n_2) \wedge \mathsf{RBit} = \mathsf{flip}(b_1) \quad [*21*]$

$\boxed{\begin{array}{c} \tau : \ \mathsf{RFile}(n_2) = d_1 \quad [*22*] \\ \tau : \ \mathsf{RNo} = s(n_2) \quad [*23*] \\ \tau : \ \mathsf{RBit} = \mathsf{flip}(b_1) \quad [*24*] \end{array}}$

$\vdots$

Tab. 0.9: Umgebung einer Anwendung von AccDat.

$\vdots$

$\boxed{\begin{array}{c} p : [\ldots, \sigma, \circ, \tau, \ldots] \quad [\mathrm{P}] \\ \tau :\ \mathsf{AckMsg} = \mathsf{true} \quad [\mathrm{A}] \end{array}}$

aus AM1: $\sigma :\ \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}) \rightarrow (\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = \mathsf{flip}(B)) \quad [*1*]$

$\sigma :\ \neg\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}) \quad [*2*]$

$\sigma :\ (\mathsf{A})\neg\circ(\mathsf{AckMsg} = \mathsf{true}) \quad [*3*]$

$[*3*]$ auf p:

$\tau :\ \neg(\mathsf{AckMsg} = \mathsf{true}) \quad [*4*]$

$\Box\ (\mathrm{A}, *4*)$

$\sigma :\ \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = \mathsf{flip}(B) \quad [*5*]$

$\sigma :\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \wedge \mathsf{RBit} = \mathsf{flip}(b_1) \quad [*6*]$

$\boxed{\begin{array}{c} \sigma :\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [*7*] \\ \sigma :\ \mathsf{RBit} = \mathsf{flip}(b_1) \quad [*8*] \end{array}}$

aus AM2:

$\sigma :\ \forall D, B, Q :\ (\mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{SQ} = Q) \rightarrow \quad [*9*]$
$\mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \rightarrow (\mathsf{SQ} = Q|\mathsf{msg}(\lambda, B) \wedge \mathsf{RIM} = \bot))$

$\sigma :\ (\mathsf{RIM} = \mathsf{msg}(D_2, B_2) \wedge \mathsf{SQ} = Q_2) \rightarrow \quad [*10*]$
$\mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \rightarrow (\mathsf{SQ} = Q_2|\mathsf{msg}(\lambda, B_2) \wedge \mathsf{RIM} = \bot))$

$\sigma :\ \neg(\mathsf{RIM} = \mathsf{msg}(D_2, B_2) \wedge \mathsf{SQ} = Q_2) \quad [*11*]$

$\sigma :\ \neg(\mathsf{RIM} = \mathsf{msg}(D_2, B_2) \quad [*14*]$

$\Box\ \{D_2 \leftarrow d_1, B_2 \leftarrow b_1\}$

$(*7*, *14*)$

$\sigma :\ \neg(\mathsf{SQ} = Q_2) \quad [*15*]$

$\Box$ (EA: $\{Q_2 \leftarrow q_2\}$)

D_2, B_2, Q_2 einsetzen:

LG : $\sigma :\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \wedge \mathsf{SQ} = q_2 \quad [*12*]$

$\sigma :\ \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \rightarrow (\mathsf{SQ} = q_2|\mathsf{msg}(\lambda, b_1) \wedge \mathsf{RIM} = \bot)) \quad [*13*]$

$\boxed{\sigma :\ \mathsf{SQ} = q_2 \quad [*16*]}$

$\sigma :\ (\mathsf{A})\circ(\mathsf{AckMsg} = \mathsf{true} \rightarrow (\mathsf{SQ} = q_2|\mathsf{msg}(\lambda, b_1) \wedge \mathsf{RIM} = \bot)) \quad [*17*]$

$[*17*]$ auf p:

$\tau :\ \mathsf{AckMsg} = \mathsf{true} \rightarrow (\mathsf{SQ} = q_2|\mathsf{msg}(\lambda, b_1) \wedge \mathsf{RIM} = \bot) \quad [*18*]$

$\tau :\ \neg\mathsf{AckMsg} = \mathsf{true} \quad [*19*]$

$\Box\ (\mathrm{A}, *19*)$

$\tau :\ \mathsf{SQ} = q_2|\mathsf{msg}(\lambda, b_1) \wedge \mathsf{RIM} = \bot \quad [*20*]$

$\boxed{\begin{array}{c} \tau :\ \mathsf{SQ} = q_2|\mathsf{msg}(\lambda, b_1) \quad [*21*] \\ \tau :\ \mathsf{RIM} = \bot \quad [*22*] \end{array}}$

$\vdots$

Tab. 0.10: Umgebung einer Anwendung von AckMsg.

Als weiteres Schema steht die induktive Definition von unless^+ zur Verfügung:

$$\vdots$$

$$\boxed{\begin{array}{c} p : [\ldots, \sigma, \circ, \tau, \ldots] \quad [\mathrm{P}] \\ \sigma :\ A \quad [\mathrm{A1}] \\ \sigma :\ A \rightarrow \mathsf{A}(A\ \mathsf{unless}^+\ B) \quad [\mathrm{A2}] \end{array}}$$

$$\text{aus A2:} \quad \sigma :\ A \rightarrow \mathsf{A}(A\ \mathsf{unless}^+\ B) \quad [*1*]$$

$$\begin{array}{c} \sigma :\ \neg A \quad [*2*] \\ \square\ (\mathrm{A1}, *2*) \end{array} \qquad \begin{array}{c} \sigma :\ \mathsf{A}(A\ \mathsf{unless}^+\ B) \quad [*3*] \\ \sigma :\ (\mathsf{A})(A\ \mathsf{unless}^+\ B) \quad [*4*] \end{array}$$

$$\begin{array}{c} [*4*] \text{ auf } p\text{:} \\ \tau :\ \mathsf{A}(A\ \mathsf{unless}\ B) \quad [*5*] \end{array}$$

$$\boxed{\tau :\ B \quad [*6*]} \qquad \boxed{\begin{array}{c} \tau :\ A \quad [*7*] \\ \tau :\ \neg(B) \quad [*8*] \\ \tau :\ (\mathsf{A})(A\ \mathsf{unless}\ B) \quad [*9*] \end{array}}$$

$$\vdots \qquad\qquad \vdots$$

Tab. 0.11: Auswirkungen einer unless^+-Formel auf den unmittelbaren Nachfolgezustand.

Aussagen der Form „Start $\rightarrow \mathsf{A}\Box A$)“ – wobei „Start“ den Initialzustand einer Evolving Algebra bezeichnet, werden üblicherweise induktiv über die Folge der Berechnungszustände gezeigt. Dazu verwendet man als Ansatz das folgende Schema:

$$0:\ \neg(\text{Start} \rightarrow \mathsf{A}\Box A) \quad [0]$$

$$\begin{array}{c} 0:\ \text{Start} \quad [1] \\ 0:\ \neg\mathsf{A}\Box A \quad [2] \\ p : [\,0, \emptyset, \infty\,] \quad [3] \\ 0:\ p\neg\Box A \quad [4] \end{array}$$

$$\begin{array}{cc} \begin{array}{c} 0:\ \neg A \quad [5] \\ \vdots \\ \text{Tab. N.0} \end{array} & \begin{array}{c} 0:\ \neg(\neg A) \quad [6] \\ 0:\ (p)\neg\Box A \quad [7] \\ p : [\,0, \{\neg(\neg A)\}, a, \emptyset, \infty\,] \quad [8] \\ a:\ \neg A \quad [9] \end{array} \end{array}$$

$$\begin{array}{cc} \begin{array}{c} p : [\,0, \circ, a, \emptyset, \infty\,] \quad [10] \\ \vdots \\ \text{Tab. N.1} \end{array} & \begin{array}{c} p : [\,0, \{\neg(\neg A)\}, b, \circ, a, \emptyset, \infty\,] \quad [11] \\ b:\ \neg(\neg A) \quad [12] \\ \vdots \\ \text{Tab. N.2} \end{array} \end{array}$$

Tab. 0.12: Anlegen eines Induktionsbeweises:
Aufspaltung in Induktionsanfang und Induktionsschritt

Tab. N.0 beinhaltet dabei den Induktionsanfang, Tab. N.1 den ersten und Tab. N.2 einen beliebigen Induktionsschritt. Da man im allgemeinen im Induktionsschritt in Tab. N.2 nur die Formeln $b : A$ und $a : \neg A$ verwendet, ordnet sich der mittlere Ast dem rechten für $0 \equiv b$ unter.

Präfixe und Pfade werden i.a. mit lateinischen Buchstaben bezeichnet. In allen Beweisen werden in Pfadinformationsformeln i.a. nur die noch benötigten Teilformeln angegeben und mitgeführt.

Abschlüsse, die mit $\Box^*$ gekennzeichnet sind, schließen Äste unter Verwendung nichtatomarer Formeln ab. Die entsprechenden Extensionen der Äste zum Erreichen eines Abschlusses mit ausschließlich atomaren Formeln sind trivial.

5 Lemma 1: Die grundlegende Entwurfsüberlegung

Aussage von Lemma 1 ist, daß in die Projektion der Folge ($\mathsf{SIM}|\mathsf{SQ}|\mathsf{RIM}|\mathsf{SQ}$) von Nachrichten auf die Folge ihrer Kontrollbits als regulärer Ausdruck von der Form ($\mathsf{flip}(\mathsf{SBit})^* \ \mathsf{SBit}^*$) ist.

$$\text{Start} \rightarrow \mathsf{A}\Box A$$

mit

$$A \equiv A1 \wedge A2 \wedge A3 \wedge A4 \wedge A5$$

und

$$\begin{array}{ll}
A1 \equiv \forall B: & (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow \\
& (B = \mathsf{SBit} \rightarrow \quad ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge \\
& \qquad\qquad\qquad (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge \\
& \qquad\qquad\qquad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) \\
A2 \equiv \forall B, B': & (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}) \\
A3 \equiv \forall B: & (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \rightarrow \\
& (B = \mathsf{SBit} \rightarrow \quad ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge \\
& \qquad\qquad\qquad (\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q'')))) \\
A4 \equiv \forall B: & (\exists D : \mathsf{RIM} = \mathsf{msg}(D, B)) \rightarrow (B = \mathsf{SBit} \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', B)|Q')) \\
A5 \equiv \forall B, B': & (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit})
\end{array}$$

Mit reiner Prädikatenlogik lassen sich einige einfache Folgerungen beweisen:

A6: $\forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \rightarrow (B = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B)))$

A7: $\forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \rightarrow$
$(B = \mathsf{SBit} \rightarrow (\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit}))$

A8: $\forall B : (\exists D, Q, Q' : \mathsf{SQ} = Q|\mathsf{msg}(D, B)|Q') \rightarrow$
$(B = \mathsf{SBit} \rightarrow (\exists D', Q'' : \mathsf{SQ} = Q''|\mathsf{msg}(D', B)))$

A9, A10, A11 analog für RQformuliert

Analog auch für RQ.

Beweis von A6:

A2: $\forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit})$ [1]

$(\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_1)|Q'|\mathsf{msg}(D',B_1')|Q'') \rightarrow (B_1 = \mathsf{SBit} \rightarrow B_1' = \mathsf{SBit})$ [2]

¬A6: $\neg(\forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D,B)|Q) \rightarrow (B = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D',B))))$ [3]

$\neg((\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D,b_2)|Q) \rightarrow (b_2 = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D',b_2))))$ [4]

$\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D,b_2)|Q$ [5]

$\neg(b_2 = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D',b_2)))$ [6]

$\mathsf{SQ} = \mathsf{msg}(d_2,b_2)|q_2$ [7]

$b_2 = \mathsf{SBit}$ [8]

$\neg(\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D',b_2))$ [9]

$\neg(\mathsf{SQ} = Q_2'|\mathsf{msg}(D_2',b_2))$ [10]

aus Q3:

$\forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D,B)|Q') \rightarrow Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D',B'))$ [11]

$(\exists D, B : Q_3 = \mathsf{msg}(D,B)|Q_3') \rightarrow Q_3' = \varepsilon \vee (\exists D', B', Q'' : Q_3' = Q''|\mathsf{msg}(D',B'))$ [12]

$\neg(\exists D, B : Q_3 = \mathsf{msg}(D,B)|Q_3')$ [13]

$\neg(Q_3 = \mathsf{msg}(D_3,B_3)|Q_3')$ [15]

$\Box\ \{Q_3 \leftarrow \mathsf{SQ}, D_3 \leftarrow d_2$
$B_3 \leftarrow b_2, Q_3' \leftarrow q_2\}(7,15)$

$q_2 = \varepsilon \vee (\exists D', B', Q'' : q_2 = Q''|\mathsf{msg}(D',B'))$ [14]

$q_2 = \varepsilon$ [16]

$\mathsf{SQ} = \mathsf{msg}(d_2,b_2)|q_2$ [7]
$q_2 = \varepsilon$ [16]
$\neg(\mathsf{SQ} = Q_2'|\mathsf{msg}(D_2',b_2))$ [10]
$\Box\ \{Q_2' \leftarrow \varepsilon, D_2' \leftarrow d_2\}$

$\exists D', B', Q'' : q_2 = Q''|\mathsf{msg}(D',B')$ [17]

$q_2 = q_3''|\mathsf{msg}(d_3',b_3')$ [18]

$q_2 = q_3''|\mathsf{msg}(d_3',b_3')$ [18]
$\mathsf{SQ} = \mathsf{msg}(d_2,b_2)|q_2$ [7]
$\mathsf{SQ} = \mathsf{msg}(d_2,b_2)|q_3''|\mathsf{msg}(d_3',b_3')$ [19]

$\hookrightarrow$

$$\vdots$$

von [19]:

$\mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_3''|\mathsf{msg}(d_3', b_3')$ [19]

aus [2]:

$\neg(\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_1)|Q'|\mathsf{msg}(D', B_1')|Q'')$ [20]

$\neg(\mathsf{SQ} = Q_1|\mathsf{msg}(D_1, B_1)|Q_1'|\mathsf{msg}(D_1', B_1')|Q_1'')$ [22]

$\square$: $\mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_3''|\mathsf{msg}(d_3', b_3')$ [19]
$\{Q_1 = Q_1'' \leftarrow \varepsilon, Q_1' \leftarrow q_3'', D_1 \leftarrow d_2, B_1 \leftarrow b_2, D_1' \leftarrow d_3', B_1' \leftarrow b_3'\}$

B_1, B_1' einsetzen:

$(b_2 = \mathsf{SBit} \rightarrow b_3' = \mathsf{SBit})$ [23]

$\neg(b_2 = \mathsf{SBit})$ [24]

$\square(5, 24)$

$b_3' = \mathsf{SBit}$ [25]

[9] noch einmal instantiieren:

$\neg(\mathsf{SQ} = Q_4'|\mathsf{msg}(D_4', b_2))$ [26]

$\square$: $\neg(\mathsf{SQ} = Q_4'|\mathsf{msg}(D_4', b_2))$ [26]
$b_2 = \mathsf{SBit}$ [8]
$b_3' = \mathsf{SBit}$ [25]
$\mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_3''|\mathsf{msg}(d_3', b_3')$ [19]
$\{Q_4' \leftarrow \mathsf{msg}(d_2, b_2)|q_3'', D_4' \leftarrow d_3'\}$

A7 ist analog zu beweisen.

Es folgt der Beweis des Lemmas.
Er verwendet das Schema aus Tab. 0.12 zur Durchführung eines Induktionsbeweises.

Induktionsanfang: ein rein prädikatenlogisches nahezu triviales Tableau

$$
\begin{array}{c}
\vdots \\
0: \ \text{Start} \quad [1] \\
0: \ \neg A \quad [5] \\
| \\
\text{aus } [1]: \\
0: \ \mathsf{SIM} = \bot \quad [13] \\
0: \ \mathsf{SQ} = \varepsilon \quad [14] \\
0: \ \mathsf{RIM} = \bot \quad [15] \\
0: \ \mathsf{RQ} = \varepsilon \quad [16] \\
\vdots \\
\text{aus } [5]: \\
0: \ \neg A1 \vee \neg A2 \vee \neg A3 \vee \neg A4 \vee \neg A5 \quad [17] \\
\vdots
\end{array}
$$

wegen [13]-[16] sind die Implikationen A1-A5 trivialerweise erfüllt.

Das an Knoten [12] von Tab. 0.12 anschließende Tableau beinhaltet den Induktionsschritt.

Dabei ergibt sich schon sehr früh – begründet in der negierten Konjunktion der Aussagen A1-A5 – für jede der Aussagen ein Ast, der sich, da diese Teilaussagen jeweils wieder Konjunktionen von Teilaussagen sind, nochmals aufspaltet. Damit erhält man acht voneinander unabhängige Teilbeweise. Da diese insgesamt ca. 1500 Knoten enthalten, wird die Numerierung jedes Teilbeweises von den anderen isoliert betrachtet fortlaufend von dem Knoten vorgenommen, an dem er von dem Resttableau abzweigt.

Als Induktionsvoraussetzung im Zustand b wird jeweils die Gesamtaussage verwendet, wobei die Taktik ist, für jede Aussage A_n in erster Linie A_n als Induktionsvoraussetzung zu nutzen. Dies ergibt jeweils „Hauptäste“ der Teiltableaux, nur dort, wo dies nicht genügt, werden in „Seitenästen“ die anderen Teilaussagen verwendet.

Zu Beginn jedes Teilbeweises wird das Vorgehen im Stil eines „mathematischen“ Beweises beschrieben, bevor der Tableaubeweis formal ausgeführt wird.

5.1 1. Teilaussage, 1. Teil

In dem ersten Teiltableau – mit Knoten [20] beginnend – wird die Aussage A1 bewiesen. Dieses spaltet sich – entsprechend den drei Teilaussagen von A1 – in [36] in drei Teiltableaux auf.

Beweisskizze für A1, erste Teilaussage:

Situation:
$\mathsf{SIM}_a \neq \perp$, $\mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{SBit}$, $\mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_a)) \neq \mathsf{SBit}_a$,

Die Induktionsvoraussetzung A1 wird in b ausgewertet, wobei sich drei Fälle ergeben:

$\mathsf{SIM}_b = \perp$ ([51],[56]):
Man kann direkt schließen, daß in dem betrachteten Schritt SendCom angewendet wurde.
Da SendCom die erste Nachricht aus SQ_b entfernt, und SQ_a nachher nicht leer ist, enthält SQ_b mindestens zwei Nachrichten.
Nach Ind.Vor. A2 für b ist entweder $\mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b) \neq \mathsf{SBit}_b$, oder für je zwei Nachrichten in SQ_b sind die Kontrollbits gleich.
Im ersten Fall ergibt sich nach der Anwendung von SendCom $\mathsf{SIM}_a = \mathsf{head}(\mathsf{SQ}_b)$ und damit $\mathsf{SBit}_a = \mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b)) \neq \mathsf{SBit}_b$. Dazu müßte sich SBit geändert haben, was nur durch ProcAck geschehen kann, dies ist aber in b wegen $\mathsf{SIM} = \perp$ nicht anwendbar.
Im zweiten Fall ist $\mathsf{SBit}_a = \mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b)) = \mathsf{Bit}(\mathsf{head}(\mathsf{tail}(\mathsf{SQ}_b))) = \mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_a))$, womit nun in a die Bits von SIM und des Kopfes von SQ entgegen der Annahme doch übereinstimmen. Hier kommt die Voraussetzung ins Spiel, daß keine zwei SQ verändernden Regeln gleichzeitig angewendet werden – es kann also nicht durch SLose eine Nachricht verloren gehen oder durch AckMsg eine neue angehängt werden.
Damit ist also $\mathsf{SIM}_b \neq \perp$. Man stellt fest, daß sich SIM im betrachteten Schritt nicht verändert haben kann, da b einer Anwendung von SendCom und a einer Anwendung von ClMsg widerspricht.

$\mathsf{SIM}_b \neq \perp$, $\mathsf{SBit}_a = \mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{Bit}(\mathsf{SIM}_b) \neq \mathsf{SBit}_b$ ([99]):
Diese Veränderung von SBit ist jedoch ausgeschlossen, da als Voraussetzung für ProcAck $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ gelten müßte.

Bleibt die Situation in [101], in der man für b aus A1 eine Aussage erhält:
$\mathsf{SIM}_b \neq \perp$, $\mathsf{Bit}(\mathsf{SIM}) = \mathsf{SBit}$. Nach A1 ist somit SQ_b leer, oder $\mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b)) = \mathsf{SBit}_b$. Aus A2 folgt in diesem Fall weiterhin, daß alle anderen Nachrichten in SQ_b ebenfalls $SBit_b$ als Kontrollbit besitzen, aus A3, daß RIM_b – falls es nicht leer ist – ebenfalls eine Nachricht mit diesem Kontrollbit ist.
SIM ist in a und b die gleiche Nachricht, da SendCom in b nicht anwendbar ist und ClMsg in a nicht angewendet worden sein kann.
Da in beiden Zuständen Bit(SIM)=SBit ist, folgt, daß SBit in a und b ebenfalls gleich ist.
Also muß sich SQ verändert haben (zumindest das Kontrollbit der ersten Nachricht).
Dies kann nicht durch SendCom geschehen sein, da dazu SIM_b leer gewesen sein müßte.
SLose könnte die erste Nachricht entfernt haben, womit $\mathsf{head}(\mathsf{SQ}_a) = \mathsf{head}(\mathsf{tail}(\mathsf{SQ}_b))$ ist. Nach Voraussetzung ist dann $\mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b)) = \mathsf{Bit}(\mathsf{head}(\mathsf{tail}(\mathsf{SQ}_b))) = \mathsf{SBit}_b = \mathsf{SBit}_a$.

AckMsg wirkt sich nur auf $\mathsf{head}(\mathsf{SQ}_a)$ aus, falls SQ_b leer ist. In diesem Fall ist dann $\mathsf{head}(\mathsf{SQ}_a) = \mathsf{RIM}_b$ und nach Voraussetzung $\mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_a)) = \mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{SBit}_a$.

$$\vdots$$

$$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$

$$a :\ \neg A \quad [9]$$

$$b :\ A \quad [12]$$

$$\vdots$$

aus[12]:

$$b :\ A1 \quad [13]$$

$$b :\ A2 \quad [14]$$

$$b :\ A3 \quad [15]$$

$$b :\ A4 \quad [16]$$

$$b :\ A5 \quad [17]$$

$$|$$

aus[9]:

$$a :\ \neg(A1 \wedge A2 \wedge A3 \wedge A4 \wedge A5) \quad [18]$$

$$a :\ \neg A1 \vee \neg A2 \vee \neg A3 \vee \neg A4 \vee \neg A5 \quad [18']$$

$$a :\ \neg A1 \quad [20] \qquad\qquad a :\ \neg A2 \vee \neg A3 \vee \neg A4 \vee \neg A5 \quad [21]$$

↪ S. 64

$$\begin{array}{ll} a :\ \neg\forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow & [30] \\ \quad (B = \mathsf{SBit} \rightarrow \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge & \\ \quad\quad (\mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge & \\ \quad\quad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) & \end{array}$$

$$|$$

$$\begin{array}{ll} a :\ \neg((\exists D : \mathsf{SIM} = \mathsf{msg}(D, b_1)) \rightarrow & [31] \\ \quad (b_1 = \mathsf{SBit} \rightarrow \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_1)|Q^1)) \wedge & \\ \quad\quad (\mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_1)) \wedge & \\ \quad\quad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_1)|Q^3))))) & \end{array}$$

$$|$$

$$a :\ \exists D : \mathsf{SIM} = \mathsf{msg}(D, b_1) \quad [32]$$

$$|$$

$$\begin{array}{ll} a :\ \neg(b_1 = \mathsf{SBit} \rightarrow \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_1)|Q^1)) \wedge & [33] \\ \quad (\mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_1)) \wedge & \\ \quad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_1)|Q^3)))) & \end{array}$$

$$|$$

$$\boxed{a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]}$$

↪ S. 32

$\vdots$

von [33/34] (S. 31):

$$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$

$$a: \ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]$$

aus [33]:

$$\boxed{a: \ b_1 = \mathsf{SBit} \quad [35]}$$

$$\begin{aligned} a: \ \neg((&\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_1)|Q^1)) \wedge \quad [36] \\ &(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_1)) \wedge \\ &(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_1)|Q^3))) \end{aligned}$$

$$\begin{aligned} a: \ \neg((&\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_1)) \wedge \quad [38] \\ &(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_1)|Q^3))) \end{aligned}$$

$\hookrightarrow$ S. 43

$$a: \ \neg(\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_1)|Q^1)) \quad [37]$$

$$a: \ \neg(\mathsf{SQ} = \varepsilon) \quad [39]$$

$$a: \ \neg(\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_1)|Q^1) \quad [40]$$

$$\boxed{a: \ \neg(\mathsf{SQ} = \mathsf{msg}(D^1_1, b_1)|Q^1_1) \quad [41]}$$

aus F1S:

$$a: \ \mathsf{SQ} = \varepsilon \vee (\exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q \wedge \exists D', B', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')) \quad [42]$$

$$a: \ \mathsf{SQ} = \varepsilon \quad [43]$$

$$\Box \ (39, 43)$$

$$a: \ \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q \wedge \exists D', B', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B') \quad [44]$$

$$a: \ \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q \quad [45]$$

$$a: \ \exists D', B', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B') \quad [46]$$

$$\boxed{\begin{aligned} &a: \ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [47] \\ &a: \ \mathsf{SQ} = q_2'|\mathsf{msg}(d_2', b_2') \quad [48] \end{aligned}}$$

$\hookrightarrow$ S. 33

$$\vdots$$

von [47]/[48] (S. 32):

$$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]$$
$$a:\ b_1 = \mathsf{SBit} \quad [35]$$
$$a:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1) \quad [41]$$
$$a:\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [47]$$
$$a:\ \mathsf{SQ} = q_2'|\mathsf{msg}(d_2', b_2') \quad [48]$$

"passende" Induktionsvoraussetzung A1 anwenden:

$$b:\ A1 \quad [13]:$$

$$\begin{aligned} b:\ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow & \qquad [49]\\ (B = \mathsf{SBit} \rightarrow \ & ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge \\ & (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge \\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) \end{aligned}$$

$$\begin{aligned} b:\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_3)) \rightarrow & \qquad [50]\\ (B_3 = \mathsf{SBit} \rightarrow \ & ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B_3)|Q^1)) \wedge \\ & (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B_3)) \wedge \\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B_3)|Q^3)))) \end{aligned}$$

Linker Zweig:

$$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_3)) \quad [51]$$
$$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_3, B_3)) \quad [54]$$

Rechter Zweig:

B_3 einsetzen:

$$\text{LG}:\ b:\ \exists D : \mathsf{SIM} = \mathsf{msg}(D, b_9) \quad [52]$$

$$\begin{aligned} b:\ (b_9 = \mathsf{SBit} \rightarrow & \qquad [53]\\ & ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1)) \wedge \\ & (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_9)) \wedge \\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_9)|Q^3)))) \end{aligned}$$

aus [52]:

$$\boxed{b:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9) \quad [87]}$$

$\hookrightarrow$ S. 36

$$\text{aus F2S:}\quad b:\ \mathsf{SIM} = \bot \vee \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B) \quad [55]$$

$$\boxed{b:\ \mathsf{SIM} = \bot \quad [56]}$$

$\hookrightarrow$ S. 34

$$b:\ \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B) \quad [57]$$
$$b:\ \mathsf{SIM} = \mathsf{msg}(d_9, b_9) \quad [86]$$
$$\Box\ \{D_3 \leftarrow d_9, B_3 \leftarrow b_9\}(54, 86)$$

$\vdots$

von [56] (S. 33):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]

$a:\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2$ [47]

$b:\ \mathsf{SIM} = \bot$ [56]

aus SIM: $b:\ \forall M : \mathsf{SIM} = M \rightarrow \mathsf{A}(\mathsf{SIM} = M\ \mathsf{unless}^+\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})$ [58]

mit Tab. 0.11, $\{M \leftarrow \bot\}$:

$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true}$ [59]

- $a:\ \mathsf{SendCom} = \mathsf{true}$ [61]
  aus Tab. 0.1:
  $b:\ \mathsf{SIM} = \bot$ [63]
  $b:\ \mathsf{SQ} = \mathsf{msg}(d_4, b_4)|q_4$ [64]
  $a:\ \mathsf{SQ} = q_4$ [65]
  $a:\ \mathsf{SIM} = \mathsf{msg}(d_4, b_4)$ [66]

- $a:\ \mathsf{ClMsg} = \mathsf{true}$ [62]
  aus Tab. 0.8:
  $a:\ \mathsf{SIM} = \bot$ [84]
  $b:\ \mathsf{SIM} = \mathsf{msg}(d_8, b_8)$ [85]
  $\Box$ (E3, 34, 84)

$a:\ \mathsf{SIM} = \bot$ [60]
$\Box$ (E3, 34, 60)

für SendCom: A2 als Induktionsvoraussetzung liefert die Aussage:

aus $b:\ A2$ [14] :

$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit})$ [67]

$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_5)|Q'|\mathsf{msg}(D', B_5')|Q'') \rightarrow (B_5 = \mathsf{SBit} \rightarrow B_5' = \mathsf{SBit})$ [68]

- $b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_5)|Q'|\mathsf{msg}(D', B_5')|Q'')$ [69]
  $b:\ \neg(\mathsf{SQ} = Q_5|\mathsf{msg}(D_5, B_5)|Q_5'|\mathsf{msg}(D_5', B_5')|Q_5'')$ [71]

- B_5, B_5' einsetzen:
  $b:\ b_4 = \mathsf{SBit} \rightarrow b_2 = \mathsf{SBit}$ [70]
  $\hookrightarrow$ S. 35

$$\boxed{\begin{array}{l}
\Box\ a:\ \mathsf{SQ} = q_4 \quad [65] \\
\underline{a:\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [47]} \\
q_4 = \mathsf{msg}(d_2, b_2)|q_2 \\
\underline{b:\ \mathsf{SQ} = \mathsf{msg}(d_4, b_4)|q_4 \quad [64]} \\
b:\ \mathsf{SQ} = \mathsf{msg}(d_4, b_4)|\mathsf{msg}(d_2, b_2)|q_2 \\
b:\ \neg(\mathsf{SQ} = Q_5|\mathsf{msg}(D_5, B_5)|Q_5'|\mathsf{msg}(D_5', B_5')|Q_5'') \quad [71] \\
\{Q_5 = Q_5' \leftarrow \varepsilon, D_5 \leftarrow d_4, B_5 \leftarrow b_4, D_5' \leftarrow d_2, B_5' \leftarrow b_2, Q_5'' \leftarrow q_2\}
\end{array}}$$

$\vdots$

von [70] (S. 34):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]

$a :\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2$ [47]

$b :\ \mathsf{SIM} = \bot$ [56]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_4, b_4)$ [66]

$b :\ b_4 = \mathsf{SBit} \rightarrow b_2 = \mathsf{SBit}$ [70]

$b :\ \neg(b_4 = \mathsf{SBit})$ [72]

aus EA:

$b :\ \exists B : \mathsf{SBit} = B$ [75]

$b :\ \mathsf{SBit} = b_6$ [76]

LG : $b :\ b_4 = \mathsf{SBit}$ [73]

$b :\ b_2 = \mathsf{SBit}$ [74]

$$
\begin{array}{ll}
\square & b :\ b_4 = \mathsf{SBit} \quad [73] \\
& \underline{b :\ b_2 = \mathsf{SBit} \quad [74]} \\
& \rightarrow\ b_4 = b_2 \\
& a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34] \\
& \underline{a :\ \mathsf{SIM} = \mathsf{msg}(d_4, b_4) \quad [66]} \\
& \rightarrow\ b_1 = b_4 \\
& a :\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [47] \\
& \underline{a :\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1) \quad [41]} \\
& \rightarrow\ b_1 \neq b_2 \\
& \{D_1^1 \leftarrow d_2,\ Q_1^1 \leftarrow q_2\}
\end{array}
$$

aus SBit: $b :\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [77]

mit Tab. 0.11, $\{B \leftarrow b_6\}$:

$a :\ \mathsf{ProcAck} = \mathsf{true}$ [78]

mit Tab. 0.7:

$b :\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [82]

$b :\ \mathsf{SBit} = b_7$ [83]

usw.

$\square\ (56, 82)$

$a :\ \mathsf{SBit} = b_6$ [79]

$a :\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [80]

$a :\ (\mathsf{A})(\mathsf{SBit} = b_6 \ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})$ [81]

$$
\begin{array}{lll}
\square : & \multicolumn{2}{l}{a :\ \mathsf{SIM} = \mathsf{msg}(d_4, b_4) \quad [66]} \\
& \multicolumn{2}{l}{\underline{a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]}} \\
& \multicolumn{2}{l}{\rightarrow\ b_4 = b_1} \\
& a :\ \mathsf{SBit} = b_6 \quad [79] & b :\ \mathsf{SBit} = b_6 \quad [76] \\
& \underline{a :\ b_1 = \mathsf{SBit} \quad [35]} & \underline{b :\ \neg(b_4 = \mathsf{SBit}) \quad [72]} \\
& \rightarrow\ b_6 = b_1 & \rightarrow\ b_6 \neq b_4
\end{array}
$$

$\vdots$

von [87] (S. 33):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :\ b_1 = \mathsf{SBit}$ [35]

$a :\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]

$a :\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2$ [47]

$a :\ \mathsf{SQ} = q_2'|\mathsf{msg}(d_2', b_2')$ [48]

|

$b :\ (b_9 = \mathsf{SBit} \rightarrow$ [53]
$((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1)) \wedge$
$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_9)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_9)|Q^3))))$

|

$b :\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [87]

|

aus SIM: $b :\ \forall M : \mathsf{SIM} = M \rightarrow \mathsf{A}(\mathsf{SIM} = M \ \mathsf{unless}^+ \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})$ [88]

mit Tab. 0.11, $\{M \leftarrow \mathsf{msg}(d_{10}, b_9)\}$:

$a :\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true}$ [89]

$a :\ \mathsf{SendCom} = \mathsf{true}$ [91]
aus Tab. 0.1:
$b :\ \mathsf{SIM} = \bot$ [93]
$b :\ \mathsf{SQ} = \mathsf{msg}(d_{11}, b_{11})|q_{11}$ [94]
$a :\ \mathsf{SQ} = q_{11}$ [95]
$a :\ \mathsf{SIM} = \mathsf{msg}(d_{11}, b_{11})$ [96]
$\square$ (E3, 87, 93)

$a :\ \mathsf{ClMsg} = \mathsf{true}$ [92]
aus Tab. 0.8:
$a :\ \mathsf{SIM} = \bot$ [97]
$b :\ \mathsf{SIM} = \mathsf{msg}(d_{12}, b_{12})$ [98]
$\square$ (E3, 34, 97)

$\boxed{a :\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9) \quad [90]}$

[53] auflösen:

$b :\ \neg(b_9 = \mathsf{SBit})$ [99]
$\hookrightarrow$ S. 37

$\boxed{\mathrm{LG} :\ b :\ b_9 = \mathsf{SBit} \quad [100]}$

|

$b :\ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1)) \wedge$ [101]
$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_9)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_9)|Q^3)))$
$\hookrightarrow$ S. 38

$$\vdots$$

von [99] (S. 36):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ b_1 = \mathsf{SBit}$ [35]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [87]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [90]

$b:\ \neg(b_9 = \mathsf{SBit})$ [99]

$|$

aus EA:

$b:\ \exists B : \mathsf{SBit} = B$ [102]

$b:\ \mathsf{SBit} = b_{11}$ [103]

$|$

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B\ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})$ [104]

mit Tab. 0.11, $\{B \leftarrow b_{13}\}$:

Linker Zweig:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [105]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{14}, b_{14})$ [109]

$b:\ \mathsf{SBit} = b_{14}$ [110]

$$\boxed{\begin{array}{ll}
\square: & b:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9) \quad [87] \\
 & b:\ \mathsf{SIM} = \mathsf{msg}(d_{14}, b_{14}) \quad [109] \\ \hline
 & \rightarrow\ b_9 = b_{14} \\
 & b:\ \neg(b_9 = \mathsf{SBit}) \quad [99] \\
 & b:\ \mathsf{SBit} = b_{14} \quad [110] \\ \hline
 & \rightarrow\ b_9 \neq b_{14}
\end{array}}$$

Rechter Zweig:

$a:\ \mathsf{SBit} = b_{13}$ [106]

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [107]

$a:\ (\mathsf{A})(\mathsf{SBit} = b_{13}\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})$ [108]

$$\boxed{\begin{array}{ll}
\square: & a:\ \mathsf{SBit} = b_{13} \quad [106] \\
 & a:\ b_1 = \mathsf{SBit} \quad [35] \\ \hline
 & \rightarrow\ b_{13} = b_1 \\
 & a:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9) \quad [90] \\
 & a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34] \\ \hline
 & \rightarrow\ b_9 = b_1 \\
 & b:\ \mathsf{SBit} = b_{13} \quad [103] \\
 & b:\ \neg(b_9 = \mathsf{SBit}) \quad [99] \\ \hline
 & \rightarrow\ b_{13} \neq b_9
\end{array}}$$

$\vdots$

von [101] (S. 36):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :$ $\mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :$ $\neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]

$a :$ $\mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2$ [47]

$b :$ $\mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [87]

$a :$ $\mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [90]

$b :$ $b_9 = \mathsf{SBit}$ [100]

|

aus [101]:

$b :$ $\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1)$ [111]

$b :$ $\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_9)$ [112]

$b :$ $\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_9)|Q^3)$ [113]

|

aus EA:

$b :$ $\exists Q : \mathsf{SQ} = Q$ [114]

$\boxed{b : \ \mathsf{SQ} = q_{15} \quad [115]}$

|

$b :$ $\forall Q : \mathsf{SQ} = Q \rightarrow \mathsf{A}(\mathsf{SQ} = Q\ \mathsf{unless}^+\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [116]

mit Tab. 0.11, $\{Q \leftarrow q_{15}\}$:

$a :$ $\mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [117]
$\hookrightarrow$ S. 39

$a :$ $\mathsf{SQ} = q_{15}$ [118]

aus [111]:

$b :$ $\mathsf{SQ} = \varepsilon$ [154]

□	$b :$ $\mathsf{SQ} = \varepsilon$ [154]
	$b :$ $\mathsf{SQ} = q_{15}$ [115]
	$a :$ $\mathsf{SQ} = q_{15}$ [118]
	$a :$ $\mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2$ [47]
	E2

$b :$ $\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1$ [155]

$b :$ $\mathsf{SQ} = \mathsf{msg}(d_{24}^1, b_9)|q_{24}^1$ [155]

□

$$\frac{a : \ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \ [34] \qquad a : \ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9) \ [90]}{\rightarrow\ b_1 = b_9}$$

$$\frac{a : \ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1) \ [41] \qquad a : \ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2 \ [47]}{\rightarrow\ b_1 \neq b_2}$$

$b :$ $\mathsf{SQ} = \mathsf{msg}(d_{24}^1, b_9)|q_{24}^1$ [155] $\{D_1^1 \leftarrow d_{24}^1,\ Q_1^1 \leftarrow q_{24}^1\}$

$b :$ $\mathsf{SQ} = q_{15}$ [115]

$a :$ $\mathsf{SQ} = q_{15}$ [118]

$a :$ $\mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2$ [47]

$\rightarrow\ b_9 = b_2$

$\vdots$

von [117] (S. 38):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:$ $\mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:$ $\neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]

$a:$ $\mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2$ [47]

$b:$ $\mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [87]

$a:$ $\mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [90]

$b:$ $b_9 = \mathsf{SBit}$ [100]

$b:$ $\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1)$ [111]

$a:$ $\mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [117]

$a:$ $\mathsf{SendCom} = \mathsf{true}$ [119]

aus Tab. 0.1:

$b:$ $\mathsf{SIM} = \perp$ [122]

$b:$ $\mathsf{SQ} = \mathsf{msg}(d_{16}, b_{16})|q_{16}$ [123]

$a:$ $\mathsf{SQ} = q_{16}$ [124]

$a:$ $\mathsf{SIM} = \mathsf{msg}(d_{16}, b_{16})$ [125]

$\Box$ $(\mathrm{E3}, 87, 122)$

$a:$ $\mathsf{SLose} = \mathsf{true}$ [120]

aus Tab. 0.3, SL2":

$b:$ $\mathsf{SQ} \neq \varepsilon$ [126]

- $a:$ $\neg(\mathsf{SQ} = \mathsf{msg}(D_{17}, B_{17})|Q_{17})$ [127]

  $\Box$ $\{D_{17} \leftarrow d_2, B_{17} \leftarrow b_2, Q_{17} \leftarrow q_2\}$

  $(47, 127)$

- $b:$ $\mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q'_{17}$ [128]

  aus [111]:

  - $b:$ $\mathsf{SQ} = \varepsilon$ [130]

    $\Box$ $(126, 130)$

  - $b:$ $\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1$ [131]

    $b:$ $\mathsf{SQ} = \mathsf{msg}(d^1_{18}, b_9)|q^1_{18}$ [132]

- $b:$ $\mathsf{SQ} = \mathsf{msg}(d'_{17}, b'_{17})|\mathsf{msg}(d_2, b_2)|q_2$ [129]

  $\hookrightarrow$ S. 40

$a:$ $\mathsf{AckMsg} = \mathsf{true}$ [121]

aus Tab. 0.10:

$b:$ $\mathsf{RIM} = \mathsf{msg}(d_{21}, b_{21})$ [143]

$b:$ $\mathsf{RBit} = \mathsf{flip}(b_{21})$ [144]

$b:$ $\mathsf{SQ} = q_{22}$ [145]

$a:$ $\mathsf{SQ} = q_{22}|\mathsf{msg}(\lambda, b_{21})$ [146]

$a:$ $\mathsf{RIM} = \perp$ [147]

$\hookrightarrow$ S. 41

$\Box$

$$\frac{a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)\ [34] \qquad a:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)\ [90]}{\rightarrow\ b_1 = b_9}$$

$$\frac{a:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)\ [41] \qquad a:\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2\ [47]}{\rightarrow\ b_1 \neq b_2}$$

$$\frac{b:\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q'_{17}\ [128] \qquad b:\ \mathsf{SQ} = \mathsf{msg}(d^1_{18}, b_9)|q^1_{18}\ [132]}{\rightarrow\ b_9 = b_2}$$

$\{D_1^1 \leftarrow d_2, Q_1^1 \leftarrow q_2\}$

$\vdots$

von [129] (S. 39):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]

$a :\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2$ [47]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [90]

$b :\ b_9 = \mathsf{SBit}$ [100]

$b :\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1)$ [111]

$b :\ \mathsf{SQ} = \mathsf{msg}(d'_{17}, b'_{17})|\mathsf{msg}(d_2, b_2)|q_2$ [129]

aus [111]:

$b :\ \mathsf{SQ} = \varepsilon$ [133]

$\square$ $(126, 133)$

$b :\ \exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1$ [134]

$b :\ \mathsf{SQ} = \mathsf{msg}(d_{19}^1, b_9)|q_{19}^1$ [135]

verlorene erste Nachricht: Ind.Vor. A2:

$b :\ A2$ [14]

$b :\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \to (B = \mathsf{SBit} \to B' = \mathsf{SBit})$ [136]

$b :\ (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{20})|Q'|\mathsf{msg}(D', B'_{20})|Q'') \to (B_{20} = \mathsf{SBit} \to B'_{20} = \mathsf{SBit})$ [137]

$b :\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{20})|Q'|\mathsf{msg}(D', B'_{20})|Q'')$ [138]

$b :\ \neg(\mathsf{SQ} = Q_{20}|\mathsf{msg}(D_{20}, B_{20})|Q'|\mathsf{msg}(D'_{20}, B'_{20})|Q''_{20})$ [140]

$\square$ $\{\ Q_{20} = Q'_{20} \leftarrow \varepsilon, D_{20} \leftarrow d'_{17}, b_{20} \leftarrow b'_{17},$
$D'_{20} \leftarrow d_2, b'_{20} \leftarrow b_2, Q''_{20} \leftarrow q_2\}$ $(129, 140)$

$b :\ b'_{17} = \mathsf{SBit} \to b_2 = \mathsf{SBit}$ [139]

$b :\ \neg(b'_{17} = \mathsf{SBit})$ [141]

$\square$ $b :\ \mathsf{SQ} = \mathsf{msg}(d_{19}^1, b_9)|q_{19}^1$ [135]
$b :\ \mathsf{SQ} = \mathsf{msg}(d'_{17}, b'_{17})|\mathsf{msg}(d_2, b_2)|q_2$ [129]

$\to\ b_9 = b'_{17}$

$b :\ \neg(b'_{17} = \mathsf{SBit})$ [141]
$b :\ b_9 = \mathsf{SBit}$ [100]

$\to\ b_9 \neq b'_{17}$

$b :\ b_2 = \mathsf{SBit}$ [142]

$\square$ $b :\ b_2 = \mathsf{SBit}$ [142]
$b :\ b_9 = \mathsf{SBit}$ [100]

$\to\ b_2 = b_9$

$a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]
$a :\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [90]

$\to\ b_1 = b_9$

$a :\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]
$a :\ \mathsf{SQ} = \mathsf{msg}(d_2, b_2)|q_2$ [47]

$\to\ b_1 \neq b_2$

$\{D_1^1 \leftarrow d_2, Q_1^1 \leftarrow q_2\}$

⋮

von [147] (S. 39):

$p : [0, \{A\}, b, \circ, a, \emptyset, \infty]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [90]

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1)$ [111]

$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_9)$ [112]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{21}, b_{21})$ [143]

$b:\ \mathsf{SQ} = q_{22}$ [145]

$a:\ \mathsf{SQ} = q_{22}|\mathsf{msg}(\lambda, b_{21})$ [146]

aus [111]:

$b:\ \mathsf{SQ} = \varepsilon$ [148]

Quittieren einer Nachricht: Ind.Vor. A1, Teil 3:

aus [112]:

$b:\ \mathsf{RIM} = \bot$ [150]

□ (E3, 143, 150)

$b:\ \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_9)$ [151]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{24}^2, b_9)$ [152]

□ $b:\ \mathsf{SQ} = \varepsilon$ [148]

$b:\ \mathsf{SQ} = q_{22}$ [145]

$a:\ \mathsf{SQ} = q_{22}|\mathsf{msg}(\lambda, b_{21})$ [146]

$\rightarrow\ a:\ \mathsf{SQ} = \mathsf{msg}(\lambda, b_{21})$

$a:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]

$\rightarrow\ b_1 \neq b_{21}$

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{24}^2, b_9)$ [152]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{21}, b_{21})$ [143]

$\rightarrow\ b_{21} = b_9$

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [90]

$\rightarrow\ b_1 = b_9$

$\{D_1^1 \leftarrow \lambda, Q_1^1 \leftarrow \varepsilon\}$

$b:\ \exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1$ [149]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{23}^1, b_9)|q_{23}^1$ [153]

□ $b:\ \mathsf{SQ} = \mathsf{msg}(d_{23}^1, b_9)|q_{23}^1$ [153]

$b:\ \mathsf{SQ} = q_{22}$ [145]

$a:\ \mathsf{SQ} = q_{22}|\mathsf{msg}(\lambda, b_{21})$ [146]

$\rightarrow\ a:\ SQ = \mathsf{msg}(d_{23}^1, b_9)|q_{23}^1|\mathsf{msg}(\lambda, b_{21})$

$a:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_1^1, b_1)|Q_1^1)$ [41]

$\rightarrow\ b_1 \neq b_9$

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_9)$ [90]

$\rightarrow\ b_1 = b_9$

$\{D_1^1 \leftarrow d_{23}^1, Q_1^1 \leftarrow q_{23}^1|\mathsf{msg}(\lambda, b_{21})\}$

Damit ist die erste Teilaussage von A1 abgeschlossen.

5.2 1. Teilaussage, 2. Teil

Es folgt – anschließend bei Knoten [38] – die zweite Teilaussage.

Beweisskizze:

Situation:
$\mathsf{SIM}_a \neq \perp$, $\mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{SBit}_a$, $\mathsf{RIM}_a \neq \perp$, $\mathsf{Bit}(\mathsf{RIM}_a) \neq \mathsf{SBit}_a$.

Wieder wird versucht, die Induktionsvoraussetzung A1 zu verwenden:

Dabei ergibt sich zuerst der Fall $\mathsf{SIM}_b = \perp$ ([48]), wobei man eine ähnliche Situation wie in [51] der vorhergehenden Teilaussage hat:

Daraus kann man schließen, daß $\mathsf{SendCom}$ angewendet wurde.
Also ist SQ_b nicht leer und die erste Nachricht wird in SIM_a abgelegt. Damit ist $\mathsf{SBit}_a = \mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b))$.

Ist $\mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b)) \neq \mathsf{SBit}_b$, so wäre $\mathsf{SBit}_a = \mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b)) \neq \mathsf{SBit}_b$ – also SBit verändert worden. Dies könnte nur durch $\mathsf{ProcAck}$ geschehen sein, aber diese Regel ist in b nicht anwendbar.

Also ist $\mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b)) = \mathsf{SBit}_b$, und damit sind nach Induktionsvoraussetzung A2 alle weiteren Kontrollbits – insbesondere das der letzten Nachricht – in SQ_b auch gleich SBit_b, woraus man mit A3 erhält, daß ([86]) RIM_b leer oder $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{SBit}_b$ und RQ_b leer oder $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$ ist $\quad (*)$.
Ist RIM_b nicht leer, so ist $\mathsf{RIM}_a = \mathsf{RIM}_b$ (die RIM verändernden Aktionen RecCom und AckMsg können im betreffenden Schritt nicht angewendet worden sein). Damit ist $\mathsf{SBit}_a = \mathsf{SBit}_b = \mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{Bit}(\mathsf{RIM}_a)$.
Ist RIM_b leer, so muß in dem betreffenden Schritt RecCom angewendet worden sein und RIM_a enthält die erste Nachricht aus RQ_b. Womit wieder $\mathsf{SBit}_a = \mathsf{SBit}_b = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{Bit}(\mathsf{RIM}_a)$ folgt.

Damit ist also $\mathsf{SIM}_b \neq \perp$. Wie in der ersten Teilaussage stellt man fest, daß $\mathsf{SIM}_a = \mathsf{SIM}_b$ ist.

Für $\mathsf{Bit}(\mathsf{SIM}_b) \neq \mathsf{SBit}_b$ ([130]) ergibt sich sofort derselbe Widerspruch wie in [99] der ersten Teilaussage.

Situation in [131]-[134]:
Wegen $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$, ergibt die Induktionsvoraussetzung A1 für b die Aussage, daß RIM_b leer oder $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{SBit}_b$ und RQ_b leer oder $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$ ist.
Dies ist genau die oben mit $(*)$ bezeichnete Aussage.
Vergewissert man sich, daß im Abschluß des entsprechenden bei [86] beginnenden Zweiges von der Tatsache $\mathsf{SIM}_b = \perp$ kein Gebrauch gemacht wurde (was ganz einfach ist, da auf jeder Seite nur die explizit zitierten Formeln verwendet werden), so kann man das abschließende Tableau einfach übernehmen.

$$\vdots$$

von [38] (S. 32):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :\ b_1 = \mathsf{SBit}$ [35]

$a :\ \neg((\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_1)) \wedge$ [38]
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_1) | Q^3)))$

$a :\ \neg(\mathsf{RIM} = \bot)$ [39]

$a :\ \neg(\exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_1))$ [40]

$\boxed{a :\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1))\quad [43]}$

$a :\ \neg(\mathsf{RQ} = \varepsilon)$ [41]

$a :\ \neg(\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_1) | Q^3))$ [42]

$\hookrightarrow$ S. 51

aus F2R:

$a :\ \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B)$ [44]

$\boxed{a :\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)\quad [45]}$

"passende" Induktionsvoraussetzung A1 anwenden:

$b :\ A1$ [13] :

$b :\ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow$ [46]
$(B = \mathsf{SBit} \rightarrow\ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B) | Q^1)) \wedge$
$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B) | Q^3))))$

$b :\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_3)) \rightarrow (B_3 = \mathsf{SBit} \rightarrow (\ \ldots\ ))$ [47]

$b :\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_3))$ [48]

$b :\ \neg(\mathsf{SIM} = \mathsf{msg}(D_3, B_3))$ [51]

$\hookrightarrow$ S. 44

B_3 einsetzen:

LG : $b :\ \exists D : \mathsf{SIM} = \mathsf{msg}(D, b_4)$ [49]

$b :\ (b_4 = \mathsf{SBit} \rightarrow$ [50]
$((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_4) | Q^1)) \wedge$
$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_4)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_4) | Q^3))))$

$\boxed{b :\ \mathsf{SIM} = \mathsf{msg}(d_{15}, b_4)\quad [118]}$

$\hookrightarrow$ S. 49

$\vdots$

von [51] (S. 43):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :$ $\mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :$ $b_1 = \mathsf{SBit}$ [35]

$a :$ $\neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1))$ [43]

$a :$ $\mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [45]

$b :$ $\neg(\mathsf{SIM} = \mathsf{msg}(D_3, B_3))$ [51]

aus F2S: $b :$ $\mathsf{SIM} = \bot \vee \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)$ [52]

$\boxed{b : \mathsf{SIM} = \bot \quad [53]}$

$b :$ $\exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)$ [54]

$b :$ $\mathsf{SIM} = \mathsf{msg}(d_4, b_4)$ [117]

$\Box$ $\{D_3 \leftarrow d_4, B_3 \leftarrow b_4\}(51, 117)$

aus SIM: $b :$ $\forall M : \mathsf{SIM} = M \rightarrow \mathsf{A}(\mathsf{SIM} = M \text{ unless}^+ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})$ [55]

mit Tab. 0.11, $\{M \leftarrow \bot\}$ aus [53]:

$a :$ $\mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true}$ [56]

$a :$ $\mathsf{SIM} = \bot$ [57]

$\Box$ (E3, 34, 57)

$a :$ $\mathsf{SendCom} = \mathsf{true}$ [58]

aus Tab. 0.1:

$b :$ $\mathsf{SIM} = \bot$ [60]

$b :$ $\mathsf{SQ} = \mathsf{msg}(d_6, b_6)|q_6$ [61]

$a :$ $\mathsf{SQ} = q_6$ [62]

$\boxed{a : \mathsf{SIM} = \mathsf{msg}(d_6, b_6) \quad [63]}$

$a :$ $\mathsf{ClMsg} = \mathsf{true}$ [59]

aus Tab. 0.8:

$a :$ $\mathsf{SIM} = \bot$ [116]

$\Box$ (E3, 34, 116)

A6 (Folgerung aus A2) anwenden:

$b :$ $\forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \rightarrow (B = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B)))$ [64]

$b :$ $(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_7)|Q) \rightarrow (B_7 = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B_7)))$ [65]

$b :$ $\neg(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_7)|Q)$ [66]

$b :$ $\neg(\mathsf{SQ} = \mathsf{msg}(D_7, B_7)|Q_7)$ [68]

$\Box$ $\{D_7 \leftarrow d_6, B_7 \leftarrow b_6, Q_7 \leftarrow q_6\}(61, 68)$

$b :$ $b_6 = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', b_6))$ [67]

$\hookrightarrow$ S. 45

$\vdots$

von [67] (S. 44):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ b_1 = \mathsf{SBit}$ [35]

$a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1))$ [43]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [45]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_6, b_6)|q_6$ [61]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_6, b_6)$ [63]

$b:\ b_6 = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', b_6))$ [67]

Linker Zweig:

$b:\ \neg(b_6 = \mathsf{SBit})$ [69]

aus EA: $b:\ \exists B : \mathsf{SBit} = B$ [72]

$b:\ \mathsf{SBit} = b_5$ [73]

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [74]

mit Tab. 0.11, $\{B \leftarrow b_5\}$:

- $a:\ \mathsf{ProcAck} = \mathsf{true}$ [75]

  mit Tab. 0.7:

  $b:\ \mathsf{SIM} = \mathsf{msg}(d_8, b_5)$ [77]

  $\Box$ (E3, 53, 77)

- $a:\ \mathsf{SBit} = b_5$ [76]

  $\Box$ $a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]
  $a:\ \mathsf{SIM} = \mathsf{msg}(d_6, b_6)$ [63]

  $\rightarrow\ b_1 = b_6$

  $a:\ b_1 = \mathsf{SBit}$ [35]
  $a:\ \mathsf{SBit} = b_5$ [76]

  $\rightarrow\ b_1 = b_5$

  $b:\ \mathsf{SBit} = b_5$ [73]
  $b:\ \neg(b_6 = \mathsf{SBit})$ [69]

  $\rightarrow\ b_5 \neq b_6$

Rechter Zweig:

$\boxed{\text{LG}:\ b:\ b_6 = \mathsf{SBit}\ \ [70]}$

$b:\ \exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', b_6))$ [71]

$b:\ \mathsf{SQ} = q_7'|\mathsf{msg}(d_7', b_6))$ [78]

$\hookrightarrow$ S. 46

$$\vdots$$

von [78] (S. 45):

$$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$
$$a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]$$
$$a :\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1)) \quad [43]$$
$$a :\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2) \quad [45]$$
$$a :\ \mathsf{SIM} = \mathsf{msg}(d_6, b_6) \quad [63]$$
$$b :\ b_6 = \mathsf{SBit} \quad [70]$$
$$b :\ \mathsf{SQ} = q_7' | \mathsf{msg}(d_7', b_6)) \quad [78]$$

Induktionsvorauss. A3:

$$b :\ \forall B : (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \rightarrow \quad [79]$$
$$(B = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q''))))$$

$$b :\ (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_9)) \rightarrow \quad [80]$$
$$(B_9 = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B_9)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B_9)|Q''))))$$

$$b :\ \neg(\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_9)) \quad [81]$$
$$b :\ \neg(\mathsf{SQ} = Q_9|\mathsf{msg}(D_9, B_9)) \quad [83]$$
$$\Box\ \{Q_9 \leftarrow q_7', D_9 \leftarrow d_7', B_9 \leftarrow b_6\}(78, 83)$$

$$b :\ (b_6 = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_6)) \wedge \quad [82]$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_6)|Q'')))$$

$$b :\ \neg(b_6 = \mathsf{SBit}) \quad [84]$$
$$\Box\ (70, 84)$$

$$b :\ \mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_6) \quad [85]$$
$$b :\ \mathsf{RQ} = \varepsilon \vee \exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_6)|Q'' \quad [86]$$

$\hookrightarrow$ S. 47

$\vdots$

von [86] (S. 46):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1))$ [43]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [45]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_6, b_6)$ [63]

$b:\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_6)$ [85]

$b:\ \mathsf{RQ} = \varepsilon \vee \exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_6)|Q''$ [86]

$b:\ \mathsf{RIM} = \bot$ [87]

$|$

$b:\ \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_6)$ [88]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_9', b_6)$ [104]

$\hookrightarrow$ S. 48

$b:\ \forall M : \mathsf{RIM} = M \rightarrow \mathsf{A}(\mathsf{RIM} = M\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [89]

mit Tab. 0.11, $\{M \leftarrow \bot\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [90]

$a:\ \mathsf{RIM} = \bot$ [91]

$\square\ (E3, 45, 91)$

$a:\ \mathsf{RecCom} = \mathsf{true}$ [92]

aus Tab. 0.1:

$b:\ \mathsf{RIM} = \bot$ [94]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{10}, b_{10})|q_{10}$ [95]

$a:\ \mathsf{RQ} = q_{10}$ [96]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_{10}, b_{10})$ [97]

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [93]

aus Tab. 0.8:

$a:\ \mathsf{RIM} = \bot$ [102]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{12}, b_{12})$ [103]

$\square$ (E3, 87, 103)

aus [86]:

$b:\ \mathsf{RQ} = \varepsilon$ [98]

$\square\ (95, 98)$

$b:\ \exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_6)|Q''$ [99]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{11}'', b_6)|q_{11}''$ [100]

$\square$

$$\frac{a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)\ [34] \qquad a:\ \mathsf{SIM} = \mathsf{msg}(d_6, b_6)\ [63]}{\rightarrow\ b_1 = b_6}$$

$$\frac{b:\ \mathsf{RQ} = \mathsf{msg}(d_{11}'', b_6)|q_{11}''\ [100] \qquad b:\ \mathsf{RQ} = \mathsf{msg}(d_{10}, b_{10})|q_{10}\ [95]}{\rightarrow\ b_6 = b_{10}}$$

$$\frac{a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1))\ [43] \qquad a:\ \mathsf{RIM} = \mathsf{msg}(d_{10}, b_{10})\ [97]}{\rightarrow\ b_1 \neq b_{10}}$$

$\{D_1^2 \leftarrow d_{10}\}$

$\vdots$

von [104] (S. 47):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1))$ [43]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [45]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_6, b_6)$ [63]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_9', b_6)$ [104]

aus RIM: $b:\ \forall M : \mathsf{RIM} = M \rightarrow \mathsf{A}(\mathsf{RIM} = M\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [105]

mit Tab. 0.11, $\{M \leftarrow \mathsf{msg}(d_9', b_6)\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [106]

$a:\ \mathsf{RecCom} = \mathsf{true}$ [108]

aus Tab. 0.1:

$b:\ \mathsf{RIM} = \bot$ [110]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{13}, b_{13})|q_{13}$ [111]

$a:\ \mathsf{RQ} = q_{13}$ [112]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_{13}, b_{13})$ [113]

$\Box$ (E3, 104, 110)

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [109]

aus Tab. 0.8:

$a:\ \mathsf{RIM} = \bot$ [114]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{14}, b_{14})$ [115]

$\Box$ (E3, 45, 114)

$a:\ \mathsf{RIM} = \mathsf{msg}(d_9', b_6)$ [108]

$\Box$ $a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_6, b_6)$ [63]

$\rightarrow\ b_1 = b_6$

$a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1))$ [43]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_9', b_6)$ [108]

$\rightarrow\ b_1 \neq b_6$

$\{D_1^2 \leftarrow d_9'\}$

$\vdots$

von [50]/[118] (S. 43):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :$ $\mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :$ $b_1 = \mathsf{SBit}$ [35]

$a :$ $\neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1))$ [43]

$a :$ $\mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [45]

$b :$ $\mathsf{SIM} = \mathsf{msg}(d_{15}, b_4)$ [118]

aus SIM: $b :$ $\forall M : \mathsf{SIM} = M \rightarrow \mathsf{A}(\mathsf{SIM} = M \text{ unless}^+ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true})$ [119]

mit Tab. 0.11, $\{M \leftarrow \mathsf{msg}(d_{15}, b_4)\}$ aus [118]:

$a :$ $\mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true}$ [120]

$a :$ $\mathsf{SendCom} = \mathsf{true}$ [122]

aus Tab. 0.1:

$b :$ $\mathsf{SIM} = \bot$ [124]

$b :$ $\mathsf{SQ} = \mathsf{msg}(d_{16}, b_{16})|q_{16}$ [125]

$a :$ $\mathsf{SQ} = q_{16}$ [126]

$a :$ $\mathsf{SIM} = \mathsf{msg}(d_{16}, b_{16})$ [127]

$\square$ (E3, 50, 124)

$a :$ $\mathsf{CIMsg} = \mathsf{true}$ [123]

aus Tab. 0.8:

$a :$ $\mathsf{SIM} = \bot$ [128]

$b :$ $\mathsf{SIM} = \mathsf{msg}(d_{17}, b_{17})$ [129]

$\square$ (E3, 34, 128)

$a :$ $\mathsf{SIM} = \mathsf{msg}(d_{15}, b_4)$ [121]

aus [50]:

$b :$ $\neg(b_4 = \mathsf{SBit})$ [130]

wie [99] der ersten Teilaussage, mit
$a :$ $\mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]
$a :$ $b_1 = \mathsf{SBit}$ [35]
$b :$ $\mathsf{SIM} = \mathsf{msg}(d_{15}, b_4)$ [50]
$a :$ $\mathsf{SIM} = \mathsf{msg}(d_{15}, b_4)$ [121]
$b :$ $\neg(b_4 = \mathsf{SBit})$ [130]

LG : $b :$ $b_4 = \mathsf{SBit}$ [131]

$b :$ $\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_4)|Q^1)$ [132]

$b :$ $\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_4))$ [133]

$b :$ $\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_4)|Q^3)))$ [134]

wie [86] ff. mit
$a :$ $\mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]
$a :$ $\neg(\mathsf{RIM} = \mathsf{msg}(D_1^2, b_1))$ [43]
$a :$ $\mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [45]
$a :$ $\mathsf{SIM} = \mathsf{msg}(d_{15}, b_4)$ [121]
$b :$ $\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_4))$ [133]
$b :$ $\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_4)|Q^3)))$ [134]

Damit ist auch die zweite Teilaussage von A1 bewiesen.

5.3 1. Teilaussage, 3. Teil

Es folgt nach bewährtem Muster anschließend an Knoten [41] und [42], die Indizes ebenfalls wieder mit 1 beginnend, der Beweis der 3. Teilaussage:

Situation:
$\mathsf{SIM}_a \neq \perp$, $\mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{SBit}_a$, $\mathsf{RIM}_a \neq \perp$, $\mathsf{Bit}(\mathsf{RIM}_a) \neq \mathsf{SBit}_a$.

Wieder wird versucht, die Induktionsvoraussetzung A1 zu verwenden:

Dabei ergibt sich zuerst der Fall $\mathsf{SIM}_b = \perp$ ([50]), wobei man eine ähnliche Situation wie in [51] der ersten Teilaussage hat. Wieder ist also im betrachteten Schritt daß SendCom angewendet worden.
Also ist SQ_b nicht leer und die erste Nachricht wird in SIM_a abgelegt. Damit ist $\mathsf{SBit}_a = \mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b))$.

Als weiteres stellt man fest, daß ProcAck nicht angewendet worden ist, es gilt also $\mathsf{SBit}_a = \mathsf{SBit}_b$.

Damit sind nach Induktionsvoraussetzung A2 alle weiteren Kontrollbits – insbesondere das der letzten Nachricht – in SQ_b auch gleich SBit_b.
Für RQ erhält man mit A3 die folgenden Aussage:
„Falls RQ_b nicht leer ist, gilt $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$" $(**)$.
In jedem Fall müssen die Auswirkungen auf RQ_a unter Berücksichtigung der RQ verändernden Regeln untersucht werden: Dabei ist zu beachten, daß vorausgesetzt wurde, daß keine zwei RQ verändernden Regeln gleichzeitig angewendet werden.
Falls RQ_b nicht leer ist:
RecCom: Die in RQ_b zweite Nachricht rückt – falls sie existiert – an erste Stelle. Nach A5 hat diese das gleiche Kontrollbit wie die erste: $\mathsf{SBit}_b = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a)) \neq \mathsf{SBit}_a$. Folglich hat sich SBit durch Anwendung von ProcAck geändert, was wiederum unmöglich ist, da ProcAck als Nachbedingung $\mathsf{SIM} = \perp$ hat.
RLose: Im Prinzip wie RecCom. Entweder bleibt die erste Nachricht erhalten, oder die zweite rückt an ihre Stelle.
ReTrans und ProcAck oder keine der Regeln: Die erste Nachricht bleibt in beiden Fällen erhalten. Im übrigen wurde für festgestellt, daß ProcAck nicht angewendet wurde.
Falls RQ_b leer ist:
ProcAck ist nicht anwendbar. Für ReTrans ergibt sich folgendes Bild: ReTrans hängt eine Nachricht mit Kontrollbit SBit_b an RQ an. Man erhält also wieder $\mathsf{SBit}_b = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a)) \neq \mathsf{SBit}_a$.
Da ProcAck nicht anwendbar ist, ergibt sich wieder ein Widerspruch.

Damit ist also $\mathsf{SIM}_b \neq \perp$. Wie in der ersten Teilaussage stellt man fest, daß $\mathsf{SIM}_a = \mathsf{SIM}_b$ ist.

Für $\mathsf{Bit}(\mathsf{SIM}_b) \neq \mathsf{SBit}_b$ ergibt sich sofort derselbe Widerspruch wie in [99] der ersten Teilaussage.

Bleibt der Fall zu betrachten, daß in a und in b $\mathsf{Bit}(\mathsf{SIM}) = \mathsf{SBit}$ gilt, man also in b aus A1 die Aussage
„Falls RQ_b nicht leer ist, gilt $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$."
erhält. Dies ist genau die oben mit $(**)$ bezeichnete Aussage.

Vergewissert man sich, daß im Abschluß des entsprechenden Zweiges von der Tatsache $\mathsf{SIM}_b = \bot$ kein Gebrauch gemacht wurde, so kann man das Tableau einfach übernehmen.

$$\vdots$$

von [41]/[42] (S. 43):

$$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$
$$a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]$$
$$a :\ b_1 = \mathsf{SBit} \quad [35]$$
$$|$$
$$a :\ \neg(\mathsf{RQ} = \varepsilon) \quad [41]$$
$$a :\ \neg(\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_1)|Q^3)) \quad [42]$$
$$|$$
$$\boxed{a :\ \neg(\mathsf{RQ} = \mathsf{msg}(D^3_1, b_1)|Q^3_1) \quad [43]}$$
$$|$$

aus F1R:

$$a :\ \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q \quad [44]$$
$$a :\ \exists D', B', Q' : \mathsf{RQ} = Q'|\mathsf{msg}(D', B') \quad [45]$$
$$\boxed{\begin{array}{l} a :\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [46] \\ a :\ \mathsf{RQ} = q'_2|\mathsf{msg}(d'_2, b'_2) \quad [47] \end{array}}$$
$$|$$

"passende" Induktionsvoraussetzung A1 anwenden:

$$b :\ A1 \quad [13] :$$
$$\begin{array}{ll} b :\ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \to & [48] \\ \quad (B = \mathsf{SBit} \to \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge & \\ \quad\quad (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge & \\ \quad\quad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) & \end{array}$$
$$|$$
$$b :\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_3)) \to (B_3 = \mathsf{SBit} \to (\ \ldots\ )) \quad [49]$$

Linker Zweig:

$$b :\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_3)) \quad [50]$$
$$b :\ \neg(\mathsf{SIM} = \mathsf{msg}(D_3, B_3)) \quad [53]$$

$\hookrightarrow$ S. 52

Rechter Zweig:

B_3 einsetzen:

$$\mathrm{LG} :\ b :\ \exists D : \mathsf{SIM} = \mathsf{msg}(D, b_4) \quad [51]$$
$$|$$
$$\begin{array}{ll} b :\ (B = \mathsf{SBit} \to & [52] \\ \quad ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge & \\ \quad (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge & \\ \quad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) & \end{array}$$
$$|$$
$$\boxed{b :\ \mathsf{SIM} = \mathsf{msg}(d_{16}, b_4) \quad [142]}$$

$\hookrightarrow$ S. 60

$\vdots$

von [53] (S. 51):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:$ $\mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:$ $b_1 = \mathsf{SBit}$ [35]

$a:$ $\neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]

$a:$ $\mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]

$b:$ $\neg(\mathsf{SIM} = \mathsf{msg}(D_3, B_3))$ [53]

aus F2S: $b:$ $\mathsf{SIM} = \bot \vee \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)$ [54]

$\boxed{b:\ \mathsf{SIM} = \bot \quad [55]}$

aus EA: $b:$ $\exists B : \mathsf{SBit} = B$ [57]

$\boxed{b:\ \mathsf{SBit} = b_5 \quad [58]}$

$b:$ $\exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)$ [56]

$b:$ $\mathsf{SIM} = \mathsf{msg}(d_4, b_4)$ [141]

$\Box$ $\{D_3 \leftarrow d_4, B_3 \leftarrow b_4\}(53, 141)$

aus SBit: $b:$ $\forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \text{ unless}^+ \mathsf{ProcAck} = \mathsf{true})$ [59]

mit Tab. 0.11, $\{B \leftarrow b_5\}$:

$a:$ $\mathsf{ProcAck} = \mathsf{true}$ [60]

mit Tab. 0.7:

$b:$ $\mathsf{SIM} = \mathsf{msg}(d_6, b_5)$ [63]

$\Box$ (E3, 55, 63)

$\boxed{\begin{array}{c} a:\ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [61] \\ a:\ \mathsf{SBit} = b_5 \quad [62] \end{array}}$

aus SIM: $b:$ $\forall M : \mathsf{SIM} = M \rightarrow \mathsf{A}(\mathsf{SIM} = M \text{ unless}^+ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true})$ [64]

mit Tab. 0.11, $\{M \leftarrow \bot\}$:

$a:$ $\mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true}$ [65]

$a:$ $\mathsf{SendCom} = \mathsf{true}$ [67]

aus Tab. 0.1:

$b:$ $\mathsf{SIM} = \bot$ [69]

$b:$ $\mathsf{SQ} = \mathsf{msg}(d_7, b_7)|q_7$ [70]

$a:$ $\mathsf{SQ} = q_7$ [71]

$\boxed{a:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7) \quad [72]}$

$\hookrightarrow$ S. 53

$a:$ $\mathsf{CIMsg} = \mathsf{true}$ [68]

aus Tab. 0.8:

$a:$ $\mathsf{SIM} = \bot$ [140]

$\Box$ (E3, 34, 140)

$a:$ $\mathsf{SIM} = \bot$ [66]

$\Box$ (E3, 34, 66)

$\vdots$

von [72] (S. 52):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :$ $\mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :$ $b_1 = \mathsf{SBit}$ [35]

$a :$ $\neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]

$a :$ $\mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]

$b :$ $\mathsf{SBit} = b_5$ [58]

$a :$ $\neg(\mathsf{ProcAck} = \mathsf{true})$ [61]

$a :$ $\mathsf{SBit} = b_5$ [62]

$a :$ $\mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [72]

A6 (Folgerung aus A2) anwenden:

$b :$ $\forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \rightarrow (B = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B)))$ [73]

$b :$ $(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_8)|Q) \rightarrow (B_8 = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B_8)))$ [74]

$b :$ $\neg(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_6)|Q)$ [75]

$b :$ $\neg(\mathsf{SQ} = \mathsf{msg}(D_6, B_6)|Q_6)$ [77]

$\Box$ $\{D_8 \leftarrow d_7, B_8 \leftarrow b_7, Q_8 \leftarrow q_7\}(69, 77)$

$b :$ $b_7 = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', b_7))$ [76]

$b :$ $\neg(b_7 = \mathsf{SBit})$ [78]

$\Box$ $a :$ $\mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :$ $\mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [72]

$\rightarrow$ $b_1 = b_7$

$a :$ $b_1 = \mathsf{SBit}$ [35]

$a :$ $\mathsf{SBit} = b_5$ [62]

$\rightarrow$ $b_1 = b_5$

$b :$ $\mathsf{SBit} = b_5$ [58]

$b :$ $\neg(b_7 = \mathsf{SBit})$ [78]

$\rightarrow$ $b_5 \neq b_7$

$\boxed{\text{LG} : b : b_7 = \mathsf{SBit} \quad [79]}$

$b :$ $\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', b_7)$ [80]

$b :$ $\mathsf{SQ} = q_8'|\mathsf{msg}(d_8', b_7)$ [81]

$\hookrightarrow$ S. 54

$\vdots$

von [81] (S. 53):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :\ b_1 = \mathsf{SBit}$ [35]

$a :\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]

$a :\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]

$b :\ \mathsf{SBit} = b_5$ [58]

$a :\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [61]

$a :\ \mathsf{SBit} = b_5$ [62]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [72]

$b :\ b_7 = \mathsf{SBit}$ [79]

$b :\ \mathsf{SQ} = q_8'|\mathsf{msg}(d_8', b_7))$ [81]

Induktionsvorauss. A3:

$$b :\ \forall B : (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \to \quad [82]$$
$$(B = \mathsf{SBit} \to \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q''))))$$

$$b :\ (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_9)) \to \quad [83]$$
$$(B_9 = \mathsf{SBit} \to \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B_9)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B_9)|Q''))))$$

$b :\ \neg(\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_9))$ [84]

$b :\ \neg(\mathsf{SQ} = Q_9|\mathsf{msg}(D_9, B_9))$ [86]

$\square\ \{Q_9 \leftarrow q_8', D_9 \leftarrow d_8', B_9 \leftarrow b_7\}(81, 86)$

$$b :\ (b_7 = \mathsf{SBit} \to \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_7)) \wedge \quad [85]$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_7)|Q'')))$$

$b :\ \neg(b_7 = \mathsf{SBit})$ [87]

$\square\ (78, 86)$

$b :\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_7)$ [88]

$b :\ \mathsf{RQ} = \varepsilon \vee \exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_7)|Q''$ [89]

$\hookrightarrow$ S. 55

$\vdots$

von [89] (S. 54):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a :\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1) | Q_1^3)$ [43]

$a :\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2) | q_2$ [46]

$a :\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [61]

$a :\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [72]

$b :\ b_7 = \mathsf{SBit}$ [79]

$b :\ \mathsf{RQ} = \varepsilon \vee \exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_7) | Q''$ [89]

$b :\ \mathsf{RQ} = \varepsilon$ [90]

$b :\ \exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_7) | Q''$ [91]

$b :\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7) | q_9''$ [106]

$\hookrightarrow$ S. 56

aus RQ:

$b :\ \forall Q : \mathsf{RQ} = Q \rightarrow \mathsf{A}(\mathsf{RQ} = Q\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [92]

mit Tab. 0.11, $\{Q \leftarrow \varepsilon\}$:

$a :\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}$ [93]

$a :\ \mathsf{RQ} = \varepsilon$ [94]

$\Box$ (E2, 46, 94)

$a :\ \mathsf{RecCom} = \mathsf{true}$ [95]

aus Tab. 0.2:

$b :\ \mathsf{RIM} = \bot$ [99]

$b :\ \mathsf{RQ} = \mathsf{msg}(d_{10}, b_{10}) | q_{10}$ [100]

$\Box$ (E2, 90, 100)

$a :\ \mathsf{ProcAck} = \mathsf{true}$ [98]

$\Box$ (61, 98)

$a :\ \mathsf{RLose} = \mathsf{true}$ [96]

aus Tab. 0.4:

$b :\ \mathsf{RQ} \neq \varepsilon$ [101]

$\Box$ (90, 101)

$a :\ \mathsf{ReTrans} = \mathsf{true}$ [97]

aus Tab. 0.6:

$b :\ \mathsf{RQ} = q_{11}$ [102]

$b :\ \mathsf{SNo} = n_{11}$ [103]

$b :\ \mathsf{SBit} = b_{11}$ [104]

$a :\ \mathsf{RQ} = q_{11} | \mathsf{msg}(\mathsf{SFile}(n_{11}), b_{11})$ [105]

$\Box$

$$\frac{a :\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)\ [34] \qquad a :\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)\ [72]}{\rightarrow\ b_1 = b_7} \qquad \frac{b :\ b_7 = \mathsf{SBit}\ [79] \qquad b :\ \mathsf{SBit} = b_{11}\ [104]}{\rightarrow\ b_7 = b_{11}}$$

$$\frac{b :\ \mathsf{RQ} = \varepsilon\ [90] \qquad b :\ \mathsf{RQ} = q_{11}\ [102]}{\rightarrow\ q_{11} = \varepsilon} \qquad \frac{a :\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1) | Q_1^3)\ [43] \qquad a :\ \mathsf{RQ} = q_{11} | \mathsf{msg}(\mathsf{SFile}(n_{11}), b_{11})\ [105]}{\rightarrow\ b_1 \neq b_{11}}$$

$\Box\ \{D_1^3 \leftarrow \mathsf{SFile}(n_{11}),\ Q_1^3 \leftarrow q_{11}\}(43, 105)$

$\vdots$

von [106] (S. 55):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ b_1 = \mathsf{SBit}$ [35]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [61]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [72]

$b:\ b_7 = \mathsf{SBit}$ [79]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9''$ [106]

$b:\ \forall Q : \mathsf{RQ} = Q \rightarrow \mathsf{A}(\mathsf{RQ} = Q \text{ unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [107]

mit Tab. 0.11, $\{Q \leftarrow \mathsf{msg}(d_9'', b_7)|q_9''\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}$ [108]

- $a:\ \mathsf{RecCom} = \mathsf{true}$ [110] $\hookrightarrow$ S. 57
- $a:\ \mathsf{RLose} = \mathsf{true}$ [111] $\hookrightarrow$ S. 58
- $a:\ \mathsf{ReTrans} = \mathsf{true}$ [112]

  aus Tab. 0.6:

  $b:\ \mathsf{RQ} = q_{16}$ [136]

  $b:\ \mathsf{SNo} = n_{16}$ [137]

  $b:\ \mathsf{SBit} = b_{16}$ [138]

  $a:\ \mathsf{RQ} = q_{16}|\mathsf{msg}(\mathsf{SFile}(n_{16}), b_{16})$ [139]

$\square$ $b:\ \mathsf{RQ} = q_{16}$ [136] $b:\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9''$ [106] $a:\ \mathsf{RQ} = q_{16}|\mathsf{msg}(\mathsf{SFile}(n_{16}), b_{16})$ [139] ——— $\rightarrow\ a:\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9''|\mathsf{msg}(\mathsf{SFile}(n_{16}), b_{16})$ $a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43] ——— $\rightarrow\ b_1 \neq b_7$ $\{D_1^3 \leftarrow \mathsf{SFile}(n_{16}),\ Q_1^3 \leftarrow q_{16}\}$	$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34] $a:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [72] ——— $\rightarrow\ b_1 = b_7$

- $a:\ \mathsf{ProcAck} = \mathsf{true}$ [113]

  $\square$ (61, 113)

$a:\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9''$ [109]

$\square$ $a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34] $a:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [72] ——— $\rightarrow\ b_1 = b_7$ $a:\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9''$ [109] $a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43] ——— $\rightarrow\ b_1 \neq b_7$ $\{D_1^3 \leftarrow \mathsf{msg}(d_9'', b_7),\ Q_1^3 \leftarrow q_9''\}$

$\vdots$

von [110] (S. 56):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :\ b_1 = \mathsf{SBit}$ [35]

$a :\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]

$a :\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]

$b :\ b_7 = \mathsf{SBit}$ [79]

$b :\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9''$ [106]

$a :\ \mathsf{RecCom} = \mathsf{true}$ [110]

aus Tab. 0.2:

$b :\ \mathsf{RIM} = \perp$ [114]

$b :\ \mathsf{RQ} = \mathsf{msg}(d_{12}, b_{12})|q_{12}$ [115]

$a :\ \mathsf{RQ} = q_{12}$ [116]

$a :\ \mathsf{RIM} = \mathsf{msg}(d_{12}, b_{12})$ [117]

Ind.Vor. A5:

$b :\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \to (B = \mathsf{SBit} \to B' = \mathsf{SBit})$ [118]

$b :\ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{13})|Q'|\mathsf{msg}(D', B_{13}')|Q'') \to (B_{13} = \mathsf{SBit} \to B_{13}' = \mathsf{SBit})$ [119]

$b :\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{13})|Q'\mathsf{msg}(D', B_{13}')|Q'')$ [120]

$b :\ \neg(\mathsf{RQ} = Q_{13}|\mathsf{msg}(D_{13}, B_{13})|Q_{13}'\mathsf{msg}(D_{13}', B_{13}')|Q_{13}'')$ [122]

□ $a :\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]
$a :\ \mathsf{RQ} = q_{12}$ [116]
$b :\ \mathsf{RQ} = \mathsf{msg}(d_{12}, b_{12})|q_{12}$ [115]

$b :\ \mathsf{RQ} = \mathsf{msg}(d_{12}, b_{12})|\mathsf{msg}(d_2, b_2)|q_2$

$b :\ \neg(\mathsf{RQ} = Q_{13}|\mathsf{msg}(D_{13}, B_{13})|Q_{13}'|\ \mathsf{msg}(D_{13}', B_{13}')|Q_{13}''))$ [122]

$\{Q_{13}, Q_{13}' \leftarrow \varepsilon,\ D_{13} \leftarrow d_{12},\ B_{13} \leftarrow b_{12},\ D_{13}' \leftarrow d_2,\ B_{13}' \leftarrow b_2,\ Q_{13}'' \leftarrow q_2\}$

$B_{13},\ B_{13}'$ einsetzen:

$b :\ b_{12} = \mathsf{SBit} \to b_2 = \mathsf{SBit}$ [121]

$b :\ \neg(b_{12} = \mathsf{SBit})$ [123]

□ $b :\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9''$ [106]
$b :\ \mathsf{RQ} = \mathsf{msg}(d_{12}, b_{12})|q_{12}$ [115]

$\to\ b_7 = b_{12}$

$b :\ b_7 = \mathsf{SBit}$ [79]
$b :\ \neg(b_{12} = \mathsf{SBit})$ [123]

$\to\ b_7 \neq b_{12}$

$b :\ b_2 = \mathsf{SBit}$ [124]

□ $a :\ b_1 = \mathsf{SBit}$ [35]
$b :\ b_2 = \mathsf{SBit}$ [124]

$\to\ b_1 = b_2$

$a :\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]
$a :\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]

$\to\ b_1 \neq b_2$

$\vdots$

von [111] (S. 56):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ b_1 = \mathsf{SBit}$ [35]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [72]

$b:\ b_7 = \mathsf{SBit}$ [79]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9''$ [106]

$a:\ \mathsf{RLose} = \mathsf{true}$ [111]

|

mit Tab. 0.3:

$b:\ \mathsf{RQ} \neq \varepsilon$ [125]

Linker Zweig:

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_{14}, B_{14})|Q_{14}))$ [126]

$\Box\ \{D_{14} \leftarrow d_2,\ B_{14} \leftarrow b_2,\ Q_{14} \leftarrow q_2\}(46, 126)$

Rechter Zweig:

D_{14}, B_{14}, Q_{14} einsetzen:

|

$b:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_{14}'$ [127]

$\Box\ a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]
$a:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [72]
$\rightarrow\ b_1 = b_7$
$b:\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9''$ [106]
$b:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_{14}'$ [127]
$\rightarrow\ b_7 = b_2$
$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]
$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]
$\rightarrow\ b_1 \neq b_2$

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{14}', b_{14}')|\mathsf{msg}(d_2, b_2)|q_2$ [128]

$\hookrightarrow$ S. 59

$$\vdots$$

von [128] (S. 58):

$$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]$$
$$a:\ b_1 = \mathsf{SBit} \quad [35]$$
$$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3) \quad [43]$$
$$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [46]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7) \quad [72]$$
$$b:\ b_7 = \mathsf{SBit} \quad [79]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9'' \quad [106]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_{14}', b_{14}')|\mathsf{msg}(d_2, b_2)|q_2 \quad [128]$$

Ind.Vor. A5:

$$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}) \quad [129]$$
$$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{15})|Q'|\mathsf{msg}(D', B_{15}')|Q'') \rightarrow (B_{15} = \mathsf{SBit} \rightarrow B_{15}' = \mathsf{SBit}) \quad [130]$$

$$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{15})|Q'\mathsf{msg}(D', B_{15}')|Q'') \quad [131]$$
$$b:\ \neg(\mathsf{RQ} = Q_{15}|\mathsf{msg}(D_{15}, B_{15})|Q_{15}'\mathsf{msg}(D_{15}', B_{15}')|Q_{15}'') \quad [133]$$
$$\Box\ \{Q_{15}, Q_{15}' \leftarrow \varepsilon,\ D_{15} \leftarrow d_{14}',\ B_{15} \leftarrow b_{14}', D_{15}' \leftarrow d_2,\ B_{15}' \leftarrow b_2,\ Q_{15}'' \leftarrow q_2\}$$
$$(128, 133)$$

$B_{15},\ B_{15}'$ einsetzen:

$$b:\ b_{14}' = \mathsf{SBit} \rightarrow b_2 = \mathsf{SBit} \quad [132]$$

$$b:\ \neg(b_{14}' = \mathsf{SBit}) \quad [134]$$

$$\boxed{\begin{array}{l} \Box\ b:\ \mathsf{RQ} = \mathsf{msg}(d_9'', b_7)|q_9'' \quad [106] \\ \quad b:\ \mathsf{RQ} = \mathsf{msg}(d_{14}', b_{14}')|\mathsf{msg}(d_2, b_2)|q_2 \quad [134] \\ \hline \quad \rightarrow\ b_7 = b_{14}' \\ \quad b:\ b_7 = \mathsf{SBit} \quad [79] \\ \quad b:\ \neg(b_{14}' = \mathsf{SBit}) \quad [120] \\ \hline \quad \rightarrow\ b_7 \neq b_{14}' \end{array}}$$

$$b:\ b_2 = \mathsf{SBit} \quad [135]$$

$$\boxed{\begin{array}{l} \Box\ a:\ b_1 = \mathsf{SBit} \quad [35] \\ \quad b:\ b_2 = \mathsf{SBit} \quad [135] \\ \hline \quad \rightarrow\ b_1 = b_2 \\ \quad a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3) \quad [43] \\ \quad a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [46] \\ \hline \quad \rightarrow\ b_1 \neq b_2 \end{array}}$$

$\vdots$

von [52]/[142] (S. 51):

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ b_1 = \mathsf{SBit}$ [35]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{16}, b_4)$ [142]

aus SIM: $b:\ \forall M : \mathsf{SIM} = M \to \mathsf{A}(\mathsf{SIM} = M\ \mathsf{unless}^+\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true})$ [143]

mit Tab. 0.11, $\{M \leftarrow \mathsf{msg}(d_{16}, b_4)\}$:

$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true}$ [144]

$a:\ \mathsf{SendCom} = \mathsf{true}$ [146]

aus Tab. 0.1:

$b:\ \mathsf{SIM} = \bot$ [148]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{17}, b_{17})|q_{17}$ [149]

$a:\ \mathsf{SQ} = q_{17}$ [150]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_{17})$ [151]

$\square$ (E3, 50, 148)

$a:\ \mathsf{CIMsg} = \mathsf{true}$ [147]

aus Tab. 0.8:

$a:\ \mathsf{SIM} = \bot$ [152]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{18}, b_{18})$ [153]

$\square$ (E3, 34, 152)

$\boxed{a:\ \mathsf{SIM} = \mathsf{msg}(d_{16}, b_4)\quad [145]}$

[52] komplett auflösen:

$b:\ \neg(b_4 = \mathsf{SBit})$ [154]

wie [99] der 1.Teilaussage (S. 37) :

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ b_1 = \mathsf{SBit}$ [35]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{16}, b_4)$ [142]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{16}, b_4)$ [145]

$b:\ \neg(b_4 = \mathsf{SBit})$ [154]

$\boxed{\mathrm{LG}:\ b:\ b_4 = \mathsf{SBit}\quad [155]}$

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_4)|Q^1)$ [156]

$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_4)$ [157]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_4)|Q^3)$ [158]

bis auf ProcAck wie [89] ff. (S. 55) mit

$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1)$ [34]

$a:\ b_1 = \mathsf{SBit}$ [35]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3)$ [43]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [46]

$b:\ b_4 = \mathsf{SBit}$ [155]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{16}, b_4)$ [145]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_4)|Q^3)$ [158]

$\hookrightarrow$ S. 61

In diesem Fall hat man allerdings keinen Knoten $a:\ \neg(\mathsf{ProcAck} = \mathsf{true})$, da man in dieser Situation eine Anwendung von ProcAck nicht ausschließen kann. ProcAck bringt dennoch keine großen Neuigkeiten: An den entsprechenden Stellen angehängt, ergibt das folgende Tableau die gesuchten Abschlüsse:

$$\vdots$$

von [158] (S. 60):

$$p : [\,0, \{A\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]$$
$$a:\ b_1 = \mathsf{SBit} \quad [35]$$
$$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3) \quad [43]$$
$$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [46]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_{16}, b_4) \quad [145]$$
$$b:\ b_4 = \mathsf{SBit} \quad [155]$$
$$|$$
$$a:\ \mathsf{ProcAck} = \mathsf{true} \quad [\mathrm{V}]$$

aus Tab. 0.10:

$$b:\ \mathsf{SIM} = \mathsf{msg}(d_{20}, b_{20}) \quad [159]$$
$$b:\ \mathsf{SBit} = b_{20} \quad [160]$$
$$b:\ \mathsf{RQ} = q_{21} \quad [161]$$
$$b:\ \mathsf{SNo} = n_{21} \quad [162]$$

Linker Zweig:

$$a:\ (\mathsf{SFile}(s(n_{21})) = d_{22} \quad [169]$$
$$a:\ \mathsf{RQ} = q_{21}|\mathsf{msg}(\mathsf{SFile}(s(n_{21})), \mathsf{flip}(b_{20})) \quad [164]$$
$$a:\ \mathsf{SNo} = s(n_{21}) \quad [165]$$
$$a:\ \mathsf{SBit} = \mathsf{flip}(b_{20}) \quad [166]$$

$$\Box\ a:\ b_1 = \mathsf{SBit} \quad [35]$$
$$a:\ \mathsf{SBit} = \mathsf{flip}(b_{20}) \quad [166]$$
$$\to\ b_1 = \mathsf{flip}(b_{20})$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_{16}, b_4) \quad [145]$$
$$\to\ b_1 = b_4$$
$$b:\ b_4 = \mathsf{SBit} \quad [155]$$
$$b:\ \mathsf{SBit} = b_{20} \quad [160]$$
$$\to\ b_4 = b_{20}$$

E5: $\forall B : B \neq \mathsf{flip}(B)$

Rechter Zweig:

$$a:\ \mathsf{SFile}(s(n_{21})) = \bot \quad [167]$$
$$a:\ \mathsf{RQ} = q_{21} \quad [168]$$
$$a:\ \mathsf{SNo} = n_{21} \quad [169]$$
$$a:\ \mathsf{SBit} = b_{20} \quad [170]$$
$$a:\ \mathsf{ready} = \mathsf{true} \quad [171]$$

RQ nicht verändert: analog [94] bzw. [109]:

für $b : \mathsf{RQ} = \varepsilon$:

$$b:\ \mathsf{RQ} = q_{21} \quad [161]$$
$$a:\ \mathsf{RQ} = q_{21} \quad [168]$$
$$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [46]$$

$\Box$ (E2)

für $b : \mathsf{RQ} = \mathsf{msg}(d_{19}^3, b_4)|q_{19}^3$:

$$a:\ \mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [34]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_{16}, b_4) \quad [145]$$
$$\to\ b_1 = b_4$$
$$b:\ \mathsf{RQ} = q_{21} \quad [161]$$
$$a:\ \mathsf{RQ} = q_{21} \quad [168]$$
$$\to\ a:\ \mathsf{RQ} = \mathsf{msg}(d_{19}^3, b_4)|q_{19}^3$$
$$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1^3, b_1)|Q_1^3) \quad [43]$$
$$\to\ b_4 \neq b_1$$
$$\{D_1^3 \leftarrow d_{19}^3,\ Q_1^3 \leftarrow q_{19}^3\}$$

Damit ist auch die dritte Teilaussage von A1 gezeigt.

5.4 2. Teilaussage

Vollkommen anders wird der Beweis für Aussage A2 geführt: Versucht man, ihn ebenfalls über Anwendung der passenden Induktionshypothese zu führen, bekommt man im Zusammenhang mit SLose jede Menge Probleme mit der Gleichheitsbehandlung der Queues.

Er setzt an Knoten [21] an, die Knotennumerierung beginnt entsprechend bei [22] und die Indizes werden bei 1 beginnend numeriert.

Dieser Teilbeweis stellt relativ hohe Anforderungen an die Gleichheitsbehandlung, da der assoziative Operator "|" im Mittelpunkt steht. Des weiteren sind für eine automatische Beweisführung die mit Hilfe der Datenstrukturaxiome Q1-Q3 durchgeführten Fallunterscheidungen problematisch. Sie sind potentiell unendlich oft anwendbar und um diejenigen Segmente von SQ festzustellen, auf die sie angewendet werden müssen, werden spezielle Heuristiken benötigt.

Beweisskizze:

Situation: $\mathsf{SQ}_a \neq \varepsilon$, es gibt eine Nachricht $m_1 = \mathsf{msg}(d_1, b_1)$ in SQ_a, deren Kontrollbit $b_1 = \mathsf{SBit}_a$ ist, sowie eine weitere, in SQ neuere Nachricht $m_2 = \mathsf{msg}(d_2, b_2)$, deren Kontrollbit $b_2 \neq \mathsf{SBit}_a$ ist.

In diesem Fall wird – unter intensiver Einbeziehung der Gleichheit – "rückblickend" betrachtet, wie SQ vorher ausgesehen haben kann, und alle diese Situationen als unmöglich erkannt.

Wurde $\mathsf{SendCom}$ angewendet, ergibt sich, daß alle Nachrichten, die in SQ_a enthalten sind, auch schon in SQ_b enthalten waren. Damit liefert A2 als Induktionsvoraussetzung den gewünschten Widerspruch – falls $\mathsf{SBit}_b = b_1 = \mathsf{SBit}_a$ ist.

Es ergibt sich an dieser Stelle, daß $\mathsf{ProcAck}$ SBit nicht verändert haben kann: Dazu müßte $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ und somit nach A1 das erste sowie nach A2 alle Kontrollbits von SQ_b gleich $\mathsf{SBit}_b \neq \mathsf{SBit}_a$ sein.

Somit ist also $\mathsf{SBit}_a = \mathsf{SBit}_b$.

Wurde SLose angewendet, so sind ebenfalls alle Nachrichten aus SQ_a schon in SQ_b enthalten gewesen. Vorgehen analog dem eben betrachteten Fall.

Wurde AckMsg angewendet, wird unterschieden, ob m_2 die letzte – also durch AckMsg angehängte – Nachricht ist, oder ob m_1 und m_2 beide bereits in SQ_b enthalten waren. Im zweiten Fall geht man analog den bereits betrachteten Fällen vor.

Im ersten Fall muß weiter unterschieden werden, ob m_1 die in SQ_a vorletzte – also in SQ_b letzte – Nachricht ist, womit A3 ausreicht, um $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_a) = \mathsf{SBit}_a$ zu zeigen, oder ob auf m_1 in SQ_b weitere Nachrichten folgen, womit man erst aus A2 eine Aussage über die letzte Nachricht und dann mit A3 das gesuchte Ergebnis bekommt.

In allen Fällen ergibt sich die Anwendbarkeit der Induktionsvoraussetzung aus $\mathsf{SBit}_a = \mathsf{SBit}_b$ wie oben.

Ist SQ nicht verändert worden, erhält man den Beweis sofort aus A2.

Man hätte den Beweis optisch ansprechender gestalten können, wenn man das bei [50] beginnende Teiltableau an den Anfang gestellt hätte (Anwendung auf eine durch das EA-Axiom $b: \exists B : \mathsf{SBit} = B$ eingeführte Skolemkonstante). Da das Zurechtlegen aller Konstanten und anschließende Zusammenstückeln des Beweises aber nicht der elegante Weg ist und im übrigen durch Heuristiken nicht nachvollziehbar ist (welche Konstanten werden benötigt?), wird es soweit möglich unterlassen.

$\vdots$

von [21] (S. 31):

$a:\ \neg A2 \vee \neg A3 \vee \neg A4 \vee \neg A5$ [21]

$a:\ \neg A2$ [22]

$a:\ \neg A3 \vee \neg A4 \vee \neg A5$ [23]

↪ S. 81

$a:\ \neg(\forall B, B' :\ (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'')$ [24]
$\rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}))$

$a:\ \neg((\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,b_1)|Q'|\mathsf{msg}(D',b_1')|Q'') \rightarrow (b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit}))$ [25]

$a:\ (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,b_1)|Q'|\mathsf{msg}(D',b_1')|Q'')$ [26]

$a:\ \neg(b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit})$ [27]

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1''$ [28]
$a:\ b_1 = \mathsf{SBit}$ [29]
$a:\ \neg(b_1' = \mathsf{SBit})$ [30]

aus EA: $b:\ \exists Q : \mathsf{SQ} = q$ [31]

$b:\ \mathsf{SQ} = q_2$ [32]

aus SQ:

$b:\ \forall Q : \mathsf{SQ} = Q \rightarrow \mathsf{A}(\mathsf{SQ} = Q \text{ unless}^+ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [33]

aus Tab. 0.11:

$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [34]

$a:\ \mathsf{SQ} = q_2$ [35]

↪ S. 79

$a:\ \mathsf{SendCom} = \mathsf{true}$ [36]

aus Tab. 0.1:

$b:\ \mathsf{SIM} = \perp$ [39]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_3,b_3)|q_3$ [40]

$a:\ \mathsf{SQ} = q_3$ [41]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_3,b_3)$ [42]

↪ S. 65

$a:\ \mathsf{SLose} = \mathsf{true}$ [37]

↪ S. 70

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [38]

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{15},b_{15})$ [108]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{15})$ [109]

$b:\ \mathsf{SQ} = q_{16}$ [110]

$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda,b_{15})$ [111]

$a:\ \mathsf{RIM} = \perp$ [112]

↪ S. 71

$$\vdots$$

von [42] (S. 64):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1'' \quad [28]$$
$$a:\ b_1 = \mathsf{SBit} \quad [29]$$
$$a:\ \neg(b_1' = \mathsf{SBit}) \quad [30]$$
$$b:\ \mathsf{SQ} = \mathsf{msg}(d_3,b_3)|q_3 \quad [40]$$
$$a:\ \mathsf{SQ} = q_3 \quad [41]$$

Induktionsvoraussetzung A2:

aus $b:\ A2\ [14]:$

$$b:\ \forall B,B' : (\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}) \quad [43]$$

$$b:\ (\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_4)|Q'|\mathsf{msg}(D',B_4')|Q'') \rightarrow (B_4 = \mathsf{SBit} \rightarrow B_4' = \mathsf{SBit}) \quad [44]$$

$$b:\ \neg(\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_4)|Q'|\mathsf{msg}(D',B_4')|Q'') \quad [45]$$
$$b:\ \neg(\mathsf{SQ} = Q_4|\mathsf{msg}(D_4,B_4)|Q_4'|\mathsf{msg}(D_4',B_4')|Q_4'') \quad [48]$$

$$\boxed{\begin{array}{l}
\square\ a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1'' \quad [28] \\
\quad a:\ \mathsf{SQ} = q_3 \quad [41] \\
\hline
q_3 = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1'' \\
b:\ \mathsf{SQ} = \mathsf{msg}(d_3,b_3)|q_3 \quad [40] \\
\hline
b:\ \mathsf{SQ} = \mathsf{msg}(d_3,b_3)|q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1'' \\
b:\ \neg(\mathsf{SQ} = Q_4|\mathsf{msg}(D_4,B_4)|Q_4'|\mathsf{msg}(D_4',B_4')|Q_4'') \quad [48] \\
\{Q_4 \leftarrow \mathsf{msg}(d_3,b_3)|q_1, D_4 \leftarrow d_1, B_4 \leftarrow b_1, Q_4' \leftarrow q_1', D_4' \leftarrow d_1', B_4' \leftarrow b_1', Q_4'' \leftarrow q_1''\}
\end{array}}$$

B_4, B_4' einsetzen:

$$\mathrm{LG}:\ b:\ \exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,b_1)|Q'|\mathsf{msg}(D',b_1')|Q'' \quad [46]$$
$$b:\ b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit} \quad [47]$$
$$b:\ \mathsf{SQ} = q_5|\mathsf{msg}(d_5,b_1)|q_5'|\mathsf{msg}(d_5',b_1')|q_5'' \quad [49]$$

$$\boxed{b:\ \neg(b_1 = \mathsf{SBit}) \quad [50]}$$

$\hookrightarrow$ S. 66

$$\mathrm{LG}:\ b:\ b_1 = \mathsf{SBit} \quad [51]$$
$$b:\ b_1' = \mathsf{SBit} \quad [52]$$

$$\boxed{\begin{array}{ll}
\square\ b:\ b_1 = \mathsf{SBit} \quad [51] & a:\ b_1 = \mathsf{SBit} \quad [29] \\
\quad b:\ b_1' = \mathsf{SBit} \quad [52] & a:\ \neg(b_1' = \mathsf{SBit}) \quad [30] \\
\hline
\rightarrow b_1 = b_1' & \rightarrow b_1 \neq b_1'
\end{array}}$$

Das an dieser Stelle beginnende Teiltableau zeigt, daß in der gegebenen Situation, falls SQ_b eine Nachricht mit Kontrollbit b_1 (der Rest von SQ_b ist nicht relevant) enthält, $\mathsf{SBit} = b_1$ ist.

$$\vdots$$

von [50] (S. 65):

$a:\ b_1 = \mathsf{SBit}$ [29]

$b:\ \mathsf{SQ} = q_5|\mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5''$ [49]

$b:\ \neg(b_1 = \mathsf{SBit})$ [50]

aus EA: $b:\ \exists B : \mathsf{SBit} = B$ [53]

$b:\ \mathsf{SBit} = b_6$ [54]

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \to \mathsf{A}(\mathsf{SBit} = B\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [55]

mit Tab. 0.11, $\{B \leftarrow b_6\}$:

Linker Zweig:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [56]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [58]

$b:\ \mathsf{SBit} = b_7$ [59]

$b:\ \mathsf{RQ} = q_8$ [60]

$b:\ \mathsf{SNo} = n_8$ [61]

Linker Unterzweig:

$a:\ \mathsf{SFile}(s(n_8)) = d_9$ [62]

$a:\ \mathsf{RQ} = q_8|\mathsf{msg}(\mathsf{SFile}(s(n_8)), \mathsf{flip}(b_7))$ [63]

$a:\ \mathsf{SNo} = s(n_8)$ [64]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_7)$ [65]

$\hookrightarrow$ S. 67

Rechter Unterzweig:

$a:\ \mathsf{SFile}(s(n_8)) = \bot$ [66]

$a:\ \mathsf{RQ} = q_8$ [67]

$a:\ \mathsf{SNo} = n_8$ [68]

$a:\ \mathsf{SBit} = b_7$ [69]

$a:\ \mathsf{ready} = \mathsf{true}$ [70]

$$\boxed{\begin{array}{ll} \square: & a:\ b_1 = \mathsf{SBit}\quad [29] \\ & a:\ \mathsf{SBit} = b_7\quad [69] \\ \hline & \to\ b_1 = b_7 \\ & b:\ \neg(b_1 = \mathsf{SBit})\quad [50] \\ & b:\ \mathsf{SBit} = b_7\quad [59] \\ \hline & \to\ b_1 \neq b_7 \end{array}}$$

Rechter Zweig:

$a:\ \mathsf{SBit} = b_6$ [57]

$$\boxed{\begin{array}{ll} \square: & a:\ b_1 = \mathsf{SBit}\quad [29] \\ & a:\ \mathsf{SBit} = b_6\quad [57] \\ \hline & \to\ b_1 = b_6 \\ & b:\ \neg(b_1 = \mathsf{SBit})\quad [50] \\ & b:\ \mathsf{SBit} = b_6\quad [54] \\ \hline & \to\ b_1 \neq b_6 \end{array}}$$

$$\vdots$$

von [65] (S. 66):

$$b:\ \mathsf{SQ} = q_5|\mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5'' \quad [49]$$
$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [50]$$
$$b:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7) \quad [58]$$
$$b:\ \mathsf{SBit} = b_7 \quad [59]$$

Induktionsvoraussetzung A1:

$$b:\ A1 \quad [13]:$$

$$\begin{array}{ll} b:\ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow & [71] \\ \quad (B = \mathsf{SBit} \rightarrow \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge & \\ \qquad (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge & \\ \qquad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) & \end{array}$$

$$\begin{array}{ll} b:\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{10})) \rightarrow & [72] \\ \quad (B_{10} = \mathsf{SBit} \rightarrow \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B_{10})|Q^1)) \wedge & \\ \qquad (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B_{10})) \wedge & \\ \qquad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B_{10})|Q^3)))) & \end{array}$$

Linker Zweig:

$$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{10})) \quad [73]$$
$$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{10}, B_{10})) \quad [74]$$
$$\square\ \{D_{10} \leftarrow d_7,\ B_{10} \leftarrow b_7\}(58, 74)$$

Rechter Zweig:

B_{10} einsetzen, weiter auflösen:

$$b:\ \neg(b_7 = \mathsf{SBit}) \quad [75]$$
$$\square\ (59, 75)$$

$$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_7)|Q^1) \quad [76]$$
$$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_7)) \quad [77]$$
$$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_7)|Q^3) \quad [78]$$

aus [76]:

$$b:\ \mathsf{SQ} = \varepsilon \quad [79]$$
$$\square\ (\mathrm{E2}, 49, 79)$$

$$b:\ \exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_7)|Q^1 \quad [80]$$
$$b:\ \mathsf{SQ} = \mathsf{msg}(d_{10}^1, b_7)|q_{10}^1 \quad [81]$$

↪ S. 68

$\vdots$

von [81] (S. 67):

$b:\ \mathsf{SQ} = q_5|\mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5''$ [49]

$b:\ \neg(b_1 = \mathsf{SBit})$ [50]

$b:\ \mathsf{SBit} = b_7$ [59]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{10}^1, b_7)|q_{10}^1$ [81]

$|$

"Fallunterscheidung":

Q4: $b:\ \forall Q, Q' : (\exists D, B : Q = Q'|\mathsf{msg}(D, B)) \to Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = \mathsf{msg}(D', B')|Q'')$ [82]

$b:\ (\exists D, B : Q_{11} = Q_{11}'|\mathsf{msg}(D, B)) \to Q_{11}' = \varepsilon \vee (\exists D', B', Q'' : Q_{11}' = \mathsf{msg}(D', B')|Q'')$ [83]

$b:\ \neg(\exists D, B : Q_{11} = Q_{11}'|\mathsf{msg}(D, B))$ [84]

$b:\ \neg(Q_{11} = Q_{11}'|\mathsf{msg}(D_{11}, B_{11}))$ [86]

$\Box\ \{Q_{11} \leftarrow q_5|\mathsf{msg}(d_5, b_1)\ , Q_{11}' \leftarrow q_5, \ldots\}(49, 86)$

Q_{11}' einsetzen:

$b:\ q_5 = \varepsilon \vee (\exists D', B', Q'' : q_5 = \mathsf{msg}(D', B')|Q''$ [85]

$b:\ q_5 = \varepsilon$ [87]

$\Box\ b:\ q_5 = \varepsilon$ [87]

$b:\ \mathsf{SQ} = q_5|\mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5''$ [49]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5''$

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{10}^1, b_7)|q_{10}^1$ [81]

$\to\ b_1 = b_7$

$b:\ \neg(b_1 = \mathsf{SBit})$ [50]

$b:\ \mathsf{SBit} = b_7$ [59]

$\to\ b_1 \neq b_7$

$b:\ \exists D', B', Q'' : q_5 = \mathsf{msg}(D', B')|Q''$ [88]

$b:\ q_5 = \mathsf{msg}(d_{11}', b_{11}')|q_{11}''$ [89]

$\hookrightarrow$ S. 69

$$\vdots$$

von [89] (S. 68):

$$b:\ \mathsf{SQ} = q_5|\mathsf{msg}(d_5,b_1)|q_5'|\mathsf{msg}(d_5',b_1')|q_5'' \quad [49]$$
$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [50]$$
$$b:\ \mathsf{SBit} = b_7 \quad [59]$$
$$b:\ \mathsf{SQ} = \mathsf{msg}(d_{10}^1,b_7)|q_{10}^1 \quad [81]$$
$$b:\ q_5 = \mathsf{msg}(d_{11}',b_{11}')|q_{11}'' \quad [89]$$

Induktionsvoraussetzung A2:

$$b:\ \forall B,B' : (\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'') \to (B = \mathsf{SBit} \to B' = \mathsf{SBit}) \quad [90]$$

$$b:\ (\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_{12})|Q'|\mathsf{msg}(D',B_{12}')|Q'') \to (B_{12} = \mathsf{SBit} \to B_{12}' = \mathsf{SBit}) \quad [91]$$

$$b:\ \neg(\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_{12})|Q'|\mathsf{msg}(D',B_{12}')|Q'') \quad [92]$$
$$b:\ \neg(\mathsf{SQ} = Q_{12}|\mathsf{msg}(D_{12},B_{12})|Q_{12}'|\mathsf{msg}(D_{12}',B_{12}')|Q_{12}'') \quad [94]$$

$$\boxed{\begin{array}{l} \Box\ b:\ \mathsf{SQ} = q_5|\mathsf{msg}(d_5,b_1)|q_5'|\mathsf{msg}(d_5',b_1')|q_5'' \quad [49] \\ \quad b:\ q_5 = \mathsf{msg}(d_{11}',b_{11}')|q_{11}'' \quad [89] \\ \quad b:\ \mathsf{SQ} = \mathsf{msg}(d_{10}^1,b_7)|q_{10}^1 \quad [81] \\ \quad \{Q_{12} \leftarrow \epsilon, D_{12} \leftarrow d_{10}^1, B_{12} \leftarrow b_7, Q_{12}' \leftarrow q_{11}'', D_{12}' \leftarrow d_5, \\ \quad B_{12}' \leftarrow b_1, Q_{12}'' \leftarrow q_5'|\mathsf{msg}(d_5',b_1')|q_5''\} \end{array}}$$

B_{12}, B_{12}' einsetzen:

$$b:\ b_7 = \mathsf{SBit} \to b_1 = \mathsf{SBit} \quad [93]$$

$$b:\ \neg(b_7 = \mathsf{SBit}) \quad [95] \qquad\qquad b:\ b_1 = \mathsf{SBit} \quad [96]$$
$$\Box\ (59,95) \qquad\qquad \Box(50,96)$$

$\vdots$

von [37] (S. 64):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1'' \quad [28]$$
$$a:\ b_1 = \mathsf{SBit} \quad [29]$$
$$a:\ \neg(b_1' = \mathsf{SBit}) \quad [30]$$
$$a:\ \mathsf{SLose} = \mathsf{true} \quad [37]$$

aus Tab. 0.3 mit SL2':

$$b:\ \mathsf{SQ} \neq \varepsilon \quad [97]$$

$$a:\ \neg(\mathsf{SQ} = Q_{13}|\mathsf{msg}(D_{13},B_{13})|Q_{13}'|\mathsf{msg}(D_{13}',B_{13}')|Q_{13}'') \quad [98]$$
$$\square\ \{Q_{13} \leftarrow q_1, D_{13} \leftarrow d_1, B_{13} \leftarrow b_1, Q_{13}' \leftarrow q_1', D_{13}' \leftarrow d_1', B_{13}' \leftarrow b_1', Q_{13}'' \leftarrow q_1''\}(28,98)$$

$$b:\ \mathsf{SQ} = r_{13}|\mathsf{msg}(d_1,b_1)|r_{13}'|\mathsf{msg}(d_1',b_1')|r_{13}'' \quad [99]$$

Induktionsvoraussetzung A2:

aus $b:\ A2$ [14] :

$$b:\ \forall B,B' : (\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}) \quad [100]$$

$$b:\ (\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_{14})|Q'|\mathsf{msg}(D',B_{14}')|Q'') \rightarrow (B_{14} = \mathsf{SBit} \rightarrow B_{14}' = \mathsf{SBit}) \quad [101]$$

$$b:\ \neg(\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_{14})|Q'|\mathsf{msg}(D',B_{14}')|Q'') \quad [102]$$
$$b:\ \neg(\mathsf{SQ} = Q_{14}|\mathsf{msg}(D_{14},B_{14})|Q_{14}'|\mathsf{msg}(D_{14}',B_{14}')|Q_{14}'') \quad [104]$$
$$\square\ \{Q_{14} \leftarrow r_{13}, D_{14} \leftarrow d_1, B_{14} \leftarrow b_1,$$
$$Q_{14}' \leftarrow r_{13}', D_{14}' \leftarrow d_1', B_{14}' \leftarrow b_1', Q_{14}'' \leftarrow r_{13}''\}(99,104)$$

B_{14}, B_{14}' einsetzen:

$$b:\ b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit} \quad [103]$$

$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [105]$$

wie [50] mit
[99] anstelle [49], [105] anstelle [50]

LG : $b:\ b_1 = \mathsf{SBit}$ [106]

$b:\ b_1' = \mathsf{SBit}$ [107]

$$\square \quad \begin{array}{l} b:\ b_1 = \mathsf{SBit}\ [106] \\ b:\ b_1' = \mathsf{SBit}\ [107] \\ \hline \rightarrow b_1 = b_1' \end{array} \qquad \begin{array}{l} a:\ b_1 = \mathsf{SBit}\ [29] \\ a:\ \neg(b_1' = \mathsf{SBit})\ [30] \\ \hline \rightarrow b_1 = b_1' \end{array}$$

$$\vdots$$

von [112] (S. 64):

$$a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28]$$
$$a: \ b_1 = \mathsf{SBit} \quad [29]$$
$$a: \ \neg(b_1' = \mathsf{SBit}) \quad [30]$$
$$b: \ \mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15}) \quad [108]$$
$$b: \ \mathsf{SQ} = q_{16} \quad [110]$$
$$a: \ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111]$$

"Fallunterscheidung" Q2:

$$a: \ \forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)|Q') \to Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B') \quad [113]$$
$$a: \ (\exists D, B : Q_{17} = \mathsf{msg}(D, B)|Q_{17}') \to Q_{17}' = \varepsilon \vee (\exists D', B', Q'' : Q_{17}' = Q''|\mathsf{msg}(D', B') \quad [114]$$

$$a: \ \neg(\exists D, B : Q_{17} = \mathsf{msg}(D, B)|Q_{17}') \quad [115]$$
$$a: \ \neg(Q_{17} = \mathsf{msg}(D_{17}, B_{17})|Q_{17}') \quad [117]$$
$$\Box \ \{Q_{17} \leftarrow \mathsf{msg}(d_1', b_1')|q_1'', Q_{17}' \leftarrow q_1''\}$$

Q_{17}' einsetzen:

$$a: \ q_1'' = \varepsilon \vee (\exists D', B', Q'' : q_1'' = Q''|\mathsf{msg}(D', B') \quad [116]$$

$$\boxed{a: \ q_1'' = \varepsilon \quad [118]}$$

$$a: \ \exists D', B', Q'' : q_1'' = Q''|\mathsf{msg}(D', B') \quad [119]$$
$$\boxed{a: \ q_1'' = q_{17}''|\mathsf{msg}(d_{17}', b_{17}') \quad [156]}$$

↪ S. 78

"Fallunterscheidung" Q3:

$$a: \ \forall Q, Q' : (\exists D, B : Q = Q'|\mathsf{msg}(D, B)) \to Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B')) \quad [120]$$
$$a: \ (\exists D, B : Q_{18} = Q_{18}'|\mathsf{msg}(D, B)) \to Q_{18}' = \varepsilon \vee (\exists D', B', Q'' : Q_{18}' = Q''|\mathsf{msg}(D', B')) \quad [121]$$

$$a: \ \neg(\exists D, B : Q_{18} = Q_{18}'|\mathsf{msg}(D, B)) \quad [122]$$
$$a: \ \neg(Q_{18} = Q_{18}'|\mathsf{msg}(D_{18}, B_{18})) \quad [124]$$
$$\Box \ \{Q_{18} \leftarrow q_1'|\mathsf{msg}(d_1', b_1'), Q_{18}' \leftarrow q_1'\}$$

Q_{18}' einsetzen:

$$a: \ q_1' = \varepsilon \vee (\exists D', B', Q'' : q_1' = Q''|\mathsf{msg}(D', B')) \quad [123]$$

$$\boxed{a: \ q_1' = \varepsilon \quad [125]}$$

↪ S. 72

$$a: \ \exists D', B', Q'' : q_1' = Q''|\mathsf{msg}(D', B') \quad [126]$$
$$\boxed{a: \ q_1' = q_{21}''|\mathsf{msg}(d_{21}', b_{21}') \quad [139]}$$

↪ S. 75

$\vdots$

von [125] (S. 71):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1''$ [28]

$a:\ b_1 = \mathsf{SBit}$ [29]

$a:\ \neg(b_1' = \mathsf{SBit})$ [30]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15})$ [108]

$b:\ \mathsf{SQ} = q_{16}$ [110]

$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15})$ [111]

$a:\ q_1'' = \varepsilon$ [118]

$a:\ q_1' = \varepsilon$ [125]

Induktionsvoraussetzung A3:

$b:\ \forall B : (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \rightarrow$ [127]
$(B = \mathsf{SBit} \rightarrow\ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q''))))$

$b:\ (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{19})) \rightarrow$ [128]
$(B_{19} = \mathsf{SBit} \rightarrow\ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B_{19})) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B_{19})|Q''))))$

$b:\ \neg(\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{19}))$ [129]

$b:\ \neg(\mathsf{SQ} = Q_{19}|\mathsf{msg}(D_{19}, B_{19}))$ [131]

$\Box$ $a:\ \mathsf{SQ} = q_1\|\mathsf{msg}(d_1, b_1)\|q_1'\|\mathsf{msg}(d_1', b_1')\|q_1''$ [28]
$a:\ q_1'' = \varepsilon$ [118]
$a:\ q_1' = \varepsilon$ [125]
$\rightarrow\ a:\ \mathsf{SQ} = q_1\|\mathsf{msg}(d_1, b_1)\|\mathsf{msg}(d_1', b_1')$
$a:\ \mathsf{SQ} = q_{16}\|\mathsf{msg}(\lambda, b_{15})$ [111]
$\rightarrow\ q_{16} = q_1\|\mathsf{msg}(d_1, b_1)$
$b:\ \mathsf{SQ} = q_{16}$ [110]
$b:\ \neg(\mathsf{SQ} = Q_{19}\|\mathsf{msg}(D_{19}, B_{19}))$ [131]
$\{Q_{19} \leftarrow q_1, D_{19} \leftarrow d_1, B_{19} \leftarrow b_1\}$

$b:\ b_1 = \mathsf{SBit} \rightarrow\ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1)) \wedge$ [130]
$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_1)|Q'')))$

$b:\ \neg(b_1 = \mathsf{SBit})$ [132]

$\hookrightarrow$ S. 73

LG : $b:\ b_1 = \mathsf{SBit}$ [133]

$b:\ \mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1)$ [134]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_1)|Q'')$ [135]

$\hookrightarrow$ S. 74

$$\vdots$$

von [132] (S. 72):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28]$$
$$a:\ b_1 = \mathsf{SBit} \quad [29]$$
$$b:\ \mathsf{SQ} = q_{16} \quad [110]$$
$$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111]$$
$$a:\ q_1'' = \varepsilon \quad [118]$$
$$a:\ q_1' = \varepsilon \quad [125]$$
$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [132]$$
$$\downarrow$$

Man hat – mit dem folgenden Gleichheitsresultat

$$\begin{array}{l}
a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28] \\
a:\ q_1'' = \varepsilon \quad [118] \\
a:\ q_1' = \varepsilon \quad [125] \\
\hline
\to\ a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|\mathsf{msg}(d_1', b_1') \\
a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111] \\
\hline
\to\ q_{16} = q_1|\mathsf{msg}(d_1, b_1) \\
b:\ \mathsf{SQ} = q_{15} \quad [110] \\
\hline
**\quad b:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad **
\end{array}$$

– dieselbe Situation wie in [50]

$$a:\ b_1 = \mathsf{SBit} \quad [29]$$
$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [132]$$
$$**\quad b:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad **$$

wobei bei den Abschlüssen obiges Gleichheitsresultat verwendet wird.

$$\vdots$$

von [134]/[135] (S. 72):

$$a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28]$$

$$a: \ b_1 = \mathsf{SBit} \quad [29]$$

$$a: \ \neg(b_1' = \mathsf{SBit}) \quad [30]$$

$$b: \ \mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15}) \quad [108]$$

$$a: \ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111]$$

$$a: \ q_1'' = \varepsilon \quad [118]$$

$$b: \ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1) \quad [134]$$

$$b: \ \mathsf{RIM} = \bot \quad [136]$$

$$\Box \ (\mathrm{E3}, 108, 136)$$

$$b: \ \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1) \quad [137]$$

$$b: \ \mathsf{RIM} = \mathsf{msg}(d_{20}', b_1) \quad [138]$$

$$\boxed{\begin{array}{ll}
\Box & b: \ \mathsf{RIM} = \mathsf{msg}(d_{20}', b_1) \quad [138] \\
 & b: \ \mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15}) \quad [108] \\
\hline
 & \rightarrow \ b_1 = b_{15} \\
 & a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28] \\
 & a: \ q_1'' = \varepsilon \quad [118] \\
 & a: \ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111] \\
\hline
 & \rightarrow \ b_1' = b_{15} \\
 & a: \ b_1 = \mathsf{SBit} \quad [29] \\
 & a: \ \neg(b_1' = \mathsf{SBit}) \quad [30] \\
\hline
 & \rightarrow \ b_1 \neq b_1'
\end{array}}$$

$$\vdots$$

von [139] (S. 71):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28]$$

$$a:\ b_1 = \mathsf{SBit} \quad [29]$$

$$a:\ \neg(b_1' = \mathsf{SBit}) \quad [30]$$

$$b:\ \mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15}) \quad [108]$$

$$b:\ \mathsf{SQ} = q_{16} \quad [110]$$

$$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111]$$

$$a:\ q_1'' = \varepsilon \quad [118]$$

$$a:\ q_1' = q_{21}''|\mathsf{msg}(d_{21}', b_{21}') \quad [139]$$

$$|$$

Induktionsvoraussetzung A3:

$$b:\ \forall B : (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \rightarrow \quad [140]$$
$$(B = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q''))))$$

$$|$$

$$b:\ (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{22})) \rightarrow \quad [141]$$
$$(B_{22} = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B_{22})) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B_{22})|Q''))))$$

$$b:\ \neg(\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{22})) \quad [142]$$

$$b:\ \neg(\mathsf{SQ} = Q_{22}|\mathsf{msg}(D_{22}, B_{22})) \quad [144]$$

$$\boxed{\begin{array}{l}
\Box\ a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28]\\
a:\ q_1'' = \varepsilon \quad [118]\\
a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111]\\
\hline
\rightarrow\ q_{16} = q_1|\mathsf{msg}(d_1, b_1)|q_1'\\
a:\ q_1' = q_{21}''|\mathsf{msg}(d_{21}', b_{21}') \quad [139]\\
\hline
\rightarrow\ q_{16} = q_1|\mathsf{msg}(d_1, b_1)|q_{21}''|\mathsf{msg}(d_{21}', b_{21}')\\
b:\ \mathsf{SQ} = q_{16} \quad [110]\\
b:\ \neg(\mathsf{SQ} = Q_{22}|\mathsf{msg}(D_{22}, B_{22})) \quad [144]\\
\{Q_{22} \leftarrow q_1|\mathsf{msg}(d_1, b_1)|q_{21}'', D_{22} \leftarrow d_{21}', B_{22} \leftarrow b_{21}'\}
\end{array}}$$

$$b:\ b_{21}' = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_{21}')) \wedge \quad [143]$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_{21}')|Q'')))$$

$\hookrightarrow$ S. 76

$\vdots$

von [143] (S. 75):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1''$ [28]

$a:\ b_1 = \mathsf{SBit}$ [29]

$a:\ \neg(b_1' = \mathsf{SBit})$ [30]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15})$ [108]

$b:\ \mathsf{SQ} = q_{16}$ [110]

$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15})$ [111]

$a:\ q_1'' = \varepsilon$ [118]

$a:\ q_1' = q_{21}''|\mathsf{msg}(d_{21}'', b_{21}')$ [139]

$|$

$b:\ b_{21}' = \mathsf{SBit} \rightarrow\ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_{21}')) \wedge$ [143]
$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_{21}')|Q'')))$

$b:\ \neg(b_{21}' = \mathsf{SBit})$ [145]

LG : $b:\ b_{21}' = \mathsf{SBit}$ [146]

$b:\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_{21}')$ [147]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_{21}')|Q'')$ [148]

$\hookrightarrow$ S. 77

Induktionsvoraussetzung A2:

$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit})$ [149]

$|$

$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{23})|Q'|\mathsf{msg}(D', B_{23}')|Q'') \rightarrow (B_{23} = \mathsf{SBit} \rightarrow B_{23}' = \mathsf{SBit})$ [150]

$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{23})|Q'|\mathsf{msg}(D', B_{23}')|Q'')$ [151]

$b:\ \neg(\mathsf{SQ} = Q_{23}|\mathsf{msg}(D_{23}, B_{23})|Q_{23}'|\mathsf{msg}(D_{23}', B_{23}')|Q_{23}'')$ [153]

□ $a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1''$ [28]
$a:\ q_1' = q_{21}''|\mathsf{msg}(d_{21}'', b_{21}')$ [139]
$a:\ q_1'' = \varepsilon$ [118]

$\rightarrow\ a : \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_{21}''|\mathsf{msg}(d_{21}'', b_{21}')|\mathsf{msg}(d_1', b_1')$
$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15})$ [111]

$\rightarrow\ q_{16} = q_1|\mathsf{msg}(d_1, b_1)|q_{21}''|\mathsf{msg}(d_{21}'', b_{21}')$
$b:\ \mathsf{SQ} = q_{16}$ [110]
$b:\ \neg(\mathsf{SQ} = Q_{23}|\mathsf{msg}(D_{23}, B_{23})|Q_{23}'|\mathsf{msg}(D_{23}', B_{23}')|Q_{23}'')$ [153]
$\{Q_{23} \leftarrow q_1, D_{23} \leftarrow d_1, B_{23} \leftarrow b_1, Q_{23}' \leftarrow q_{21}'',$
$D_{23}' \leftarrow d_{21}', B_{23}' \leftarrow b_{21}', Q_{23}'' \leftarrow \varepsilon\}$

$b:\ b_1 = \mathsf{SBit} \rightarrow b_{21}' = \mathsf{SBit}$ [152]

$\hookrightarrow$ S. 77

$$\vdots$$

von [152] (S. 76):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28]$$
$$b:\ \mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15}) \quad [108]$$
$$b:\ \mathsf{SQ} = q_{16} \quad [110]$$
$$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111]$$
$$a:\ q_1'' = \varepsilon \quad [118]$$
$$a:\ q_1' = q_{21}''|\mathsf{msg}(d_{21}', b_{21}') \quad [139]$$
$$b:\ b_1 = \mathsf{SBit} \to b_{21}' = \mathsf{SBit} \quad [152]$$

$b:\ \neg(b_1 = \mathsf{SBit})$ [154]	$b:\ b_{21}' = \mathsf{SBit}$ [155]
$\downarrow$	$\Box$ (145, 155)

In [154] hat man unter Berücksichtigung des Gleichheitsresultats

$$\begin{array}{l}
a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28] \\
a:\ q_1'' = \varepsilon \quad [118] \\
a:\ q_1' = q_{21}''|\mathsf{msg}(d_{21}', b_{21}') \quad [139] \\
\hline
\to\ a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_{21}''|\mathsf{msg}(d_{21}', b_{21}')|\mathsf{msg}(d_1', b_1') \\
a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111] \\
b:\ \mathsf{SQ} = q_{16} \quad [110] \\
\hline
**\quad b:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_{21}''|\mathsf{msg}(d_{21}', b_{21}') \quad **
\end{array}$$

dieselbe Situation wie in [50]

$$a:\ b_1 = \mathsf{SBit} \quad [29]$$
$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [154]$$
$$**\quad b:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_{21}''|\mathsf{msg}(d_{21}', b_{21}') \quad **$$

wobei man bei den Abschlüssen diese Gleichheiten ausnutzt.

Der bei [146]-[148] (S. 76): offene Zweig ist dieselbe Situation wie in [135] (74):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28]$$
$$a:\ b_1 = \mathsf{SBit} \quad [29]$$
$$a:\ \neg(b_1' = \mathsf{SBit}) \quad [30]$$
$$b:\ \mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15}) \quad [108]$$
$$b:\ \mathsf{SQ} = q_{16} \quad [110]$$
$$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda, b_{15}) \quad [111]$$
$$a:\ q_1'' = \varepsilon \quad [118]$$
$$b:\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_{21}') \quad [147]$$

$$\vdots$$

von [156] (S. 71):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1'' \quad [28]$$

$$a:\ b_1 = \mathsf{SBit} \quad [29]$$

$$a:\ \neg(b_1' = \mathsf{SBit}) \quad [30]$$

$$b:\ \mathsf{SQ} = q_{16} \quad [110]$$

$$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda,b_{15}) \quad [111]$$

$$a:\ q_1'' = q_{17}''|\mathsf{msg}(d_{17}',b_{17}') \quad [156]$$

Induktionsvoraussetzung A2:

aus $b:\ A2$ [14] :

$$b:\ \forall B,B' : (\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}) \quad [157]$$

$$b:\ (\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_{24})|Q'|\mathsf{msg}(D',B_{24}')|Q'') \rightarrow (B_{24} = \mathsf{SBit} \rightarrow B_{24}' = \mathsf{SBit}) \quad [158]$$

$$b:\ \neg(\exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_{24})|Q'|\mathsf{msg}(D',B_{24}')|Q'') \quad [159]$$

$$b:\ \neg(\mathsf{SQ} = Q_{24}|\mathsf{msg}(D_{24},B_{24})|Q_{24}'|\mathsf{msg}(D_{24}',B_{24}')|Q_{24}'') \quad [162]$$

$\square$ $a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1''$ [28]

$a:\ q_1'' = q_{17}''|\mathsf{msg}(d_{17}',b_{17}')$ [156]

$\rightarrow$ $a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_{17}''|\mathsf{msg}(d_{17}',b_{17}')$

$a:\ \mathsf{SQ} = q_{16}|\mathsf{msg}(\lambda,b_{15})$ [111]

$b:\ \mathsf{SQ} = q_{16}$ [110]

$\rightarrow$ $b:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_{17}''$

$b:\ \neg(\mathsf{SQ} = Q_{24}|\mathsf{msg}(D_{24},B_{24})|Q_{24}'|\mathsf{msg}(D_{24}',B_{24}')|Q_{24}'')$ [162]

$\{Q_{24} \leftarrow q_1, D_{24} \leftarrow d_1, B_{24} \leftarrow b_1, Q_{24}' \leftarrow q_1', D_{24}' \leftarrow d_1', B_{24}' \leftarrow b_1', Q_{24}'' \leftarrow q_{17}''\}$

B_{24}, B_{24}' einsetzen:

$$\text{LG}:\ b:\ \exists D,D',Q,Q',Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,b_1)|Q'|\mathsf{msg}(D',b_1')|Q'' \quad [160]$$

$$b:\ b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit} \quad [161]$$

$$b:\ \mathsf{SQ} = q_{25}|\mathsf{msg}(d_{25},b_1)|q_{25}'|\mathsf{msg}(d_{25}',b_1')|q_{25}'' \quad [163]$$

$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [164]$$

wie [50] mit
[163] anstelle [49], [164] anstelle [50]

$$\text{LG}:\ b:\ b_1 = \mathsf{SBit} \quad [165]$$

$$b:\ b_1' = \mathsf{SBit} \quad [166]$$

$\square$ $b:\ b_1 = \mathsf{SBit}$ [165]	$a:\ b_1 = \mathsf{SBit}$ [29]
$b:\ b_1' = \mathsf{SBit}$ [166]	$a:\ \neg(b_1' = \mathsf{SBit})$ [30]
$\rightarrow b_1 = b_1'$	$\rightarrow b_1 = b_1'$

$$\vdots$$

von [35] (S. 64):

$a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28]$

$a: \ b_1 = \mathsf{SBit} \quad [29]$

$a: \ \neg(b_1' = \mathsf{SBit}) \quad [30]$

$b: \ \mathsf{SQ} = q_2 \quad [32]$

$a: \ \mathsf{SQ} = q_2 \quad [35]$

Induktionsvoraussetzung A2:

aus $b: \ A2$ [14] :

$b: \ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}) \quad [167]$

$b: \ (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{26})|Q'|\mathsf{msg}(D', B_{26}')|Q'') \rightarrow (B_{26} = \mathsf{SBit} \rightarrow B_{26}' = \mathsf{SBit}) \quad [168]$

$b: \ \neg(\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{26})|Q'|\mathsf{msg}(D', B_{26}')|Q'') \quad [169]$

$b: \ \neg(\mathsf{SQ} = Q_{26}|\mathsf{msg}(D_{26}, B_{26})|Q_{26}'|\mathsf{msg}(D_{26}', B_{26}')|Q_{26}'') \quad [171]$

$\square$ $a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [28]$
$a: \ \mathsf{SQ} = q_2 \quad [35]$
$b: \ \mathsf{SQ} = q_2 \quad [32]$
$b: \ \neg(\mathsf{SQ} = Q_{26}|\mathsf{msg}(D_{26}, B_{26})|Q_{26}'|\mathsf{msg}(D_{26}', B_{26}')|Q_{26}'') \quad [171]$
$\{Q_{26} \leftarrow q_1, D_{26} \leftarrow d_1, B_{26} \leftarrow b_1, Q_{26}' \leftarrow q_1',$
$D_{26}' \leftarrow d_1', B_{26}' \leftarrow b_1', Q_{26}'' \leftarrow q_1''\}$

B_{26}, B_{26}' einsetzen:

$b: \ b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit} \quad [170]$

$b: \ \neg(b_1 = \mathsf{SBit}) \quad [172]$

wie [50] mit
[28],[32],[35] anstelle [49],
[172] anstelle [50]

LG : $b: \ b_1 = \mathsf{SBit} \quad [173]$

$b: \ b_1' = \mathsf{SBit} \quad [174]$

$\square$ $\dfrac{b: \ b_1 = \mathsf{SBit} \ [173] \qquad b: \ b_1' = \mathsf{SBit} \ [174]}{\rightarrow b_1 = b_1'}$ $\qquad \dfrac{a: \ b_1 = \mathsf{SBit} \ [29] \qquad a: \ \neg(b_1' = \mathsf{SBit}) \ [30]}{\rightarrow b_1 = b_1'}$

Damit ist der Beweis der Teilaussage A2 von Lemma 1 abgeschlossen. Analog zum Beweis der ersten Teilaussage folgt derjenige der dritten, wobei die Knoten bei [23], die Indizes wieder bei 1 beginnen.

5.5 3. Teilaussage, 1. Teil

Situation: $\mathsf{SQ}_a \neq \varepsilon$, $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_a)) = \mathsf{SBit}_a$, $\mathsf{RIM}_a \neq \perp$, $\mathsf{Bit}(\mathsf{RIM}_a) \neq \mathsf{SBit}_a$.

Es wird versucht, A3 als Induktionsvoraussetzung zu verwenden.
Dabei wird zuerst die Situation behandelt, daß SQ_b leer ist. Da SQ_a nicht leer ist, muß also AckMsg ausgeführt worden sein. Danach wäre aber RIM_a leer.

Als zweite Situation ist SQ_b nicht leer, aber $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_b)) \neq \mathsf{SBit}_b$. In diesem Fall stellt man zuerst fest, daß sich SBit nicht geändert haben kann: Dazu müßte $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ und nach A1 $\mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b)) = \mathsf{SBit}_b$ und nach A2/A6 weiterhin $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_b)) = \mathsf{SBit}_b$ sein.
Also muß SQ – speziell die letzte Nachricht – verändert worden sein:
Falls SendCom die letzte Nachricht verändert, ist SQ nachher leer.
Falls SLose die letzte Nachricht entfernt, tritt die vorletzte an ihre Stelle. Nach Annahme ist deren Kontrollbit gleich $\mathsf{SBit}_a = \mathsf{SBit}_b$, womit nach A2 in in b ebenfalls $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_b)) = \mathsf{SBit}_b$ gelten müßte.
AckMsg kann die Veränderung ebenfalls nicht verursacht haben, da danach $\mathsf{RIM}_a = \perp$ wäre.

Also ist $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_b)) = \mathsf{SBit}_b$ und damit A3 in b anwendbar. Damit ist RIM_b entweder leer, oder $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{SBit}_b$, weiterhin ist RQ_b entweder leer, oder $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$.
SBit kann sich wieder nicht verändert haben, denn für ProcAck stellt man diesmal fest, daß – wäre ProcAck ausgeführt worden und hätte SBit verändert – $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b \neq \mathsf{SBit}_a$ gelten müßte: Nach A1 und A2 haben dann alle Nachrichten in SQ_b ebenfalls Kontrollbit $\mathsf{SBit}_b \neq \mathsf{SBit}_a$. Da aus demselben Grund wie oben AckMsg nicht ausgeführt wurde, war die in a letzte Nachricht in SQ_a also in b auch schon in SQ_b enthalten. Dies würde $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_a)) = \mathsf{SBit}_b \neq \mathsf{SBit}_a$ bedeuten.
Ist nun RIM_b leer, so enthält RIM_a die erste Nachricht aus RQ_b, es gilt also $\mathsf{Bit}(\mathsf{RIM}_a) = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b = \mathsf{SBit}_a$. Ist RIM_b nicht leer, so stellt man unschwer fest, daß $\mathsf{RIM}_a = \mathsf{RIM}_b$ gilt, womit auch das Kontrollbit dasselbe bleibt.

$\vdots$

von [23] (S. 64):

$a:\ \neg A3 \vee \neg A4 \vee \neg A5 \quad [23]$

$a:\ \neg A3 \quad [24]$

$a:\ \neg A4 \vee \neg A5 \quad [25]$

$\hookrightarrow$ S. 123

$$a:\ \neg\forall B : (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \rightarrow \quad [26]$$
$$(B = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q''))))$$

$$a:\ (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, b_1)) \rightarrow \quad [27]$$
$$(b_1 = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_1)|Q''))))$$

$$a:\ \exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, b_1) \quad [28]$$

$$a:\ \neg(b_1 = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1)) \wedge \quad [29]$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_1)|Q''))))$$

$$\boxed{\begin{array}{c} a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30] \\ a:\ b_1 = \mathsf{SBit} \quad [31] \end{array}}$$

$$a:\ \neg((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1)) \wedge (\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_1)|Q''))) \quad [32]$$

$$a:\ \neg(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_1)|Q'')) \quad [34]$$

$\hookrightarrow$ S. 98

$$a:\ \neg(\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1)) \quad [33]$$
$$a:\ \neg(\mathsf{RIM} = \bot) \quad [35]$$
$$a:\ \neg(\exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1)) \quad [36]$$
$$\boxed{a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D'_1, b_1)) \quad [37]}$$

aus F2R: $a:\ \mathsf{RIM} = \bot \vee \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \quad [38]$

$a:\ \mathsf{RIM} = \bot \quad [39]$

$\Box\ (35, 39)$

$a:\ \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \quad [40]$

$$\boxed{a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2) \quad [41]}$$

$\hookrightarrow$ S. 82

$\vdots$

von [41] (S. 81):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$$
$$a:\ b_1 = \mathsf{SBit} \quad [31]$$
$$a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1', b_1)) \quad [37]$$
$$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2) \quad [41]$$

"passende" Induktionsvoraussetzung A3 anwenden:

$$b:\ A3 \quad [15]$$
$$b:\ \forall B : (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \rightarrow \quad [42]$$
$$(B = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q''))))$$

$$b:\ (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_3)) \rightarrow \quad [43]$$
$$(B_3 = \mathsf{SBit} \rightarrow \ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B_3)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B_3)|Q''))))$$

$$b:\ \neg(\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_3)) \quad [44]$$
$$b:\ \neg(\mathsf{SQ} = Q_3|\mathsf{msg}(D_3, B_3)) \quad [46]$$

↪ S. 83

B_3 einsetzen (aus [51]):

$$\text{LG}:\ b:\ \exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, b_5') \quad [45]$$
$$\boxed{b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5') \quad [68]}$$

[43] komplett auflösen:

$$\boxed{b:\ \neg(b_5' = \mathsf{SBit}) \quad [69]}$$

aus EA:

$$b:\ \exists B : \mathsf{SBit} = B \quad [73]$$
$$\boxed{b:\ \mathsf{SBit} = b_9 \quad [74]}$$

↪ S. 84

$$\boxed{\text{LG}:\ b:\ b_5' = \mathsf{SBit} \quad [70]}$$
$$b:\ \mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_5') \quad [71]$$
$$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_5')|Q'') \quad [72]$$

↪ S. 89

$\vdots$

von [46] (S. 82):

$a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$

$a: \ \mathsf{RIM} = \mathsf{msg}(d_2, b_2) \quad [41]$

$b: \ \neg(\mathsf{SQ} = Q_3|\mathsf{msg}(D_3, B_3)) \quad [46]$

aus F1S:

$b: \ \mathsf{SQ} = \varepsilon \vee (\exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q \wedge \exists D', B', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')) \quad [47]$

$b: \ \mathsf{SQ} = \varepsilon \quad [48]$

$b: \ \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q \quad [49]$

$b: \ \exists D', B', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B') \quad [50]$

$b: \ \mathsf{SQ} = q'_5|\mathsf{msg}(d'_5, b'_5) \quad [51]$

$\square \ \{Q_3 \leftarrow q'_5, \ D_3 \leftarrow d'_5, \ B_3 \leftarrow b'_5\}(46, 51)$

aus SQ:

$b: \ \forall Q : \mathsf{SQ} = Q \rightarrow \mathsf{A}(\mathsf{SQ} = Q \ \mathsf{unless}^+ \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}) \quad [52]$

aus Tab. 0.11:

$a: \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true} \quad [53]$

$a: \ \mathsf{SQ} = \varepsilon \quad [54]$

$\square \ (\mathrm{E2}, 30, 54)$

$a: \ \mathsf{SendCom} = \mathsf{true} \quad [55]$

aus Tab. 0.1:

$b: \ \mathsf{SIM} = \bot \quad [58]$

$b: \ \mathsf{SQ} = \mathsf{msg}(d_6, b_6)|q_6 \quad [59]$

$a: \ \mathsf{SQ} = q_6 \quad [60]$

$a: \ \mathsf{SIM} = \mathsf{msg}(d_6, b_6) \quad [61]$

$\square(\mathrm{E2}, 48, 59)$

$a: \ \mathsf{SLose} = \mathsf{true} \quad [56]$

$b: \ \mathsf{SQ} \neq \varepsilon \quad [62]$

$\square \ (48, 62)$

$a: \ \mathsf{AckMsg} = \mathsf{true} \quad [57]$

aus Tab. 0.10:

$b: \ \mathsf{RIM} = \mathsf{msg}(d_7, b_7) \quad [63]$

$b: \ \mathsf{RBit} = \mathsf{flip}(b_7) \quad [64]$

$b: \ \mathsf{SQ} = q_8 \quad [65]$

$a: \ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7) \quad [66]$

$a: \ \mathsf{RIM} = \bot \quad [67]$

$\square \ (\mathrm{E3}, 41, 67)$

$$\vdots$$

von [74] (S. 82):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$$
$$a:\ b_1 = \mathsf{SBit} \quad [31]$$
$$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2) \quad [41]$$
$$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5') \quad [68]$$
$$b:\ \neg(b_5' = \mathsf{SBit}) \quad [69]$$
$$b:\ \mathsf{SBit} = b_9 \quad [74]$$

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true}) \quad [75]$

mit Tab. 0.11, $\{B \leftarrow b_9\}$:

$$a:\ \mathsf{ProcAck} = \mathsf{true} \quad [76]$$

mit Tab. 0.7:

$$b:\ \mathsf{SIM} = \mathsf{msg}(d_{10}, b_{10}) \quad [78]$$
$$\boxed{b:\ \mathsf{SBit} = b_{10} \quad [79]}$$

$$\boxed{a:\ \mathsf{SBit} = b_9 \quad [77]}$$

↪ S. 86

Induktionsvoraussetzung A1:

$$b:\ A1 \quad [13]:$$

$$\begin{aligned} b:\ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow & \qquad [80] \\ (B = \mathsf{SBit} \rightarrow \ & ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge \\ & (\mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge \\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) \end{aligned}$$

$$\begin{aligned} b:\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{11})) \rightarrow & \qquad [81] \\ (B_{11} = \mathsf{SBit} \rightarrow \ & ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B_{11})|Q^1)) \wedge \\ & (\mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B_{11})) \wedge \\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B_{11})|Q^3)))) \end{aligned}$$

$$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{11})) \quad [82]$$
$$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{11}, B_{11})) \quad [83]$$
$$\square\ \{D_{11} \leftarrow d_{10}, B_{11} \leftarrow b_{10}\}(78, 83)$$

[81] komplett auflösen:

$$b:\ \neg(b_{10} = \mathsf{SBit}) \quad [84]$$
$$\square\ (79, 84)$$

$$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{10})|Q^1) \quad [85]$$
$$b:\ \mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_{10}) \quad [86]$$
$$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_{10})|Q^3) \quad [87]$$

↪ S. 85

$\vdots$

von [85]-[87] (S. 84):

$b: \ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5') \quad [68]$

$b: \ \neg(b_5' = \mathsf{SBit}) \quad [69]$

$b: \ \mathsf{SBit} = b_{10} \quad [79]$

$b: \ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{10})|Q^1) \quad [85]$

$b: \ \mathsf{SQ} = \varepsilon \quad [88]$

$\Box$ (E2, 68, 88)

$b: \ \exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{10})|Q^1 \quad [89]$

$b: \ \mathsf{SQ} = \mathsf{msg}(d_{12}^1, b_{10})|q_{12}^1 \quad [90]$

A6 (Folgerung aus A2) anwenden:

$b: \ \forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \rightarrow (B = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B))) \quad [91]$

$b: \ (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{13})|Q) \rightarrow (B_{13} = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B_{13}))) \quad [92]$

$b: \ \neg(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{13})|Q) \quad [93]$

$b: \ \neg(\mathsf{SQ} = \mathsf{msg}(D_{13}, B_{13})|Q_{13}) \quad [95]$

$\Box \ \{D_{13} \leftarrow d_{12}^1, B_{13} \leftarrow b_{10}, Q_{13} \leftarrow q_{12}^1\}(90, 95)$

$b: \ b_{10} = \mathsf{SBit} \rightarrow (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', b_{10})) \quad [94]$

$b: \ \neg(b_{10} = \mathsf{SBit}) \quad [96]$

$\Box$ (79, 96)

$b: \ \exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', b_{10}) \quad [97]$

$b: \ \mathsf{SQ} = q_{13}'|\mathsf{msg}(d_{13}', b_{10}) \quad [98]$

$\Box \ b: \ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5') \quad [68]$

$b: \ \mathsf{SQ} = q_{13}'|\mathsf{msg}(d_{13}', b_{10}) \quad [98]$

$\rightarrow \ b_5' = b_{10}$

$b: \ \neg(b_5' = \mathsf{SBit}) \quad [69]$

$b: \ \mathsf{SBit} = b_{10} \quad [79]$

$\rightarrow \ b_5' \neq b_{10}$

$\vdots$

von [77] (S. 84):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [41]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5')$ [68]

$b:\ \neg(b_5' = \mathsf{SBit})$ [69]

$b:\ \mathsf{SBit} = b_9$ [74]

$a:\ \mathsf{SBit} = b_9$ [77]

aus SQ:

$b:\ \forall Q : \mathsf{SQ} = Q \rightarrow \mathsf{A}(\mathsf{SQ} = Q \ \mathsf{unless}^+ \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [99]

aus Tab. 0.11 ($Q \leftarrow q_4|\mathsf{msg}(d_4, b_5')$ aus [68]):

$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [100]

$a:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5')$ [101]

$$\boxed{\begin{array}{l} \Box\ \dfrac{a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)\ [30] \qquad a:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5')\ [101]}{\rightarrow\ b_1 = b_5'} \\[2ex] \dfrac{a:\ b_1 = \mathsf{SBit}\ [31] \quad a:\ \mathsf{SBit} = b_9\ [77]}{\rightarrow\ b_1 = b_9} \qquad \dfrac{b:\ \neg(b_5' = \mathsf{SBit})\ [69] \quad b:\ \mathsf{SBit} = b_9\ [74]}{\rightarrow\ b_5' \neq b_9} \end{array}}$$

$a:\ \mathsf{SendCom} = \mathsf{true}$ [102]

aus Tab. 0.1:

$b:\ \mathsf{SIM} = \perp$ [105]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{14}, b_{14})|q_{14}$ [106]

$a:\ \mathsf{SQ} = q_{14}$ [107]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{14}, b_{14})$ [108]

$\hookrightarrow$ S. 87

$a:\ \mathsf{SLose} = \mathsf{true}$ [103]

aus Tab. 0.3, SL2"':

$\sigma:\ \mathsf{SQ} \neq \varepsilon$ [117]

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [104]

aus Tab. 0.10:

$a:\ \mathsf{RIM} = \perp$ [128]

$\Box$ (E3, 41, 128)

$a:\ \neg(\mathsf{SQ} = Q_6|\mathsf{msg}(D_6, B_6))$ [118]

$\Box\ \{Q_6 \leftarrow q_1, D_6 \leftarrow d_1, B_6 \leftarrow b_1\}(30, 118)$

$b:\ \mathsf{SQ} = q_6'|\mathsf{msg}(d_1, b_1)$ [119]

$$\boxed{\Box\ \dfrac{a:\ b_1 = \mathsf{SBit}\ [31] \quad a:\ \mathsf{SBit} = b_9\ [77]}{\rightarrow\ b_1 = b_9} \qquad \dfrac{b:\ \mathsf{SQ} = q_6'|\mathsf{msg}(d_1, b_1)\ [119] \quad b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5')\ [68]}{\rightarrow\ b_1 = b_5'} \qquad \dfrac{b:\ \neg(b_5' = \mathsf{SBit})\ [69] \quad b:\ \mathsf{SBit} = b_9\ [74]}{\rightarrow\ b_5' \neq b_9}}$$

$b:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|\mathsf{msg}(d_6', b_6')$ [120]

$\hookrightarrow$ S. 88

$$\vdots$$

von [108] (S. 86):

$a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$

$a: \ b_1 = \mathsf{SBit} \quad [31]$

$b: \ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b'_5) \quad [68]$

$b: \ \neg(b'_5 = \mathsf{SBit}) \quad [69]$

$b: \ \mathsf{SBit} = b_9 \quad [74]$

$a: \ \mathsf{SBit} = b_9 \quad [77]$

$b: \ \mathsf{SQ} = \mathsf{msg}(d_{14}, b_{14})|q_{14} \quad [106]$

$a: \ \mathsf{SQ} = q_{14} \quad [107]$

aus Q2:

$b: \ \forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D,B)|Q') \rightarrow Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B')) \quad [109]$

$b: \ (\exists D, B : Q = \mathsf{msg}(D,B)|Q'_{15}) \rightarrow Q'_{15} = \varepsilon \vee (\exists D', B', Q'' : Q'_{15} = Q''|\mathsf{msg}(D', B')) \quad [110]$

$b: \ \neg(\exists D, B : Q_{15} = \mathsf{msg}(D,B)|Q'_{15}) \quad [111]$

$b: \ \neg(Q_{15} = \mathsf{msg}(D_{15}, B_{15})|Q'_{15}) \quad [113]$

$\Box \ \{Q_{15} \leftarrow \mathsf{SQ}, Q'_{15} \leftarrow q_{14}\}(106, 113)$

$b: \ q_{14} = \varepsilon \vee (\exists D', B', Q'' : q_{14} = Q''|\mathsf{msg}(D', B')) \quad [112]$

$b: \ q_{14} = \varepsilon \quad [114]$

$\Box \ a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$

$a: \ \mathsf{SQ} = q_{14} \quad [107]$

$b: \ q_{14} = \varepsilon \quad [114]$

(E2)

$b: \ \exists D', B', Q'' : q_{14} = Q''|\mathsf{msg}(D', B') \quad [115]$

$b: \ q_{14} = q''_{16}|\mathsf{msg}(d'_{16}, b'_{16}) \quad [116]$

$\Box \ b: \ \mathsf{SQ} = \mathsf{msg}(d_{14}, b_{14})|q_{14} \quad [106]$

$b: \ q_{14} = q''_{16}|\mathsf{msg}(d'_{16}, b'_{16}) \quad [116]$

$b: \ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b'_5) \quad [68]$

$\rightarrow \ b'_5 = b'_{16}$

$a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$

$a: \ \mathsf{SQ} = q_{14} \quad [107]$

$b: \ q_{14} = q''_{16}|\mathsf{msg}(d'_{16}, b'_{16}) \quad [116]$

$\rightarrow \ b_1 = b'_{16}$

$a: \ b_1 = \mathsf{SBit} \quad [31]$

$a: \ \mathsf{SBit} = b_9 \quad [77]$

$\rightarrow \ b_1 = b_9$

$b: \ \neg(b'_5 = \mathsf{SBit}) \quad [69]$

$b: \ \mathsf{SBit} = b_9 \quad [74]$

$\rightarrow \ b'_5 \neq b_9$

$\vdots$

von [120] (S. 86):

$a:\ b_1 = \mathsf{SBit}\quad [31]$

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b'_5)\quad [68]$

$b:\ \neg(b'_5 = \mathsf{SBit})\quad [69]$

$b:\ \mathsf{SBit} = b_9\quad [74]$

$a:\ \mathsf{SBit} = b_9\quad [77]$

$b:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|\mathsf{msg}(d'_6, b'_6)\quad [120]$

Induktionsvoraussetzung A2:

$b:\ A2\quad [14]:$

$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \to (B = \mathsf{SBit} \to B' = \mathsf{SBit})\quad [121]$

$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{17})|Q'|\mathsf{msg}(D', B'_{17})|Q'') \to (B_{17} = \mathsf{SBit} \to B'_{17} = \mathsf{SBit})\quad [122]$

$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{17})|Q'|\mathsf{msg}(D', B'_{17})|Q'')\quad [123]$

$b:\ \neg(\mathsf{SQ} = Q_{17}|\mathsf{msg}(D_{17}, B_{17})|Q'_{17}|\mathsf{msg}(D'_{17}, B'_{17})|Q''_{17})\quad [125]$

$\Box\ \{Q_{17} \leftarrow q_1, D_{17} \leftarrow d_1, B_{17} \leftarrow b_1, Q'_{17} \leftarrow \varepsilon,$
$D'_{17} \leftarrow d'_6, B'_{17} \leftarrow b'_6, Q''_{17} \leftarrow \varepsilon\}(120, 125)$

B_{17}, B'_{17} einsetzen:

$b:\ b_1 = \mathsf{SBit} \to b'_6 = \mathsf{SBit}\quad [124]$

$b:\ \neg(b_1 = \mathsf{SBit})\quad [126]$

$\Box\ a:\ b_1 = \mathsf{SBit}\quad [31]$
$a:\ \mathsf{SBit} = b_9\quad [77]$
$\to\ b_1 = b_9$
$b:\ \neg(b_1 = \mathsf{SBit})\quad [126]$
$b:\ \mathsf{SBit} = b_9\quad [74]$
$\to\ b_1 \neq b_9$

$b:\ b'_6 = \mathsf{SBit}\quad [127]$

$\Box\ b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b'_5)\quad [68]$
$b:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|\mathsf{msg}(d'_6, b'_6)\quad [120]$
$\to\ b'_5 = b'_6$
$b:\ \neg(b'_5 = \mathsf{SBit})\quad [69]$
$b:\ b'_6 = \mathsf{SBit}\quad [127]$
$\to\ b'_5 \neq b'_6$

$$\vdots$$

von [72] (S. 82):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D'_1, b_1))$ [37]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [41]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b'_5)$ [68]

$b:\ b'_5 = \mathsf{SBit}$ [70]

$b:\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b'_5)$ [71]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b'_5)|Q'')$ [72]

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \to \mathsf{A}(\mathsf{SBit} = B\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [129]

mit Tab. 0.11, $\{B \leftarrow b'_5\}$:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [130]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{18}, b_{18})$ [132]

$\boxed{b:\ \mathsf{SBit} = b_{18}\quad [133]}$

$\boxed{a:\ \mathsf{SBit} = b'_5\quad [131]}$

$\hookrightarrow$ S. 93

$\boxed{a:\ \mathsf{SBit} = \mathsf{flip}(b_{18})\quad [134]}$

$a:\ \mathsf{SBit} = b_{18}$ [135]

wie [131] ff. da SBit unverändert

$\Box$

Induktionsvoraussetzung A1:

$b:\ A1$ [13] :

$$\begin{aligned} b:\ &\forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \to && [136]\\ &(B = \mathsf{SBit} \to ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge \\ &\qquad (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge \\ &\qquad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) \end{aligned}$$

$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{19}))$ [137]

$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{19}, B_{19}))$ [142]

$\Box\ \{D_{19} \leftarrow d_{18}, B_{19} \leftarrow b_{18}\}(132, 142)$

[136] komplett auflösen:

$b:\ \neg(b_{18} = \mathsf{SBit})$ [138]

$\Box\ (133, 138)$

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{18})|Q^1)$ [139]

$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_{18})$ [140]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_{18})|Q^3)$ [141]

$\hookrightarrow$ S. 90

$\vdots$

von [139]-[141] (S. 89):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [41]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5')$ [68]

$b:\ b_5' = \mathsf{SBit}$ [70]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{18}, b_{18})$ [132]

$b:\ \mathsf{SBit} = b_{18}$ [133]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{18})$ [134]

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{18})|Q^1)$ [139]

$b:\ \mathsf{SQ} = \varepsilon$ [143]

$\square$ (E2, 68, 143)

$b:\ \exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{18})|Q^1$ [144]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{20}^1, b_{18})|q_{20}^1$ [145]

mit A7 (Folgerung aus A2):

$b:\ \forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \rightarrow$ [146]

$(B = \mathsf{SBit} \rightarrow (\forall Q, Q', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$

$b:\ (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{21})|Q) \rightarrow$ [147]

$(B_{21} = \mathsf{SBit} \rightarrow (\forall Q, Q', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$

$b:\ \neg(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{21})|Q)$ [148]

$b:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_{21}, B_{21})|Q_{21})$ [150]

$\square\ \{D_{21} \leftarrow d_{20}^1, B_{21} \leftarrow b_{18}, Q_{21} \leftarrow q_{20}^1\}(145, 150)$

B_{21} einsetzen:

$b:\ b_{18} = \mathsf{SBit} \rightarrow (\forall Q, Q', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit})$ [149]

$b:\ \neg(b_{18} = \mathsf{SBit})$ [151]

$\square$ (133, 151)

$b:\ \forall Q, Q', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}$ [152]

$b:\ \mathsf{SQ} = Q_{21}'|\mathsf{msg}(D_{21}', B_{21}')|Q_{21}' \rightarrow B_{21}' = \mathsf{SBit}$ [153]

$\hookrightarrow$ S. 91

$\vdots$

von [153] (S. 90):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [41]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5')$ [68]

$b:\ b_5' = \mathsf{SBit}$ [70]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{18}, b_{18})$ [132]

$b:\ \mathsf{SBit} = b_{18}$ [133]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{18})$ [134]

$b:\ \mathsf{SQ} = Q_{21}'|\mathsf{msg}(D_{21}', B_{21}')|Q_{21}' \to B_{21}' = \mathsf{SBit}$ [153]

aus SQ:

$b:\ \forall Q : \mathsf{SQ} = Q \to \mathsf{A}(\mathsf{SQ} = Q\ \mathsf{unless}^+\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [154]

aus Tab. 0.11, $\{Q \leftarrow q_4|\mathsf{msg}(d_4, b_5')\}$ aus [68]:

$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [155]

$a:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5')$ [156]

$\Box$ $a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5')$ [156]

$\to\ b_1 = b_5'$

$b:\ b_5' = \mathsf{SBit}$ [70]

$b:\ \mathsf{SBit} = b_{18}$ [133]

$\to\ b_5' = b_{18}$

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{18})$ [134]

$\to\ b_1 = \mathsf{flip}(b_{18})$

$a:\ \mathsf{SendCom} = \mathsf{true}$ [157]

aus Tab. 0.1:

$b:\ \mathsf{SIM} = \perp$ [160]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{22}, b_{22})|q_{22}$ [161]

$\Box(\mathrm{E2}, 132, 160)$

$a:\ \mathsf{SLose} = \mathsf{true}$ [158]

$\hookrightarrow$ S. 92

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [159]

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})$ [168]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{24})$ [169]

$b:\ \mathsf{SQ} = q_{25}$ [170]

$a:\ \mathsf{SQ} = q_{25}|\mathsf{msg}(\lambda, b_{24})$ [171]

$a:\ \mathsf{RIM} = \perp$ [172]

$\Box$ $(\mathrm{E3}, 41, 172)$

$\vdots$

von [158] (S. 91):

$a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a: \ b_1 = \mathsf{SBit}$ [31]

$b: \ \mathsf{SBit} = b_{18}$ [133]

$a: \ \mathsf{SBit} = \mathsf{flip}(b_{18})$ [134]

$b: \ \mathsf{SQ} = Q'_{21}|\mathsf{msg}(D'_{21}, B'_{21})|Q'_{21} \rightarrow B'_{21} = \mathsf{SBit}$ [153]

$a: \ \mathsf{SLose} = \mathsf{true}$ [158]

aus Tab. 0.3:

$b: \ \mathsf{SQ} \neq \varepsilon$ [162]

$a: \ \neg(\mathsf{SQ} = Q_{23}|\mathsf{msg}(D_{23}, B_{23}))$ [163]

$\square \ \{Q_{23} \leftarrow q_1, D_{23} \leftarrow d_1, B_{23} \leftarrow b_1\}(30, 163)$

$b: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)|\mathsf{msg}(d'_{23}, b'_{23})$ [165]

wie [164], mit $\{Q'_{21} \leftarrow \mathsf{msg}(d'_{23}, b'_{23})\}$.

$\square$

$b: \ \mathsf{SQ} = q'_{23}|\mathsf{msg}(d_1, b_1)$ [164]

aus [153]:

$b: \ \neg(\mathsf{SQ} = Q'_{21}|\mathsf{msg}(D'_{21}, B'_{21})|Q'_{21})$ [166]

$\square \ \{Q'_{21} \leftarrow q'_{23}, D'_{21} \leftarrow d_1, B'_{21} \leftarrow b_1, Q'_{21} \leftarrow \varepsilon\}(164, 166)$

$b: \ b_1 = \mathsf{SBit}$ [167]

$\square$ $b: \ b_1 = \mathsf{SBit}$ [167]

$b: \ \mathsf{SBit} = b_{18}$ [133]

$\rightarrow \ b_1 = b_{18}$

$a: \ b_1 = \mathsf{SBit}$ [31]

$a: \ \mathsf{SBit} = \mathsf{flip}(b_{18})$ [134]

$\rightarrow b_1 = \mathsf{flip}(b_{18})$

$\vdots$

von [131] (S. 89):

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1', b_1))$ [37]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)$ [41]

$b:\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_5')$ [71]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_5')|Q'')$ [72]

$a:\ \mathsf{SBit} = b_5'$ [131]

aus [71]:

$b:\ \mathsf{RIM} = \bot$ [173]

aus RIM:

$b:\ \forall M : \mathsf{RIM} = M \to \mathsf{A}(\mathsf{RIM} = M \ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [175]

aus Tab. 0.11

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [176]

$a:\ \mathsf{RecCom} = \mathsf{true}$ [178]

aus Tab. 0.2:

$b:\ \mathsf{RIM} = \bot$ [180]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{26}, b_{26})|q_{26}$ [181]

$a:\ \mathsf{RQ} = q_{26}$ [182]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_{26}, b_{26})$ [183]

aus [72]:

$b:\ \mathsf{RQ} = \varepsilon$ [184]

$\square$ (E2, 181, 184)

$b:\ \exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_5')|Q''$ [185]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{27}'', b_5')|q_{27}''$ [186]

$\square$

$$\frac{b:\ \mathsf{RQ} = \mathsf{msg}(d_{27}'', b_5')|q_{27}''\ [186] \qquad b:\ \mathsf{RQ} = \mathsf{msg}(d_{26}, b_{26})|q_{26}\ [181]}{\to\ b_5' = b_{26}} \qquad \frac{a:\ b_1 = \mathsf{SBit}\ [31] \qquad a:\ \mathsf{SBit} = b_5'\ [131]}{\to\ b_1 = b_5'}$$

$$\frac{a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_1', b_1))\ [37] \quad \{D_1' \leftarrow d_{26} \qquad a:\ \mathsf{RIM} = \mathsf{msg}(d_{26}, b_{26})\ [183]}{\to\ b_1 \neq b_{26}}$$

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [179]

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{28}, b_{28})$ [187]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{28})$ [188]

$b:\ \mathsf{SQ} = q_{29}$ [189]

$a:\ \mathsf{SQ} = q_{29}|\mathsf{msg}(\lambda, b_{28})$ [190]

$a:\ \mathsf{RIM} = \bot$ [191]

$\square$ (E3, 41, 191)

$a:\ \mathsf{RIM} = \bot$ [177]

$\square$ (E3, 41, 177)

$b:\ \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_5')$ [174]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{30}', b_5')$ [192]

$\hookrightarrow$ S. 94

$\vdots$

von [192] (S. 93):

$a:\ b_1 = \mathsf{SBit}\quad [31]$

$a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D'_1, b_1))\quad [37]$

$a:\ \mathsf{RIM} = \mathsf{msg}(d_2, b_2)\quad [41]$

$a:\ \mathsf{SBit} = b'_5\quad [131]$

$b:\ \mathsf{RIM} = \mathsf{msg}(d'_{30}, b'_5)\quad [192]$

aus RIM:

$b:\ \forall M : \mathsf{RIM} = M \rightarrow \mathsf{A}(\mathsf{RIM} = M\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\quad [193]$

aus Tab. 0.11

$a:\ \mathsf{RIM} = \mathsf{msg}(d'_{30}, b'_5)\quad [195]$

$\square\ a:\ b_1 = \mathsf{SBit}\quad [31]$

$a:\ \mathsf{SBit} = b'_5\quad [131]$

$\rightarrow\ b_1 = b'_5$

$a:\ \neg(\mathsf{RIM} = \mathsf{msg}(D'_1, b_1))\quad [37]$

$a:\ \mathsf{RIM} = \mathsf{msg}(d'_{30}, b'_5)\quad [195]$

$\rightarrow\ b_1 \neq b'_5$

$\{D'_1 \leftarrow d'_{30}\}$

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}\quad [194]$

$a:\ \mathsf{RecCom} = \mathsf{true}\quad [196]$

aus Tab. 0.2:

$b:\ \mathsf{RIM} = \bot\quad [198]$

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{31}, b_{31})|q_{26}\quad [199]$

$a:\ \mathsf{RQ} = q_{31}\quad [200]$

$a:\ \mathsf{RIM} = \mathsf{msg}(d_{31}, b_{31})\quad [201]$

$\square$ (E3, 192, 198)

$a:\ \mathsf{AckMsg} = \mathsf{true})\quad [197]$

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{32}, b_{32})\quad [202]$

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{32})\quad [203]$

$b:\ \mathsf{SQ} = q_{33}\quad [204]$

$a:\ \mathsf{SQ} = q_{33}|\mathsf{msg}(\lambda, b_{32})\quad [205]$

$a:\ \mathsf{RIM} = \bot\quad [206]$

$\square$ (E3, 41, 206)

An dieser Stelle ist der Beweis der ersten Teilaussage von A3 beendet.

5.6 3. Teilaussage, 2. Teil

Beweis der zweiten Teilaussage:

Der Beweis schließt an Knoten [34] des vorhergehenden Teilbeweises an. Wieder beginnt die Numerierung der Indizes bei 1.

Situation: $\mathsf{SQ}_a \neq \varepsilon$, $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_a)) = \mathsf{SBit}_a$, $\mathsf{RQ}_a \neq \varepsilon$, $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a)) \neq \mathsf{SBit}_a$.

Es wird wieder versucht, A3 als Induktionsvoraussetzung anzuwenden.

Als erstes hat man wieder die Situation zu behandeln, daß $\mathsf{SQ}_b = \varepsilon$ ist. Da SQ_a nicht leer ist, muß also AckMsg ausgeführt worden sein. Es folgt, daß $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_a)) = \mathsf{SBit}_a$ ist. ProcAck kann SBit nicht verändert haben kann, da sonst $\mathsf{SBit}_b = \mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{SBit}_a = \mathsf{flip}(\mathsf{SBit}_b)$ wäre. Also gilt $\mathsf{SBit}_b = \mathsf{SBit}_a = \mathsf{Bit}(\mathsf{RIM}_b)$, womit man nach A4 die Aussage „Falls RQ_b nicht leer ist, gilt $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$“ $\quad (**)$.
In jedem Fall müssen die Auswirkungen auf RQ_a unter Berücksichtigung der RQ verändernden Regeln untersucht werden: Dabei ist zu beachten, daß vorausgesetzt wurde, daß keine zwei RQ verändernden Regeln gleichzeitig angewendet werden.
Falls RQ_b nicht leer ist:
RecCom ist nicht anwendbar (AckMsg hat $\mathsf{RIM} \neq \perp$ als Vorbedingung).
RLose: Entweder bleibt die erste Nachricht erhalten, oder die zweite rückt an ihre Stelle. Im ersten Fall rückt die in RQ_b zweite Nachricht – falls sie existiert – an erste Stelle. Nach A5 hat diese das gleiche Kontrollbit wie die erste: $\mathsf{SBit}_b = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a)) \neq \mathsf{SBit}_a$. Da ProcAck nicht angewendet worden sein kann, ergibt sich ein Widerspruch.
RLose: Im Prinzip wie RecCom.
ReTrans und ProcAck oder keine der Regeln: Die erste Nachricht bleibt in beiden Fällen erhalten.
Falls RQ_b leer ist:
RecCom und RLose sind nicht anwendbar. Für ReTrans ergibt sich folgendes Bild: ReTrans hängt eine Nachricht mit Kontrollbit SBit_b an RQ an. Man erhält also wieder $\mathsf{SBit}_b = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a)) \neq \mathsf{SBit}_a$. Wurde ProcAck angewandt und hat SQ und SBit verändert, so ist $\mathsf{SBit}_a = \mathsf{flip}(\mathsf{SBit}_b) = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a))$ im Widerspruch zur Annahme.

Als nächstes wird der Fall betrachtet, daß $\mathsf{SQ}_b \neq \emptyset$ und $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_b)) \neq \mathsf{SBit}_b$ ist, wobei man fast den gleichen Widerspruch wie in [72] ff. der ersten Teilaussage von A3 erhält. Nur bei [126] (Ausführung von AckMsg) muß man anders abschließen: Wie dort schließt man ProcAck aus, erhält so $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_a)) = \mathsf{SBit}_a = \mathsf{SBit}_b$ und nach A4 die Aussage „Falls RQ_b nicht leer ist, gilt $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$“ und erreicht so denselben Stand wie oben.

Bleibt der Fall zu betrachten, daß in a und in b $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ})) = \mathsf{SBit}$ gilt, man also in b aus A1 die Aussage
“Falls RQ_b nicht leer ist, gilt $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$.“
erhält.
Als erstes wird festgestellt, daß $\mathsf{SBit}_a = \mathsf{SBit}_b$ ist: Sonst müßte ProcAck angewendet worden sein, also $\mathsf{SIM}_b \neq \perp$ und $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$, und somit nach A1 die Kontrollbits aller in b existenten Nach-

richten auch gleich $\mathsf{SBit}_b \neq \mathsf{SBit}_a$. Damit kann (Betrachtung aller SQ beeinflussenden Regeln) nicht $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_a)) = \mathsf{SBit}_a \neq \mathsf{SBit}_b$ sein.
Für $\mathsf{SBit}_a = \mathsf{SBit}_b$ wird schlußendlich die oben erhaltene Induktionsvoraussetzung ausgenutzt, um $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a)) = \mathsf{SBit}_b = \mathsf{SBit}_a$ zu zeigen.

$\vdots$

von [34] (S. 81):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)\quad [30]$

$a:\ b_1 = \mathsf{SBit}\quad [31]$

$a:\ \neg(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_1)|Q''))\quad [34]$

$|$

$\boxed{a:\ \neg(\mathsf{RQ} = \varepsilon)\quad [35]}$

$a:\ \neg(\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_1)|Q''))\quad [36]$

$\boxed{a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D''_1, b_1)|Q''_1)\quad [37]}$

$|$

aus F1R:

$a:\ \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q\quad [38]$

$a:\ \exists D', B', Q' : \mathsf{RQ} = Q'|\mathsf{msg}(D', B')\quad [39]$

$$\boxed{\begin{array}{l} a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2\quad [40] \\ a:\ \mathsf{RQ} = q'_2|\mathsf{msg}(d'_2, b'_2)\quad [41] \end{array}}$$

$|$

“passende“ Induktionsvoraussetzung A3 anwenden:

$b:\ A3\quad [15]$

$$\begin{array}{ll} b:\ \forall B : (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \rightarrow & [42] \\ \quad (B = \mathsf{SBit} \rightarrow\ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge & \\ \qquad (\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q'')))) & \end{array}$$

$|$

$$\begin{array}{ll} b:\ (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_3)) \rightarrow & [43] \\ \quad (B_3 = \mathsf{SBit} \rightarrow\ ((\mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B_3)) \wedge & \\ \qquad (\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B_3)|Q'')))) & \end{array}$$

$b:\ \neg(\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_3))\quad [44]$

$b:\ \neg(\mathsf{SQ} = Q_3|\mathsf{msg}(D_3, B_3))\quad [46]$

$\hookrightarrow$ S. 99

B_3 einsetzen (aus [51]):

$\mathrm{LG}:\ b:\ \exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, b_5)\quad [45]$

$\boxed{b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)\quad [160]}$

[43] komplett auflösen:

$\boxed{b:\ \neg(b_5 = \mathsf{SBit})\quad [161]}$

$|$

aus EA:

$b:\ \exists B : \mathsf{SBit} = B\quad [165]$

$\boxed{b:\ \mathsf{SBit} = b_{23}\quad [166]}$

$\hookrightarrow$ S. 108

$\boxed{\mathrm{LG}:\ b:\ b_5 = \mathsf{SBit}\quad [162]}$

$b:\ \mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_5)\quad [163]$

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_5)|Q'')\quad [164]$

$\hookrightarrow$ S. 110

$$\vdots$$

von [46] (S. 98):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)\quad [30]$

$a:\ b_1 = \mathsf{SBit}\quad [31]$

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')\quad [37]$

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2\quad [40]$

$b:\ \neg(\mathsf{SQ} = Q_3|\mathsf{msg}(D_3, B_3))\quad [46]$

aus F1S:

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q \wedge \exists D', B', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B'))\quad [47]$

$\boxed{b:\ \mathsf{SQ} = \varepsilon\quad [48]}$

$b:\ \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q\quad [49]$

$b:\ \exists D', B', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B'))\quad [50]$

$b:\ \mathsf{SQ} = \mathsf{msg}(d_5, b_5)|q_5\quad [51]$

$\Box\ \{D_3 \leftarrow d_5, B_3 \leftarrow b_5, Q_3 \leftarrow q_5\}(46, 51)$

aus SQ:

$b:\ \forall Q : \mathsf{SQ} = Q \rightarrow \mathsf{A}(\mathsf{SQ} = Q\ \mathsf{unless}^+\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\quad [52]$

aus Tab. 0.11:

$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}\quad [53]$

$a:\ \mathsf{SQ} = \varepsilon\quad [54]$

$\Box\ (\mathrm{E2}, 30, 54)$

$a:\ \mathsf{SendCom} = \mathsf{true}\quad [55]$

aus Tab. 0.1:

$b:\ \mathsf{SIM} = \perp\quad [58]$

$b:\ \mathsf{SQ} = \mathsf{msg}(d_6, b_6)|q_6\quad [59]$

$a:\ \mathsf{SQ} = q_6\quad [60]$

$a:\ \mathsf{SIM} = \mathsf{msg}(d_6, b_6)\quad [61]$

$\Box(\mathrm{E2}, 48, 59)$

$a:\ \mathsf{SLose} = \mathsf{true}\quad [56]$

aus Tab. 0.3:

$b:\ \mathsf{SQ} \neq \varepsilon\quad [62]$

$\Box\ (48, 62)$

$a:\ \mathsf{AckMsg} = \mathsf{true}\quad [57]$

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_7, b_7)\quad [63]$

$b:\ \mathsf{RBit} = \mathsf{flip}(b_7)\quad [64]$

$b:\ \mathsf{SQ} = q_8\quad [65]$

$a:\ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7)\quad [66]$

$a:\ \mathsf{RIM} = \perp\quad [67]$

$\hookrightarrow$ S. 100

$\vdots$

von [67] (S. 99):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D''_1, b_1)|Q''_1)$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_7, b_7)$ [63]

$b:\ \mathsf{SQ} = q_8$ [65]

$a:\ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7)$ [66]

$a:\ \mathsf{RIM} = \perp$ [67]

Induktionsvoraussetzung A4:

$b:\ A4$ [16]

$b:\ \forall B : (\exists D : \mathsf{RIM} = \mathsf{msg}(D, B)) \rightarrow$ [68]
$(B = \mathsf{SBit} \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', B)|Q'))$

$b:\ (\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_9)) \rightarrow$ [69]
$(B_9 = \mathsf{SBit} \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', B_9)|Q'))$

$b:\ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_9))$ [70]

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_9, B_9))$ [72]

$\Box\ \{D_9 \leftarrow d_7, B_9 \leftarrow b_7\}(63, 72)$

$b:\ (b_7 = \mathsf{SBit} \rightarrow$ [71]
$(\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_7)|Q'))$

$b:\ \neg(b_7 = \mathsf{SBit})$ [73]

aus EA:

$b:\ \exists B : \mathsf{SBit} = B$ [76]

$b:\ \mathsf{SBit} = b_{10}$ [77]

$\boxed{\text{LG}:\ b:\ b_7 = \mathsf{SBit}\ [74]}$

$b:\ \mathsf{RQ} = \varepsilon \vee$ [75]
$hspace2.5cm$
$\exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_7)|Q'$

$\hookrightarrow$ S. 102

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \text{ unless}^+ \mathsf{ProcAck} = \mathsf{true})$ [78]

mit Tab. 0.11, $\{B \leftarrow b_{10}\}$:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [79]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{11}, b_{11})$ [81]

$b:\ \mathsf{SBit} = b_{11}$ [82]

$\hookrightarrow$ S. 101

$a:\ \mathsf{SBit} = b_{10}$ [80]

$\Box$

$$\frac{a:\ b_1 = \mathsf{SBit}\ [31] \qquad a:\ \mathsf{SBit} = b_{10}\ [80]}{\rightarrow\ b_1 = b_{10}} \qquad \frac{a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)\ [30] \qquad a:\ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7)\ [66]}{\rightarrow\ b_1 = b_7}$$

$$\frac{b:\ \neg(b_7 = \mathsf{SBit})\ [73] \qquad b:\ \mathsf{SBit} = b_{10}\ [77]}{\rightarrow\ b_1 \neq b_7}$$

$$\vdots$$

von [82] (S. 100):

$$b:\ \mathsf{RIM} = \mathsf{msg}(d_7, b_7) \quad [63]$$
$$b:\ \neg(b_7 = \mathsf{SBit}) \quad [73]$$
$$b:\ \mathsf{SIM} = \mathsf{msg}(d_{11}, b_{11}) \quad [81]$$
$$b:\ \mathsf{SBit} = b_{11} \quad [82]$$

Induktionsvoraussetzung A1:

$$b:\ A1 \quad [13]:$$

$$\begin{aligned}
b:\ & \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow \qquad [83]\\
& (B = \mathsf{SBit} \rightarrow ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge\\
& (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge\\
& (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3))))
\end{aligned}$$

$$\begin{aligned}
b:\ & (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{12})) \rightarrow \qquad [84]\\
& (B_{12} = \mathsf{SBit} \rightarrow ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B_{12})|Q^1)) \wedge\\
& (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B_{12})) \wedge\\
& (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B_{12})|Q^3))))
\end{aligned}$$

$$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{12})) \quad [85]$$
$$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{12}, B_{12})) \quad [86]$$
$$\square\ \{D_{12} \leftarrow d_{11}, B_{12} \leftarrow b_{11}\}(81, 86)$$

[84] komplett auflösen:

$$b:\ \neg(b_{11} = \mathsf{SBit}) \quad [87]$$
$$\square\ (82, 87)$$

$$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{11})|Q^1) \quad [88]$$
$$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_{11}) \quad [89]$$
$$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_{11})|Q^3) \quad [90]$$

$$b:\ \mathsf{RIM} = \bot \quad [91]$$
$$\square\ (63, 91)$$

$$b:\ \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_{11}) \quad [92]$$
$$b:\ \mathsf{RIM} = \mathsf{msg}(d^2_{12}, b_{11}) \quad [93]$$

$$\boxed{\square \quad \begin{array}{l} b:\ \mathsf{RIM} = \mathsf{msg}(d_7, b_7) \quad [63] \\ b:\ \mathsf{RIM} = \mathsf{msg}(d^2_{12}, b_{11}) \quad [93] \\ \hline \rightarrow b_{11} = b_7 \end{array} \qquad \begin{array}{l} b:\ \neg(b_7 = \mathsf{SBit}) \quad [73] \\ b:\ \mathsf{SBit} = b_{11} \quad [82] \\ \hline \rightarrow b_{11} \neq b_7 \end{array}}$$

$\vdots$

von [75] (S. 100):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$$
$$a:\ b_1 = \mathsf{SBit} \quad [31]$$
$$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'') \quad [37]$$
$$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [40]$$
$$a:\ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7) \quad [66]$$
$$b:\ b_7 = \mathsf{SBit} \quad [74]$$
$$b:\ \mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_7)|Q' \quad [75]$$

$$b:\ \mathsf{RQ} = \varepsilon \quad [94]$$

$$b:\ \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_7)|Q' \quad [95]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9' \quad [123]$$

↪ S. 104

aus RQ:

$$b:\ \forall Q : \mathsf{RQ} = Q \to \mathsf{A}(\mathsf{RQ} = Q \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}) \quad [96]$$

mit Tab. 0.11, $\{Q \leftarrow \varepsilon\}$:

$$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true} \quad [97]$$

$$a:\ \mathsf{RQ} = \varepsilon \quad [98]$$
$\square$ (E2, 40, 98)

$$a:\ \mathsf{RecCom} = \mathsf{true} \quad [99]$$
aus Tab. 0.2:
$$b:\ \mathsf{RIM} = \bot \quad [103]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_{12}, b_{12})|q_{12} \quad [104]$$
$\square$ (E2, 94, 104)

$$a:\ \mathsf{ProcAck} = \mathsf{true} \quad [102]$$

↪ S. 103

$$a:\ \mathsf{RLose} = \mathsf{true} \quad [100]$$
aus Tab. 0.4:
$$b:\ \mathsf{RQ} \neq \varepsilon \quad [105]$$
$\square$ (94, 102)

$$a:\ \mathsf{ReTrans} = \mathsf{true} \quad [101]$$
aus Tab. 0.6:
$$b:\ \mathsf{RQ} = q_{13} \quad [106]$$
$$b:\ \mathsf{SNo} = n_{13} \quad [107]$$
$$b:\ \mathsf{SBit} = b_{13} \quad [108]$$
$$a:\ \mathsf{RQ} = q_{13}|\mathsf{msg}(\mathsf{SFile}(n_{13}), b_{13}) \quad [109]$$

$\square$

$$\frac{a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \ [30] \qquad a:\ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7) \ [66]}{\to\ b_1 = b_7} \qquad \frac{b:\ b_7 = \mathsf{SBit} \ [74] \qquad b:\ \mathsf{SBit} = b_{13} \ [108]}{\to\ b_7 = b_{13}}$$

$$\frac{b:\ \mathsf{RQ} = q_{13} \ [106] \qquad b:\ \mathsf{RQ} = \varepsilon \ [94]}{\to\ q_{13} = \varepsilon} \qquad \frac{a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'') \ [37] \qquad a:\ \mathsf{RQ} = q_{13}|\mathsf{msg}(\mathsf{SFile}(n_{13}), b_{13}) \ [109]}{\to\ b_1 \neq b_{13}}$$

$$\{D_1'' \leftarrow \mathsf{msg}(\mathsf{SFile}(n_{13}), b_{13}),\ Q_1'' \leftarrow \varepsilon\}$$

$\vdots$

von [102] (S. 102):

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ \mathsf{RQ} = \varepsilon$ [94]

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [102]

|

aus Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{14}, b_{14})$ [110]

$b:\ \mathsf{SBit} = b_{14}$ [111]

$b:\ \mathsf{RQ} = q_{15}$ [112]

$b:\ \mathsf{SNo} = n_{15}$ [113]

Linker Zweig:

$a:\ \mathsf{SFile}(s(n_{15})) = d_{16}$ [114]

$a:\ \mathsf{RQ} = q_{15}|\mathsf{msg}(\mathsf{SFile}(s(n_{15})), \mathsf{flip}(b_{14}))$ [115]

$a:\ \mathsf{SNo} = s(n_{15})$ [116]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{14})$ [117]

□ $a:\ b_1 = \mathsf{SBit}$ [31]
$a:\ \mathsf{SBit} = \mathsf{flip}(b_{14})$ [117]

$\to\ b_1 = \mathsf{flip}(b_{14})$

$b:\ \mathsf{RQ} = \varepsilon$ [94]

$b:\ \mathsf{RQ} = q_{15}$ [112]

$a:\ \mathsf{RQ} = q_{15}|\mathsf{msg}(\mathsf{SFile}(s(n_{15})), \mathsf{flip}(b_{14}))$ [115]

$\to\ a:\ \mathsf{RQ} = \mathsf{msg}(\mathsf{SFile}(s(n_{15})), \mathsf{flip}(b_{14}))$

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$\to b_1 \neq \mathsf{flip}(b_{14})$

$\{D_1'' \leftarrow \mathsf{SFile}(s(n_{15})),\ Q_1'' \leftarrow \varepsilon\}$

Rechter Zweig:

$a:\ \mathsf{SFile}(s(n_{15})) = \bot$ [118]

$a:\ \mathsf{RQ} = q_{15}$ [119]

$a:\ \mathsf{SNo} = n_{15}$ [120]

$a:\ \mathsf{SBit} = b_{14}$ [121]

$a:\ \mathsf{ready} = \mathsf{true}$ [122]

□ $b:\ \mathsf{RQ} = \varepsilon$ [94]
$b:\ \mathsf{RQ} = q_{15}$ [112]
$a:\ \mathsf{RQ} = q_{15}$ [119]

$\to\ a: \mathsf{RQ} = \varepsilon$

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$\vdots$

von [95]/[123] (S. 102):

$a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a: \ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b: \ \mathsf{RIM} = \mathsf{msg}(d_7, b_7)$ [63]

$a: \ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7)$ [66]

$b: \ b_7 = \mathsf{SBit}$ [74]

$b: \ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9'$ [123]

$b: \ \forall Q: \mathsf{RQ} = Q \rightarrow \mathsf{A}(\mathsf{RQ} = Q \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [124]

mit Tab. 0.11, $\{Q \leftarrow \mathsf{msg}(d_9', b_7)|q_9'\}$:

$a: \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}$ [125]

$a: \ \mathsf{RecCom} = \mathsf{true}$ [127]

aus Tab. 0.2:

$b: \ \mathsf{RIM} = \bot$ [131]

$\square$ $(E3, 63, 131)$

$a: \ \mathsf{RLose} = \mathsf{true}$ [128]

$\hookrightarrow$ S. 105

$a: \ \mathsf{ReTrans} = \mathsf{true}$ [129]

aus Tab. 0.6:

$b: \ \mathsf{RQ} = q_{19}$ [143]

$b: \ \mathsf{SNo} = n_{19}$ [144]

$b: \ \mathsf{SBit} = b_{19}$ [145]

$a: \ \mathsf{RQ} = q_{19}|\mathsf{msg}(\mathsf{SFile}(n_{19}), b_{19})$ [146]

$\square$ $a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a: \ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7)$ [66]

$\rightarrow \ b_1 = b_7$

$b: \ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9'$ [123]

$b: \ \mathsf{RQ} = q_{19}$ [143]

$a: \ \mathsf{RQ} = q_{19}|\mathsf{msg}(\mathsf{SFile}(n_{19}), b_{19})$ [146]

$\rightarrow a: \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9'|\mathsf{msg}(\mathsf{SFile}(n_{19}), b_{19})$

$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$\rightarrow \ b_7 \neq b_1$

$\{D_1'' \leftarrow d_9', \ Q_1'' \leftarrow q_9'|\mathsf{msg}(\mathsf{SFile}(n_{19}), b_{19})$

$a: \ \mathsf{ProcAck} = \mathsf{true}$ [130]

$\hookrightarrow$ S. 107

$a: \ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9'$ [126]

$\square$ $a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a: \ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7)$ [66]

$\rightarrow \ b_1 = b_7$

$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a: \ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9'$ [126]

$\rightarrow \ b_1 \neq b_7$

$\{D_1'' \leftarrow d_9', \ Q_1'' \leftarrow q_9'\}$

$$\vdots$$

von [128] (S. 104):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)\quad [30]$$
$$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')\quad [37]$$
$$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2\quad [40]$$
$$a:\ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7)\quad [66]$$
$$b:\ b_7 = \mathsf{SBit}\quad [74]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9'\quad [123]$$
$$a:\ \mathsf{RLose} = \mathsf{true}\quad [128]$$

mit Tab. 0.3:

$$b:\ \mathsf{RQ} \neq \varepsilon\quad [132]$$

$$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_{17}, B_{17})|Q_{17})\quad [133]$$
$$\Box\ \{D_{17} \leftarrow d_2,\ B_{17} \leftarrow b_2,\ Q_{17} \leftarrow q_2\}(40, 133)$$

D_{17}, B_{17}, Q_{17} einsetzen:

$$b:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_{17}'\quad [134]$$

$$\Box\ a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)\quad [30]$$
$$a:\ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7)\quad [66]$$
$$\rightarrow\ b_1 = b_7$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_{17}'\quad [134]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9'\quad [123]$$
$$\rightarrow\ b_2 = b_7$$
$$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')\quad [37]$$
$$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2\quad [40]$$
$$\rightarrow\ b_1 \neq b_2$$
$$\{D_1'' \leftarrow d_1,\ Q_1'' \leftarrow q_2\}$$

$$b:\ \mathsf{RQ} = \mathsf{msg}(d_{17}', b_{17}')|\mathsf{msg}(d_2, b_2)|q_2\quad [135]$$

$\hookrightarrow$ S. 106

$\vdots$

von [135] (S. 105):

$a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$

$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'') \quad [37]$

$a: \ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [40]$

$a: \ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7) \quad [66]$

$b: \ b_7 = \mathsf{SBit} \quad [74]$

$b: \ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9' \quad [123]$

$b: \ \mathsf{RQ} = \mathsf{msg}(d_{17}', b_{17}')|\mathsf{msg}(d_2, b_2)|q_2 \quad [135]$

Ind.Vor. A5:

$b: \ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}) \quad [136]$

$b: \ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{18})|Q'|\mathsf{msg}(D', B_{18}')|Q'') \rightarrow (B_{18} = \mathsf{SBit} \rightarrow B_{18}' = \mathsf{SBit}) \quad [137]$

$b: \ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{18})|Q'\mathsf{msg}(D', B_{18}')|Q'') \quad [138]$

$b: \ \neg(\mathsf{RQ} = Q_{18}|\mathsf{msg}(D_{18}, B_{18})|Q_{18}'\mathsf{msg}(D_{18}', B_{18}')|Q_{18}'') \quad [140]$

$\square \ \{Q_{18}, Q_{18}' \leftarrow \varepsilon, \ D_{18} \leftarrow d_{17}', \ B_{18} \leftarrow b_{17}', D_{18}' \leftarrow d_2, \ B_{18}' \leftarrow b_2, \ Q_{18}'' \leftarrow q_2\}$

$(135, 140)$

$B_{18}, \ B_{18}'$ einsetzen:

$b: \ b_{17}' = \mathsf{SBit} \rightarrow b_2 = \mathsf{SBit} \quad [139]$

$b: \ \neg(b_{17}' = \mathsf{SBit}) \quad [141]$

$\square \ b: \ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9' \quad [123]$

$b: \ \mathsf{RQ} = \mathsf{msg}(d_{17}', b_{17}')|\mathsf{msg}(d_2, b_2)|q_2 \quad [135]$

$\rightarrow \ b_7 = b_{17}'$

$b: \ b_7 = \mathsf{SBit} \quad [74]$

$b: \ \neg(b_{17}' = \mathsf{SBit}) \quad [141]$

$\rightarrow \ b_7 \neq b_{17}'$

$b: \ b_2 = \mathsf{SBit} \quad [142]$

$\square \ a: \ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$

$a: \ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7) \quad [66]$

$\rightarrow \ b_1 = b_7$

$b: \ b_2 = \mathsf{SBit} \quad [142]$

$b: \ b_7 = \mathsf{SBit} \quad [74]$

$\rightarrow \ b_2 = b_7$

$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'') \quad [37]$

$a: \ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [40]$

$\rightarrow \ b_1 \neq b_2$

$\{D_1'' \leftarrow d_1, \ Q_1'' \leftarrow q_2\}$

$\vdots$

von [130] (S. 104):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a:\ \mathsf{SQ} = q_8|\mathsf{msg}(\lambda, b_7)$ [66]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)|q_9'$ [123]

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [130]

|

aus Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{20}, b_{20})$ [147]

$b:\ \mathsf{SBit} = b_{20}$ [148]

$b:\ \mathsf{RQ} = q_{21}$ [149]

$b:\ \mathsf{SNo} = n_{21}$ [150]

Linker Zweig:

$a:\ \mathsf{SFile}(s(n_{21})) = d_{22}$ [151]

$a:\ \mathsf{RQ} = q_{21}|\mathsf{msg}(\mathsf{SFile}(s(n_{21})), \mathsf{flip}(b_{20}))$ [152]

$a:\ \mathsf{SNo} = s(n_{21})$ [153]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{20})$ [154]

□ $a:\ \mathsf{SQ} = q_1\|\mathsf{msg}(d_1, b_1)$ [30]
$a:\ \mathsf{SQ} = q_8\|\mathsf{msg}(\lambda, b_7)$ [66]
$\rightarrow\ b_1 = b_7$
$b:\ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)\|q_9'$ [123]
$b:\ \mathsf{RQ} = q_{21}$ [149]
$a:\ \mathsf{RQ} = q_{21}\|\mathsf{msg}(\mathsf{SFile}(s(n_{21})), \mathsf{flip}(b_{20}))$ [152]
$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)\|Q_1'')$ [37]
$\rightarrow\ b_1 \neq b_7$
$\{D_1'' \leftarrow d_9',\ Q_1'' \leftarrow q_9'\|\mathsf{msg}(\mathsf{SFile}(s(n_{21})), \mathsf{flip}(b_{20}))\}$

Rechter Zweig:

$a:\ \mathsf{SFile}(s(n_{21})) = \bot$ [155]

$a:\ \mathsf{RQ} = q_{21}$ [156]

$a:\ \mathsf{SNo} = n_{21}$ [157]

$a:\ \mathsf{SBit} = b_{20}$ [158]

$a:\ \mathsf{ready} = \mathsf{true}$ [159]

□ $a:\ \mathsf{SQ} = q_1\|\mathsf{msg}(d_1, b_1)$ [30]
$a:\ \mathsf{SQ} = q_8\|\mathsf{msg}(\lambda, b_7)$ [66]
$\rightarrow\ b_1 = b_7$
$b:\ \mathsf{RQ} = \mathsf{msg}(d_9', b_7)\|q_9'$ [123]
$b:\ \mathsf{RQ} = q_{21}$ [149]
$a:\ \mathsf{RQ} = q_{21}$ [156]
$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)\|Q_1'')$ [37]
$\rightarrow\ b_1 \neq b_7$
$\{D_1'' \leftarrow d_9',\ Q_1'' \leftarrow q_9'\}$

$\vdots$

von [166] (S. 98):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ \neg(\mathsf{SQ} = Q_3|\mathsf{msg}(D_3, B_3))$ [46]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)$ [160]

$b:\ \neg(b_5 = \mathsf{SBit})$ [161]

$b:\ \mathsf{SBit} = b_{23}$ [166]

|

wie [74] ff. der ersten Teilaussage von A3 (S.84) mit

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)$ [160]

$b:\ \neg(b_5 = \mathsf{SBit})$ [161]

$b:\ \mathsf{SBit} = b_{23}$ [166]

Da man keine [A3.1.41] entsprechende Formel hat, muß man bei [A3.1.104]/[A3.1.128] (Anwendung von AckMsg) anders abschließen.

Die einzige auf dem Weg zu [A3.1.104] dazukommende relevante Formel ist [A3.1.76], daß $\mathsf{SBit}_a = \mathsf{SBit}_b$ ist. Diese Information wird übernommen:

$\vdots$

entspr. [A3.76]:

$a:\ \mathsf{SBit} = b_{23}$ [167]

$\vdots$

entspr. [A3.104]:

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [168]

|

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})$ [169]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{24})$ [170]

$b:\ \mathsf{SQ} = q_{25}$ [171]

$a:\ \mathsf{SQ} = q_{25}|\mathsf{msg}(\lambda, b_{24})$ [172]

$a:\ \mathsf{RIM} = \perp$ [173]

$\hookrightarrow$ S. 109

$\vdots$

von [173] (S. 108):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D''_1, b_1)|Q''_1)$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$a:\ \mathsf{SBit} = b_{23}$ [63]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})$ [169]

$a:\ \mathsf{SQ} = q_{25}|\mathsf{msg}(\lambda, b_{24})$ [172]

$a:\ \mathsf{RIM} = \perp$ [173]

Induktionsvoraussetzung A4:

$b:\ A4$ [16]

$b:\ \forall B : (\exists D : \mathsf{RIM} = \mathsf{msg}(D, B)) \rightarrow$ [174]
$(B = \mathsf{SBit} \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', B)|Q'))$

$b:\ (\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{26})) \rightarrow$ [175]
$(B_{26} = \mathsf{SBit} \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', B_{26})|Q'))$

$b:\ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{26}))$ [176]

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{26}, B_{26}))$ [178]

$\square\ \{D_{26} \leftarrow d_{24}, B_{26} \leftarrow b_{24}\}(169, 178)$

$b:\ (b_{24} = \mathsf{SBit} \rightarrow$ [177]
$(\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_{24})|Q'))$

$b:\ \neg(b_{24} = \mathsf{SBit})$ [179]

$\square\ a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]
$a:\ \mathsf{SQ} = q_{25}|\mathsf{msg}(\lambda, b_{24})$ [172]
$\rightarrow\ b_1 = b_{24}$
$a:\ b_1 = \mathsf{SBit}$ [31]
$a:\ \mathsf{SBit} = b_{23}$ [63]
$\rightarrow\ b_1 = b_{23}$
$b:\ \mathsf{SBit} = b_{23}$ [166]
$b:\ \neg(b_{24} = \mathsf{SBit})$ [179]
$\rightarrow\ b_{23} \neq b_{24}$

LG : $b:\ \mathsf{SBit} = b_{24}$ [180]

$b:\ \mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_{24})|Q'$ [181]

wie [75] (S.102), mit
$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]
$a:\ b_1 = \mathsf{SBit}$ [31]
$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D''_1, b_1)|Q''_1)$ [37]
$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]
$b:\ \mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})$ [169]
$a:\ \mathsf{SQ} = q_{25}|\mathsf{msg}(\lambda, b_{24})$ [172]
$b:\ \mathsf{SBit} = b_{24}$ [180]
$b:\ \mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_{24})|Q'$ [181]

$\vdots$

von [164] (S. 98):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)$ [160]

$b:\ b_5 = \mathsf{SBit}$ [162]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_5)|Q'')$ [164]

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \text{ unless}^+ \mathsf{ProcAck} = \mathsf{true})$ [182]

mit Tab. 0.11, $\{B \leftarrow b_5\}$:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [183]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{27}, b_{27})$ [186]

$b:\ \mathsf{SBit} = b_{27}$ [187]

$b:\ \mathsf{RQ} = q_{28}$ [188]

$b:\ \mathsf{SNo} = n_{28}$ [189]

$a:\ \mathsf{SFile}(s(n_{28})) = d_{29}$ [190]

$a:\ \mathsf{RQ} = q_{28}|\mathsf{msg}(\mathsf{SFile}(s(n_{28})), \mathsf{flip}(b_{27}))$ [191]

$a:\ \mathsf{SNo} = s(n_{28})$ [192]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27})$ [193]

aus SQ:

$b:\ \forall Q : \mathsf{SQ} = Q \rightarrow \mathsf{A}(\mathsf{SQ} = Q \text{ unless}^+ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [199]

aus Tab. 0.11, $\{Q \leftarrow \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)\}$ aus [160]:

$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [200]

$a:\ \mathsf{SendCom} = \mathsf{true}$ [202]

$\hookrightarrow$ S. 111

$a:\ \mathsf{SLose} = \mathsf{true}$ [203]

$\hookrightarrow$ S. 112

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [204]

$\hookrightarrow$ S. 115

$a:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)$ [201]

$\square$ $a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)$ [201]

$\rightarrow b_1 = b_5$

$b:\ b_5 = \mathsf{SBit}$ [162]

$b:\ \mathsf{SBit} = b_{27}$ [187]

$\rightarrow b_5 = b_{27}$

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27})$ [193]

$\rightarrow b_5 = \mathsf{flip}(b_{27})$

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [184]

$a:\ \mathsf{SBit} = b_5$ [186]

$\hookrightarrow$ S. 116

$a:\ \mathsf{SFile}(s(n_{28})) = \perp$ [194]

$a:\ \mathsf{RQ} = q_{28}$ [195]

$a:\ \mathsf{SNo} = n_{28}$ [196]

$a:\ \mathsf{SBit} = b_{27}$ [197]

$a:\ \mathsf{ready} = \mathsf{true}$ [198]

Abschluß wie [184], da SBit unverändert, nur die Fälle, wo RQ ebenfalls unverändert.

$$\vdots$$

von [202] (S. 110):

$$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30]$$
$$a:\ b_1 = \mathsf{SBit} \quad [31]$$
$$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5) \quad [160]$$
$$b:\ b_5 = \mathsf{SBit} \quad [162]$$
$$b:\ \mathsf{SBit} = b_{27} \quad [187]$$
$$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27}) \quad [193]$$
$$a:\ \mathsf{SendCom} = \mathsf{true} \quad [202]$$

$$|$$

aus Tab. 0.1:

$$b:\ \mathsf{SIM} = \bot \quad [205]$$
$$b:\ \mathsf{SQ} = \mathsf{msg}(d_{30}, b_{30})|q_{30} \quad [206]$$
$$a:\ \mathsf{SQ} = q_{30} \quad [207]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_{30}, b_{30}) \quad [208]$$

$$|$$

Fallunterscheidung mit Q4:

$$b:\ \forall Q, Q' : (\exists D, B : Q = Q'|\mathsf{msg}(D, B)) \rightarrow Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = \mathsf{msg}(D', B')|Q'') \quad [209]$$
$$b:\ (\exists D, B : Q_{31} = Q'_{31}\mathsf{msg}(D, B)) \rightarrow Q'_{31} = \varepsilon \vee (\exists D', B', Q'' : Q'_{31} = \mathsf{msg}(D', B')|Q'') \quad [210]$$

$$b:\ \neg(\exists D, B : Q_{31} = Q'_{31}|\mathsf{msg}(D, B)) \quad [211]$$
$$b:\ \neg(Q_{31} = Q'_{31}|\mathsf{msg}(D_{31}, B_{31})) \quad [213]$$
$$\Box\ \{Q_{31} \leftarrow \mathsf{SQ},\ Q'_{31} \leftarrow q_4\}(160, 213)$$

$$b:\ q_4 = \varepsilon \vee (\exists D', B', Q'' : q_4 = \mathsf{msg}(D', B')|Q'') \quad [212]$$

$$b:\ q_4 = \varepsilon \quad [214]$$

$$\begin{array}{l}
b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5) \quad [160] \\
b:\ q_4 = \varepsilon \quad [214] \\
\hline
\rightarrow b:\ \mathsf{SQ} = \mathsf{msg}(d_4, b_5) \\
b:\ \mathsf{SQ} = \mathsf{msg}(d_{30}, b_{30})|q_{30} \quad [206] \\
\hline
\rightarrow q_{30} = \varepsilon \\
a:\ \mathsf{SQ} = q_{30} \quad [207] \\
a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30] \\
\Box\ \mathrm{E2}
\end{array}$$

$$b:\ \exists D', B', Q'' : q_4 = \mathsf{msg}(D', B')|Q'' \quad [215]$$
$$b:\ q_4 = \mathsf{msg}(d'_{31}, b'_{31})|q''_{31} \quad [216]$$

$$\begin{array}{l|l}
\Box\ a:\ b_1 = \mathsf{SBit} \quad [31] & b:\ q_4 = \mathsf{msg}(d'_{31}, b'_{31})|q''_{31} \quad [216] \\
a:\ \mathsf{SBit} = \mathsf{flip}(b_{27}) \quad [193] & b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5) \quad [160] \\
\hline
\rightarrow b_1 = \mathsf{flip}(b_{27}) & b:\ \mathsf{SQ} = \mathsf{msg}(d_{30}, b_{30})|q_{30} \quad [206] \\
\hline
b:\ b_5 = \mathsf{SBit} \quad [162] & \rightarrow q_{30} = q''_{31}|\mathsf{msg}(d_4, b_5) \\
b:\ \mathsf{SBit} = b_{27} \quad [187] & a:\ \mathsf{SQ} = q_{30} \quad [207] \\
\hline
\rightarrow b_5 = b_{27} & a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1) \quad [30] \\
\hline
 & \rightarrow b_1 = b_5
\end{array}$$

$\vdots$

von [203] (S. 110):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)$ [160]

$b:\ b_5 = \mathsf{SBit}$ [162]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{27}, b_{27})$ [186]

$b:\ \mathsf{SBit} = b_{27}$ [187]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27})$ [193]

$a:\ \mathsf{SLose} = \mathsf{true}$ [203]

aus Tab. 0.3:

$b:\ \mathsf{SQ} \neq \varepsilon$ [217]

$a:\ \neg(\mathsf{SQ} = Q_{32}|\mathsf{msg}(D_{32}, B_{32})|Q'_{32})$ [218]

$\Box\ \{Q_{32} \leftarrow q_1, D_{32} \leftarrow d_1, B_{32} \leftarrow b_1, Q'_{32} \leftarrow \varepsilon\}(30, 218)$

$b:\ \mathsf{SQ} = r_{32}|\mathsf{msg}(d_1, b_1)|r'_{32}$ [219]

Induktionsvoraussetzung A1:

$b:\ A1$ [13] :

$$b:\ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow \quad [220]$$
$$(B = \mathsf{SBit} \rightarrow \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge$$
$$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3))))$$

$$b:\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{33})) \rightarrow \quad [221]$$
$$(B_{33} = \mathsf{SBit} \rightarrow \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B_{33})|Q^1)) \wedge$$
$$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B_{33})) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B_{33})|Q^3))))$$

$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{33}))$ [222]

$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{33}, B_{33}))$ [223]

$\Box\ \{D_{33} \leftarrow d_{27}, B_{33} \leftarrow b_{27}\}(186, 223)$

[221] komplett auflösen:

$b:\ \neg(b_{27} = \mathsf{SBit})$ [224]

$\Box\ (187, 224)$

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{27})|Q^1)$ [225]

$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_{27})$ [226]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_{27})|Q^3)$ [227]

$\hookrightarrow$ S. 113

$\vdots$

von [227] (S. 112):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)$ [160]

$b:\ b_5 = \mathsf{SBit}$ [162]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{27}, b_{27})$ [186]

$b:\ \mathsf{SBit} = b_{27}$ [187]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27})$ [193]

$b:\ \mathsf{SQ} = r_{32}|\mathsf{msg}(d_1, b_1)|r'_{32}$ [219]

$b:\ \mathsf{SQ} = \varepsilon \lor (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{27})|Q^1)$ [225]

$b:\ \mathsf{SQ} = \varepsilon$ [228]

$\square$ $(219, 228)$

$b:\ \exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{27})|Q^1$ [229]

$b:\ \mathsf{SQ} = \mathsf{msg}(d^1_{32}, b_{27})|q^1_{32}$ [230]

Fallunterscheidung: Q4:

$b:\ \forall Q, Q' : (\exists D, B : Q = Q'|\mathsf{msg}(D, B)) \to Q' = \varepsilon \lor (\exists D', B', Q'' : Q' = \mathsf{msg}(D', B')|Q'')$ [231]

$b:\ (\exists D, B : Q_{35} = Q'_{35}|\mathsf{msg}(D, B)) \to Q' = \varepsilon \lor (\exists D', B', Q'' : Q'_{35} = \mathsf{msg}(D', B')|Q'')$ [232]

$b:\ \neg(\exists D, B : Q_{35} = Q'_{35}|\mathsf{msg}(D, B))$ [233]

$b:\ \neg(Q_{35} = Q'_{35}|\mathsf{msg}(D_{35}, B_{35}))$ [235]

$\square$ $\{Q_{35} \leftarrow r_{32}|\mathsf{msg}(d_1, b_1), Q'_{35} \leftarrow r_{32}\}(219, 235)$

$b:\ r_{32} = \varepsilon \lor (\exists D', B', Q'' : r_{32} = \mathsf{msg}(D', B')|Q'')$ [234]

$b:\ r_{32} = \varepsilon$ [236]

$\square$ $b:\ \mathsf{SQ} = r_{32}|\mathsf{msg}(d_1, b_1)|r'_{32}$ [219]
$b:\ r_{32} = \varepsilon$ [236]
$b:\ \mathsf{SQ} = \mathsf{msg}(d^1_{32}, b_{27})|q^1_{32}$ [230]

$\to\ b_1 = b_{27}$

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27})$ [193]

$\to\ b_1 = \mathsf{flip}(b_{27})$

$b:\ \exists D', B', Q'' : r_{32} = \mathsf{msg}(D', B')|Q''$ [237]

$b:\ r_{32} = \mathsf{msg}(d'_{35}, b'_{35})|q''_{35}$ [238]

$\hookrightarrow$ S. 114

$\vdots$

von [238] (S. 113):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$b:\ \mathsf{SQ} = q_4|\mathsf{msg}(d_4, b_5)$ [160]

$b:\ b_5 = \mathsf{SBit}$ [162]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{27}, b_{27})$ [186]

$b:\ \mathsf{SBit} = b_{27}$ [187]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27})$ [193]

$b:\ \mathsf{SQ} = r_{32}|\mathsf{msg}(d_1, b_1)|r'_{32}$ [219]

$b:\ \mathsf{SQ} = \mathsf{msg}(d^1_{32}, b_{27})|q^1_{32}$ [230]

$b:\ r_{32} = \mathsf{msg}(d'_{35}, b'_{35})|q''_{35}$ [238]

|

Induktionsvoraussetzung A2:

$b:\ A2$ [14] :

$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \to (B = \mathsf{SBit} \to B' = \mathsf{SBit})$ [239]

|

$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{36})|Q'|\mathsf{msg}(D', B'_{36})|Q'') \to (B_{36} = \mathsf{SBit} \to B'_{36} = \mathsf{SBit})$ [240]

$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{36})|Q'|\mathsf{msg}(D', B'_{36})|Q'')$ [241]

$b:\ \neg(\mathsf{SQ} = Q_{36}|\mathsf{msg}(D_{36}, B_{36})|Q'_{36}|\mathsf{msg}(D'_{36}, B'_{36})|Q''_{36})$ [243]

$\Box\ \{\ Q_{36} \leftarrow \varepsilon, D_{36} \leftarrow d'_{35}, B_{36} \leftarrow b'_{35}$

$Q'_{36} \leftarrow q''_{35}, D'_{36} \leftarrow d_1, B'_{36} \leftarrow b_1, Q''_{36} \leftarrow r'_{32}\}(219, 238, 243)$

$b:\ b'_{35} = \mathsf{SBit} \to b_1 = \mathsf{SBit}$ [242]

$b:\ \neg(b'_{35} = \mathsf{SBit})$ [244]

$\Box$ $b:\ \mathsf{SQ} = r_{32}\|\mathsf{msg}(d_1, b_1)\|r'_{32}$ [219]
$b:\ r_{32} = \mathsf{msg}(d'_{35}, b'_{35})\|q''_{35}$ [238]
$b:\ \mathsf{SQ} = \mathsf{msg}(d^1_{32}, b_{27})\|q^1_{32}$ [230]
$\to\ b'_{35} = b_{27}$
$b:\ \mathsf{SBit} = b_{27}$ [187]
$b:\ \neg(b'_{35} = \mathsf{SBit})$ [244]
$\to\ b_{27} \neq b'_{35}$

$b:\ b_1 = \mathsf{SBit}$ [245]

$\Box$ $a:\ b_1 = \mathsf{SBit}$ [31]
$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27})$ [193]
$\to\ b_1 = \mathsf{flip}(b_{27})$
$b:\ b_1 = \mathsf{SBit}$ [245]
$b:\ \mathsf{SBit} = b_{27}$ [187]
$\to\ b_1 = b_{27}$

$$\vdots$$

von [204] (S. 110):

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ b_1 = \mathsf{SBit}$ [31]

$b:\ b_5 = \mathsf{SBit}$ [162]

$b:\ \mathsf{RIM} = \perp \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_5)$ [163]

$b:\ \mathsf{SBit} = b_{27}$ [187]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27})$ [193]

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [204]

|

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{37}, b_{37})$ [246]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{37})$ [247]

$b:\ \mathsf{SQ} = q_{38}$ [248]

$a:\ \mathsf{SQ} = q_{38}|\mathsf{msg}(\lambda, b_{37})$ [249]

$a:\ \mathsf{RIM} = \perp$ [250]

|

aus [163]:

Linker Zweig:

$b:\ \mathsf{RIM} = \perp$ [251]

$\square$ (E3, 246, 251)

Rechter Zweig:

$b:\ \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_5)$ [252]

$b:\ \mathsf{RIM} = \mathsf{msg}(d'_{39}, b_5)$ [253]

$\square$ $b:\ \mathsf{RIM} = \mathsf{msg}(d'_{39}, b_5)$ [253]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{37}, b_{37})$ [246]

$\rightarrow\ b_5 = b_{37}$

$b:\ b_5 = \mathsf{SBit}$ [162]

$b:\ \mathsf{SBit} = b_{27}$ [187]

$\rightarrow\ b_5 = b_{27}$

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{27})$ [193]

$\rightarrow\ b_1 = \mathsf{flip}(b_{27})$

$a:\ \mathsf{SQ} = q_1|\mathsf{msg}(d_1, b_1)$ [30]

$a:\ \mathsf{SQ} = q_{38}|\mathsf{msg}(\lambda, b_{37})$ [249]

$\rightarrow\ b_1 = b_{37}$

$\vdots$

von [185] (S. 110):

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ b_5 = \mathsf{SBit}$ [162]

$b:\ \mathsf{RQ} = \varepsilon \lor (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_5)|Q'')$ [164]

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [184]

$a:\ \mathsf{SBit} = b_5$ [185]

aus [164]:

$b:\ \mathsf{RQ} = \varepsilon$ [254]

$b:\ \exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_5)|Q''$ [255]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}''$ [270]

$\hookrightarrow$ S. 117

aus RQ:

$b:\ \forall Q : \mathsf{RQ} = Q \to \mathsf{A}(\mathsf{RQ} = Q \ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [256]

mit Tab. 0.11, $\{Q \leftarrow \varepsilon\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true}$ [257]

$a:\ \mathsf{RQ} = \varepsilon$ [258]

$\square$ (E2, 40, 258)

$a:\ \mathsf{RecCom} = \mathsf{true}$ [259]

aus Tab. 0.2:

$b:\ \mathsf{RIM} = \bot$ [263]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{39}, b_{39})|q_{39}$ [264]

$\square$ (E2, 254, 264)

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [262]

$\square$ (184, 262)

$a:\ \mathsf{RLose} = \mathsf{true}$ [260]

aus Tab. 0.4:

$b:\ \mathsf{RQ} \neq \varepsilon$ [265]

$\square$ (254, 265)

$a:\ \mathsf{ReTrans} = \mathsf{true}$ [261]

aus Tab. 0.6:

$b:\ \mathsf{RQ} = q_{40}$ [266]

$b:\ \mathsf{SNo} = n_{40}$ [267]

$b:\ \mathsf{SBit} = b_{40}$ [268]

$a:\ \mathsf{RQ} = q_{40}|\mathsf{msg}(\mathsf{SFile}(n_{40}), b_{40})$ [269]

$$\boxed{\begin{array}{ll}
\square\ \begin{array}{l} a:\ b_1 = \mathsf{SBit}\ \ [31] \\ \underline{a:\ \mathsf{SBit} = b_5\ \ [185]} \\ \to b_1 = b_5 \end{array} & \begin{array}{l} b:\ b_5 = \mathsf{SBit}\ \ [162] \\ \underline{b:\ \mathsf{SBit} = b_{40}\ \ [268]} \\ \to b_5 = b_{40} \end{array} \\
\begin{array}{l} b:\ \mathsf{RQ} = q_{40}\ \ [265] \\ \underline{b:\ \mathsf{RQ} = \varepsilon\ \ [254]} \\ \to\ q_{40} = \varepsilon \end{array} & \begin{array}{l} a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')\ \ [37] \\ \underline{a:\ \mathsf{RQ} = q_{40}|\mathsf{msg}(\mathsf{SFile}(n_{40}), b_{40})\ \ [269]} \\ \to\ b_1 \neq b_{40} \end{array} \\
\{D_1'' \leftarrow \mathsf{msg}(\mathsf{SFile}(n_{40}), b_{40}),\ Q_1'' \leftarrow \varepsilon\} &
\end{array}}$$

$\vdots$

von [270] (S. 116):

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ b_5 = \mathsf{SBit}$ [162]

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [184]

$a:\ \mathsf{SBit} = b_5$ [185]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}''$ [270]

aus RQ:

$b:\ \forall Q : \mathsf{RQ} = Q \to \mathsf{A}(\mathsf{RQ} = Q\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [271]

mit Tab. 0.11, $\{Q \leftarrow \mathsf{msg}(d_{41}'', b_5)|q_{41}''\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true}$ [272]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}''$ [273]

□ $a:\ b_1 = \mathsf{SBit}$ [31]
$a:\ \mathsf{SBit} = b_5$ [185]
$\to b_1 = b_5$
$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]
$a:\ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}''$ [273]
$\to b_1 \neq b_5$
$\{D_1'' \leftarrow d_{41}'',\ Q_1'' \leftarrow q_{41}''\}$

$a:\ \mathsf{RecCom} = \mathsf{true}$ [274]

aus Tab. 0.2:

$b:\ \mathsf{RIM} = \perp$ [278]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{42}, b_{42})|q_{42}$ [279]

$a:\ \mathsf{RQ} = q_{42}$ [280]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_{42}, b_{42})$ [281]

↪ S. 118

$a:\ \mathsf{RLose} = \mathsf{true}$ [275]

↪ S. 119

$a:\ \mathsf{ReTrans} = \mathsf{true}$ [276]

aus Tab. 0.6:

$b:\ \mathsf{RQ} = q_{40}$ [300]

$b:\ \mathsf{SNo} = n_{40}$ [301]

$b:\ \mathsf{SBit} = b_{40}$ [302]

$a:\ \mathsf{RQ} = q_{40}|\mathsf{msg}(\mathsf{SFile}(n_{40}), b_{40})$ [303]

□ $b:\ b_5 = \mathsf{SBit}$ [162]
$b:\ \mathsf{SBit} = b_{40}$ [268]
$\to b_5 = b_{40}$
$a:\ b_1 = \mathsf{SBit}$ [31]
$a:\ \mathsf{SBit} = b_5$ [185]
$\to b_1 = b_5$
$b:\ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}''$ [270]
$b:\ \mathsf{RQ} = q_{40}$ []
$a:\ \mathsf{RQ} = q_{40}|\mathsf{msg}(\mathsf{SFile}(n_{40}), b_{40})$ [303]
$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]
$\to b_5 \neq b_1$
$\{D_1'' \leftarrow d_{41}'',\ Q_1'' \leftarrow q_{41}''\}$

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [277]

□ (184, 277)

$\vdots$

von [281] (S. 117):

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ b_5 = \mathsf{SBit}$ [162]

$a:\ \mathsf{SBit} = b_5$ [185]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}''$ [270]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{42}, b_{42})|q_{42}$ [279]

$a:\ \mathsf{RQ} = q_{42}$ [280]

Induktionsvoraussetzung A5:

$b:\ A2$ [17] :

$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'') \to (B = \mathsf{SBit} \to B' = \mathsf{SBit})$ [282]

$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B_{43})|Q'|\mathsf{msg}(D',B_{43}')|Q'') \to (B_{43} = \mathsf{SBit} \to B_{43}' = \mathsf{SBit})$ [283]

$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{SQ} = Q|\mathsf{msg}(D,B_{43})|Q'|\mathsf{msg}(D',B_{43}')|Q'')$ [284]

$b:\ \neg(\mathsf{SQ} = Q_{43}|\mathsf{msg}(D_{43},B_{43})|Q_{43}'|\mathsf{msg}(D_{43}',B_{43}')|Q_{43}'')$ [286]

☐ $a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]
$a:\ \mathsf{RQ} = q_{42}$ [280]
$b:\ \mathsf{RQ} = \mathsf{msg}(d_{42}, b_{42})|q_{42}$ [279]

$\to\ b:\ \mathsf{RQ} = \mathsf{msg}(d_{42}, b_{42})|\mathsf{msg}(d_2, b_2)|q_2$
$b:\ \neg(\mathsf{SQ} = Q_{43}|\mathsf{msg}(D_{43},B_{43})|Q_{43}'|\mathsf{msg}(D_{43}',B_{43}')|Q_{43}'')$ [286]
$\{Q_{43} \leftarrow, Q_{43}' \leftarrow \varepsilon, D_{43} \leftarrow d_{42}, B_{43} \leftarrow b_{42},$
$D_{43}' \leftarrow d_2, B_{43}' \leftarrow b_2, Q_{43}'' \leftarrow q_2\}$

$b:\ b_{42} = \mathsf{SBit} \to b_2 = \mathsf{SBit}$ [285]

$b:\ \neg(b_{42} = \mathsf{SBit})$ [287]

☐ $b:\ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}''$ [270]
$b:\ \mathsf{RQ} = \mathsf{msg}(d_{42}, b_{42})|q_{42}$ [279]

$\to\ b_5 = b_{42}$
$b:\ \neg(b_{42} = \mathsf{SBit})$ [287]
$b:\ b_5 = \mathsf{SBit}$ [162]

$\to\ b_5 \neq b_{42}$

$b:\ b_2 = \mathsf{SBit}$ [288]

☐ $b:\ b_2 = \mathsf{SBit}$ [288] $\quad$ $a:\ b_1 = \mathsf{SBit}$ [31]
$b:\ b_5 = \mathsf{SBit}$ [162] $\quad$ $a:\ \mathsf{SBit} = b_5$ [185]

$\to\ b_2 = b_5$ $\quad$ $\to\ b_1 = b_5$
$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]
$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$\to\ b_1 \neq b_5$
$\{D_1'' \leftarrow d_1, Q_1'' \leftarrow q_2\}$

$\vdots$

von [275] (S. 117):

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ b_5 = \mathsf{SBit}$ [162]

$a:\ \mathsf{SBit} = b_5$ [185]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}''$ [270]

$a:\ \mathsf{RLose} = \mathsf{true}$ [275]

|

$b:\ \mathsf{SQ} \neq \varepsilon$ [289]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_{44}, B_{44})|Q_{44}))$ [290]

$\square\ \{D_{44} \leftarrow d_2,\ B_{44} \leftarrow b_2,\ Q_{44} \leftarrow q_2\}(40, 166)$

$b:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_{44}'$ [291]

$\square\ b:\ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}''$ [270]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_{44}'$ [291]

$\rightarrow b_2 = b_5$

$a:\ b_1 = \mathsf{SBit}$ [31]

$a:\ \mathsf{SBit} = b_5$ [185]

$\rightarrow b_1 = b_5$

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$\rightarrow b_1 \neq b_2$

$\{D_1' \leftarrow d_2,\ Q_1' \leftarrow q_2\}$

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{44}', b_{44}')|\mathsf{msg}(d_2, b_2)|q_2$ [292]

$\hookrightarrow$ S. 120

$\vdots$

von [292] (S. 119):

$$a: \ b_1 = \mathsf{SBit} \quad [31]$$

$$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_1'', b_1)|Q_1'') \quad [37]$$

$$a: \ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [40]$$

$$b: \ b_5 = \mathsf{SBit} \quad [162]$$

$$a: \ \mathsf{SBit} = b_5 \quad [185]$$

$$b: \ \mathsf{RQ} = \mathsf{msg}(d_{41}'', b_5)|q_{41}'' \quad [270]$$

$$b: \ \mathsf{RQ} = \mathsf{msg}(d_{44}', b_{44}')|\mathsf{msg}(d_2, b_2)|q_2 \quad [292]$$

Induktionsvoraussetzung A5:

$$b: \ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \to (B = \mathsf{SBit} \to B' = \mathsf{SBit}) \quad [293]$$

$$b: \ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{44})|Q'|\mathsf{msg}(D', B_{44}')|Q'') \to (B_{44} = \mathsf{SBit} \to B_{44}' = \mathsf{SBit}) \quad [294]$$

$$b: \ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{44})|Q'|\mathsf{msg}(D', B_{44}')|Q'') \quad [295]$$

$$b: \ \neg(\mathsf{RQ} = Q_{44}|\mathsf{msg}(D_{44}, B_{44})|Q_{44}'|\mathsf{msg}(D_{44}', B_{44}')|Q_{44}'') \quad [297]$$

$$\square \ \{Q_{44}, \ Q_{44}' \leftarrow \varepsilon, \ D_{44} \leftarrow d_{44}', \ B_{44} \leftarrow b_{44}', \ D_{44}' \leftarrow d_2, \ B_{44}' \leftarrow b_2, \ Q_{44}'' \leftarrow q_2\}(292, 297)$$

$$b: \ b_{44}' = \mathsf{SBit} \to b_2 = \mathsf{SBit} \quad [296]$$

$$b: \ \neg(b_{44}' = \mathsf{SBit}) \quad [298]$$

$$\square \ b: \ \mathsf{RQ} = \mathsf{msg}(d_{41}', b_5)|q_{41}' \quad [270]$$

$$b: \ \mathsf{RQ} = \mathsf{msg}(d_{44}', b_{44}')|\mathsf{msg}(d_2, b_2)|q_2 \quad [292]$$

$$\to \ b_5 = b_{44}$$

$$b: \ b_5 = \mathsf{SBit} \quad [162]$$

$$b: \ \neg(b_{44}' = \mathsf{SBit}) \quad [298]$$

$$\to \ b_5 \neq b_{44}$$

$$b: \ b_2 = \mathsf{SBit} \quad [299]$$

$$\square \ b: \ b_2 = \mathsf{SBit} \quad [299]$$

$$b: \ b_5 = \mathsf{SBit} \quad [162]$$

$$\to \ b_2 = b_5$$

$$a: \ b_1 = \mathsf{SBit} \quad [31]$$

$$a: \ \mathsf{SBit} = b_5 \quad [185]$$

$$\to \ b_1 = b_5$$

$$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1') \quad [37]$$

$$a: \ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [40]$$

$$\to b_1 \neq b_2$$

$$\{D_1' \leftarrow d_2, \ Q_1' \leftarrow q_2\}$$

Damit ist der Beweis des zweiten Teils von Teilaussage A3 beendet.

5.7 4. Teilaussage

Beweis der Teilaussage A4:

Der Beweis schließt sich bei Knoten [25] des Beweises von Teilaussage 3 an. Die Numerierung der Indizes beginnt wieder bei 1.

Situation: $\mathsf{RIM}_a \neq \bot$, $\mathsf{Bit}(\mathsf{RIM}_a) = \mathsf{SBit}_a$, $\mathsf{RQ}_a \neq \varepsilon$, $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a)) \neq \mathsf{SBit}_a$.

Es wird versucht, A4 als Induktionsvoraussetzung zu verwenden.
Dabei wird zuerst die Situation behandelt, daß RIM_b leer ist. Da RIM_a nicht leer ist, muß also RecCom ausgeführt worden sein. Damit ist $\mathsf{RQ}_b \neq \varepsilon$, $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{Bit}(\mathsf{RIM}_a) = \mathsf{SBit}_a$.
Um A5 anzuwenden, muß $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$ sein. Wäre dies nicht so, also $\mathsf{SBit}_b \neq \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{Bit}(\mathsf{RIM}_a) = \mathsf{SBit}_a$, womit ProcAck SBit verändert haben müßte. Danach wäre dann $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ und nach A1 doch $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$.
Somit ist A5 anwendbar, man erhält $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a)) = \mathsf{Bit}(\mathsf{head}(\mathsf{tail}(\mathsf{RQ}_b)) = \mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b = \mathsf{SBit}_a$.

Also ist RIM_b nicht leer. Da RecCom und AckMsg beide nicht ausgeführt werden können (dazu müßte RIM_b bzw. RIM_a leer sein), ist $\mathsf{RIM}_b = \mathsf{RIM}_a$.

Als zweite Situation ist RIM_b nicht leer, aber $\mathsf{Bit}(\mathsf{RIM}_b) \neq \mathsf{SBit}_b$. Also ist $\mathsf{SBit}_a = \mathsf{Bit}(\mathsf{RIM}_a) = \mathsf{Bit}(\mathsf{RIM}_b) \neq \mathsf{SBit}_b$, womit ProcAck angewendet worden ist. Danach wäre dann $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ und nach A1 doch $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{SBit}_b$.

In der dritten Situation ist $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{SBit}_b$, also A4 als Induktionsvoraussetzung anwendbar und $\mathsf{RQ}_b = \varepsilon$ oder $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{SBit}_b$. Diese beiden Fälle werden einzeln abgehandelt und festgestellt, daß – egal wie und ob RQ verändert wurde – in allen Fällen $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_a)) = \mathsf{SBit}_a$ ist.

⋮

von [25] (S. 81):

$$a:\ \neg A4 \vee \neg A5 \quad [25]$$

$$a:\ \neg A4 \quad [26]$$

$$a:\ \neg A5 \quad [27]$$

↪ S. 137

$$a:\ \neg(\forall B : (\exists D : \mathsf{RIM} = \mathsf{msg}(D,B)) \to (B = \mathsf{SBit} \to (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D',B)|Q'))) \quad [28]$$

$$a:\ \neg((\exists D : \mathsf{RIM} = \mathsf{msg}(D,b_1)) \to (b_1 = \mathsf{SBit} \to (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D',b_1)|Q'))) \quad [29]$$

$$a:\ \exists D : \mathsf{RIM} = \mathsf{msg}(D,b_1) \quad [30]$$

$$a:\ \neg(b_1 = \mathsf{SBit} \to (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D',b_1)|Q')) \quad [31]$$

$$\boxed{\begin{array}{c} a:\ \mathsf{RIM} = \mathsf{msg}(d_1,b_1) \quad [32] \\ a:\ b_1 = \mathsf{SBit} \quad [33] \end{array}}$$

$$a:\ \neg(\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D',b_1)|Q') \quad [34]$$

$$a:\ \neg(\mathsf{RQ} = \varepsilon) \quad [35]$$

$$a:\ \neg(\exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D',b_1)|Q') \quad [36]$$

$$\boxed{a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D'_1,b_1)|Q'_1) \quad [37]}$$

aus F1R:

$$a:\ \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D,B)|Q \quad [38]$$

$$a:\ \exists D', B', Q' : \mathsf{RQ} = Q'|\mathsf{msg}(D',B') \quad [39]$$

$$\boxed{a:\ \mathsf{RQ} = \mathsf{msg}(d_2,b_2)|q_2 \quad [40]}$$

Induktionsvoraussetzung A4:

$$b:\ \forall B : (\exists D : \mathsf{RIM} = \mathsf{msg}(D,B)) \to (B = \mathsf{SBit} \to (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D',B)|Q')) \quad [41]$$

$$b:\ (\exists D : \mathsf{RIM} = \mathsf{msg}(D,B_3)) \to (B_3 = \mathsf{SBit} \to (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D',B_3)|Q')) \quad [42]$$

$$b:\ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D,B_3)) \quad [43]$$

$$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_3,B_3)) \quad [46]$$

↪ S. 124

B_3 einsetzen (aus [50]):

$$\mathrm{LG}:\ b:\ \exists D : \mathsf{RIM} = \mathsf{msg}(D,b_5) \quad [44]$$

$$b:\ b_5 = \mathsf{SBit} \to (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D',b_5)|Q') \quad [45]$$

$$b:\ \mathsf{RIM} = \mathsf{msg}(d_4,b_5) \quad [91]$$

↪ S. 127

$\vdots$

von [46] (S. 123):

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [32]

$a:\ b_1 = \mathsf{SBit}$ [33]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D'_1, b_1)|Q'_1)$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_3, B_3))$ [46]

aus F2R: $b:\ \mathsf{RIM} = \bot \vee \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B)$ [47]

$\boxed{b:\ \mathsf{RIM} = \bot \quad [48]}$

aus RIM:

$b:\ \forall M : \mathsf{RIM} = M \rightarrow \mathsf{A}(\mathsf{RIM} = M \text{ unless}^+ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [51]

mit Tab. 0.11, $\{M \leftarrow \bot\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [52]

$a:\ \mathsf{RecCom} = \mathsf{true}$ [54]

aus Tab. 0.2:

$b:\ \mathsf{RIM} = \bot$ [56]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_6, b_6)|q_6$ [57]

$a:\ \mathsf{RQ} = q_6$ [58]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_6, b_6)$ [59]

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [55]

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{11}, b_{11})$ [86]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{11})$ [87]

$b:\ \mathsf{SQ} = q_{12}$ [88]

$a:\ \mathsf{SQ} = q_{12}|\mathsf{msg}(\lambda, b_{11})$ [89]

$a:\ \mathsf{RIM} = \bot$ [90]

$\square$ (E3, 32, 90)

$a:\ \mathsf{RIM} = \bot$ [53]

$\square$ (E3, 32, 53)

$b:\ \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B)$ [49]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_5, b_5)$ [50]

$\square\ \{D_3 \leftarrow d_5,\ B_3 \leftarrow b_5\}(46, 50)$

Induktionsvoraussetzung A5:

$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit})$ [60]

$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_7)|Q'|\mathsf{msg}(D', B'_7)|Q'') \rightarrow (B_7 = \mathsf{SBit} \rightarrow B'_7 = \mathsf{SBit})$ [61]

$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_7)|Q'|\mathsf{msg}(D', B'_7)|Q'')$ [62]

$b:\ \neg(\mathsf{RQ} = Q_7|\mathsf{msg}(D_7, B_7)|Q'_7|\mathsf{msg}(D'_7, B'_7)|Q''_7)$ [64]

$\square\ b:\ \mathsf{RQ} = \mathsf{msg}(d_6, b_6)|q_6$ [57]

$a:\ \mathsf{RQ} = q_6$ [58]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ \neg(\mathsf{RQ} = Q_7|\mathsf{msg}(D_7, B_7)|Q'_7|\mathsf{msg}(D'_7, B'_7)|Q''_7)$ [64]

$\{Q_7, Q'_7 \leftarrow \varepsilon, D_7 \leftarrow d_6, B_7 \leftarrow b_6, D'_7 \leftarrow d_2, B'_7 \leftarrow b_2\}$

$b:\ b_6 = \mathsf{SBit} \rightarrow b_2 = \mathsf{SBit}$ [63]

$\hookrightarrow$ S. 125

$\vdots$

von [63] (S. 124):

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [32]

$a:\ b_1 = \mathsf{SBit}$ [33]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_6, b_6)|q_6$ [57]

$a:\ \mathsf{RQ} = q_6$ [58]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_6, b_6)$ [59]

$b:\ b_6 = \mathsf{SBit} \rightarrow b_2 = \mathsf{SBit}$ [63]

$b:\ \neg(b_6 = \mathsf{SBit})$ [65]

aus EA:

$b:\ \exists B : \mathsf{SBit} = B$ [68]

$b:\ \mathsf{SBit} = b_8$ [69]

LG : $b:\ b_6 = \mathsf{SBit}$ [66]

$b:\ b_2 = \mathsf{SBit}$ [67]

□ $b:\ b_2 = \mathsf{SBit}$ [67] $\quad$ $a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [32]

$b:\ b_6 = \mathsf{SBit}$ [66] $\quad$ $a:\ \mathsf{RIM} = \mathsf{msg}(d_6, b_6)$ [59]

$\rightarrow\ b_2 = b_6$ $\quad$ $\rightarrow\ b_1 = b_6$

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1')$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$\rightarrow\ b_1 \neq b_2$

$\{D_1' \leftarrow d_2,\ Q_1' \leftarrow q_2\}$

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \text{ unless}^+ \mathsf{ProcAck} = \mathsf{true})$ [70]

mit Tab. 0.11, $\{B \leftarrow b_8\}$:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [71]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_9, b_9)$ [73]

$b:\ \mathsf{SBit} = b_9$ [74]

↪ S. 126

$a:\ \mathsf{SBit} = b_8$ [72]

□ : $a:\ b_1 = \mathsf{SBit}$ [33] $\quad$ $a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [32]

$a:\ \mathsf{SBit} = b_8$ [72] $\quad$ $a:\ \mathsf{RIM} = \mathsf{msg}(d_6, b_6)$ [59]

$\rightarrow\ b_1 = b_8$ $\quad$ $\rightarrow\ b_1 = b_6$

$b:\ \neg(b_6 = \mathsf{SBit})$ [65]

$b:\ \mathsf{SBit} = b_8$ [69]

$\rightarrow\ b_6 \neq b_8$

$\vdots$

von [74] (S. 125):

$b: \ \mathsf{RQ} = \mathsf{msg}(d_6, b_6)|q_6 \quad [57]$

$b: \ \neg(b_6 = \mathsf{SBit}) \quad [65]$

$b: \ \mathsf{SIM} = \mathsf{msg}(d_9, b_9) \quad [73]$

$b: \ \mathsf{SBit} = b_9 \quad [74]$

$b: \ A1 \quad [13]:$

$$\begin{aligned} b: \ \forall B: (\exists D: \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow & \qquad [75] \\ (B = \mathsf{SBit} \rightarrow \ & ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge \\ & (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge \\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) \end{aligned}$$

$b: \ (\exists D: \mathsf{SIM} = \mathsf{msg}(D, B_{10})) \rightarrow (B_{10} = \mathsf{SBit} \rightarrow \ldots) \quad [76]$

$b: \ \neg(\exists D: \mathsf{SIM} = \mathsf{msg}(D, B_{10})) \quad [77]$

$b: \ \neg(\mathsf{SIM} = \mathsf{msg}(D_{10}, B_{10})) \quad [78]$

$\Box \ \{D_{10} \leftarrow d_9, \ B_{10} \leftarrow b_9\}(73, 78)$

[76] auflösen:

$b: \ \neg(b_9 = \mathsf{SBit}) \quad [79]$

$\Box \ (74, 79)$

$b: \ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_9)|Q^1) \quad [80]$

$b: \ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_9) \quad [81]$

$b: \ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_9)|Q^3) \quad [82]$

$b: \ \mathsf{RQ} = \varepsilon \quad [83]$

$\Box \ (\mathrm{E2}, 57, 83)$

$b: \ \exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_9)|Q^3 \quad [84]$

$b: \ \mathsf{RQ} = \mathsf{msg}(q^3_{10}, b_9)|q^3_{10} \quad [85]$

$$\boxed{\begin{array}{l} \Box \ b: \ \mathsf{RQ} = \mathsf{msg}(d_6, b_6)|q_6 \quad [57] \\ \quad b: \ \mathsf{RQ} = \mathsf{msg}(q^3_{10}, b_9)|q^3_{10} \quad [85] \\ \hline \quad \rightarrow b_6 = b_9 \\ \quad b: \ \neg(b_6 = \mathsf{SBit}) \quad [65] \\ \quad b: \ \mathsf{SBit} = b_9 \quad [74] \\ \hline \quad \rightarrow b_6 \neq b_9 \end{array}}$$

$$\vdots$$

von [91] (S. 123):

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [32]

$a:\ b_1 = \mathsf{SBit}$ [33]

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D'_1, b_1)|Q'_1)$ [37]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$b:\ b_5 = \mathsf{SBit} \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_5)|Q')$ [45]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)$ [91]

aus RIM: $b:\ \forall M : \mathsf{RIM} = M \rightarrow \mathsf{A}(\mathsf{RIM} = M \text{ unless}^+ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [92]

mit Tab. 0.11, $\{M \leftarrow \mathsf{msg}(d_4, b_5)\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [93] | $a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)$ [94]

$a:\ \mathsf{RecCom} = \mathsf{true}$ [95]
aus Tab. 0.2:
$b:\ \mathsf{RIM} = \bot$ [97]
$b:\ \mathsf{RQ} = \mathsf{msg}(d_{13}, b_{13})|q_{13}$ [98]
$\square$ (E3, 91, 97)

$a:\ \mathsf{AckMsg} = \mathsf{true})$ [96]
aus Tab. 0.10:
$a:\ \mathsf{SQ} = q_{15}|\mathsf{msg}(\lambda, b_{14})$ [99]
$a:\ \mathsf{RIM} = \bot$ [100]
$\square$ (E3, 32, 100)

aus [45] :

$b:\ \neg(b_5 = \mathsf{SBit})$ [101]
aus EA:
$b:\ \exists B : \mathsf{SBit} = B$ [104]
$b:\ \mathsf{SBit} = b_{16}$ [105]

LG : $b:\ b_5 = \mathsf{SBit}$ [102]
$b:\ \mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_5)|Q'$ [103]
$\hookrightarrow$ S. 129

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \text{ unless}^+ \mathsf{ProcAck} = \mathsf{true})$ [106]

mit Tab. 0.11, $\{B \leftarrow b_{16}\}$:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [107]
mit Tab. 0.7:
$b:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_{17})$ [109]
$b:\ \mathsf{SBit} = b_{17}$ [110]
$\hookrightarrow$ S. 128

$a:\ \mathsf{SBit} = b_{16}$ [108]

$$\square:\quad \begin{array}{l} a:\ b_1 = \mathsf{SBit}\ \ [33] \\ \underline{a:\ \mathsf{SBit} = b_{16}\ \ [108]} \\ \rightarrow\ b_1 = b_{16} \\ b:\ \neg(b_5 = \mathsf{SBit})\ \ [101] \\ \underline{b:\ \mathsf{SBit} = b_{16}\ \ [105]} \\ \rightarrow\ b_5 \neq b_{16} \end{array} \qquad \begin{array}{l} a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)\ \ [32] \\ \underline{a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\ \ [91]} \\ \rightarrow\ b_1 = b_5 \end{array}$$

$\vdots$

von [110] (S. 127):

$b:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\quad [91]$

$b:\ \neg(b_5 = \mathsf{SBit})\quad [101]$

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_{17})\quad [109]$

$b:\ \mathsf{SBit} = b_{17}\quad [110]$

$|$

Induktionsvoraussetzung A1:

$b:\ A1\quad [13]:$

$$\begin{array}{ll} b:\ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow & [111] \\ \quad (B = \mathsf{SBit} \rightarrow\ \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge & \\ \quad\quad (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge & \\ \quad\quad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) & \end{array}$$

$|$

$b:\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{18})) \rightarrow (B_{18} = \mathsf{SBit} \rightarrow \ldots)\quad [112]$

$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{18}))\quad [113]$

$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{18}, B_{18}))\quad [114]$

$\square\ \{D_{18} \leftarrow d_{17},\ B_{18} \leftarrow b_{17}\}(109, 114)$

[111] auflösen:

$b:\ \neg(b_{17} = \mathsf{SBit}\quad [115]$

$\square\ (110, 115)$

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_{17})|Q^1)\quad [116]$

$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_{17})\quad [117]$

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_{17})|Q^3)\quad [118]$

$b:\ \mathsf{RIM} = \bot\quad [119]$

$\square\ (91, 119)$

$b:\ \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_{17})\quad [120]$

$b:\ \mathsf{RIM} = \mathsf{msg}(d^2_{18}, b_{17})\quad [121]$

$$\boxed{\begin{array}{ll} \square & b:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\quad [91] \\ & b:\ \mathsf{RIM} = \mathsf{msg}(d^2_{18}, b_{17})\quad [121] \\ \hline & \rightarrow b_5 = b_{17} \\ & b:\ \neg(b_5 = \mathsf{SBit})\quad [101] \\ & b:\ \mathsf{SBit} = b_{17}\quad [110] \\ \hline & \rightarrow b_6 \neq b_{17} \end{array}}$$

$$\vdots$$

von [103] (S. 127):

$$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [32]$$
$$a:\ b_1 = \mathsf{SBit} \quad [33]$$
$$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1') \quad [37]$$
$$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [40]$$
$$b:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5) \quad [91]$$
$$a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5) \quad [94]$$
$$b:\ b_5 = \mathsf{SBit} \quad [102]$$
$$b:\ \mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_5)|Q' \quad [103]$$

$$b:\ \mathsf{RQ} = \varepsilon \quad [122]$$

$$b:\ \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_5)|Q' \quad [123]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}' \quad [151]$$

$\hookrightarrow$ S. 131

aus RQ:

$$b:\ \forall Q : \mathsf{RQ} = Q \to \mathsf{A}(\mathsf{RQ} = Q\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}) \quad [124]$$

mit Tab. 0.11, $\{Q \leftarrow \varepsilon\}$:

$$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true} \quad [125]$$

$$a:\ \mathsf{RQ} = \varepsilon \quad [126]$$
$$\Box\ (\mathrm{E}2, 40, 126)$$

$$a:\ \mathsf{RecCom} = \mathsf{true} \quad [127]$$

aus Tab. 0.2:

$$b:\ \mathsf{RIM} = \bot \quad [131]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_{19}, b_{19})|q_{19} \quad [132]$$
$$\Box\ (\mathrm{E}2, 91, 131)$$

$$a:\ \mathsf{ProcAck} = \mathsf{true} \quad [130]$$

$\hookrightarrow$ S. 130

$$a:\ \mathsf{RLose} = \mathsf{true} \quad [128]$$

aus Tab. 0.4:

$$b:\ \mathsf{RQ} \neq \varepsilon \quad [133]$$
$$\Box\ (122, 133)$$

$$a:\ \mathsf{ReTrans} = \mathsf{true} \quad [129]$$

aus Tab. 0.6:

$$b:\ \mathsf{RQ} = q_{20} \quad [134]$$
$$b:\ \mathsf{SNo} = n_{20} \quad [135]$$
$$b:\ \mathsf{SBit} = b_{20} \quad [136]$$
$$a:\ \mathsf{RQ} = q_{20}|\mathsf{msg}(\mathsf{SFile}(n_{20}), b_{20}) \quad [137]$$

$$\Box \quad \frac{a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)\ [32] \qquad a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\ [94]}{\to\ b_1 = b_5} \qquad \frac{b:\ b_5 = \mathsf{SBit}\ [102] \qquad b:\ \mathsf{SBit} = b_{20}\ [136]}{\to\ b_5 = b_{20}}$$

$$\frac{b:\ \mathsf{RQ} = \varepsilon\ [121] \qquad b:\ \mathsf{RQ} = q_{20}\ [134]}{\to\ q_{20} = \varepsilon} \qquad \frac{a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1')\ [37] \qquad a:\ \mathsf{RQ} = q_{20}|\mathsf{msg}(\mathsf{SFile}(n_{20}), b_{20})\ [137]}{\to\ b_1 \neq b_{20}}$$

$$\Box\ \{D_1' \leftarrow \mathsf{SFile}(n_{20}),\ Q_1' \leftarrow q_{20}\}$$

$\vdots$

von [130] (S. 129):

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [32]

$a:\ b_1 = \mathsf{SBit}$ [33]

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)$ [94]

$b:\ b_5 = \mathsf{SBit}$ [102]

$b:\ \mathsf{RQ} = \varepsilon$ [122]

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [130]

|

aus Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{21}, b_{21})$ [138]

$b:\ \mathsf{SBit} = b_{21}$ [139]

$b:\ \mathsf{RQ} = q_{22}$ [140]

$b:\ \mathsf{SNo} = n_{22}$ [141]

Linker Zweig:

$a:\ (\mathsf{SFile}(s(n_{22})) = d_{23}$ [142]

$a:\ \mathsf{RQ} = q_{22}|\mathsf{msg}(\mathsf{SFile}(s(n_{22})), \mathsf{flip}(b_{21}))$ [143]

$a:\ \mathsf{SNo} = s(n_{22})$ [144]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{21})$ [145]

□ $a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [32]
$a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)$ [94]
$\rightarrow\ b_1 = b_5$
$a:\ b_1 = \mathsf{SBit}$ [33]
$a:\ \mathsf{SBit} = \mathsf{flip}(b_{21})$ [145]
$\rightarrow\ b_1 = \mathsf{flip}(b_{27})$
$b:\ b_5 = \mathsf{SBit}$ [102]
$b:\ \mathsf{SBit} = b_{21}$ [139]
$\rightarrow\ b_5 = b_{27}$

Rechter Zweig:

$a:\ \mathsf{SFile}(s(n_{22})) = \perp$ [146]

$a:\ \mathsf{RQ} = q_{22}$ [147]

$a:\ \mathsf{SNo} = n_{22}$ [148]

$a:\ \mathsf{SBit} = b_{21}$ [149]

$a:\ \mathsf{ready} = \mathsf{true}$ [150]

□ $b:\ \mathsf{RQ} = q_{22}$ [140]
$b:\ \mathsf{RQ} = \varepsilon$ [122]
$\rightarrow\ q_{22} = \varepsilon$
$a:\ \mathsf{RQ} = q_{22}$ [147]
$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2$ [40]
□ E2

$\vdots$

von [151] (S. 129):

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)\quad [32]$

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1')\quad [37]$

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2\quad [40]$

$b:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\quad [91]$

$a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\quad [94]$

$b:\ b_5 = \mathsf{SBit}\quad [102]$

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}'\quad [151]$

aus RQ:

$$b:\ \forall Q : \mathsf{RQ} = Q \rightarrow \mathsf{A}(\mathsf{RQ} = Q \ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\quad [152]$$

mit Tab. 0.11, $\{Q \leftarrow \mathsf{msg}(d_{24}', b_5)|q_{24}'\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}\quad [153]$

$a:\ \mathsf{RecCom} = \mathsf{true}\quad [155]$

aus Tab. 0.2:

$b:\ \mathsf{RIM} = \bot\quad [159]$

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{25}, b_{25})|q_{25}\quad [160]$

$\Box$ (E2, 91, 159)

$a:\ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}'\quad [154]$

$\Box$ $a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)\quad [32]$
$a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\quad [94]$
$\rightarrow\ b_1 = b_5$
$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1')\quad [37]$
$a:\ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}'\quad [154]$
$\rightarrow\ b_1 \neq b_5$
$\{D_1' \leftarrow d_{24}',\ Q_1' \leftarrow q_{24}'\}$

$a:\ \mathsf{RLose} = \mathsf{true}\quad [156]$

$\hookrightarrow$ S. 132

$a:\ \mathsf{ReTrans} = \mathsf{true}\quad [157]$

aus Tab. 0.6:

$b:\ \mathsf{RQ} = q_{28}\quad [172]$

$b:\ \mathsf{SNo} = n_{28}\quad [173]$

$b:\ \mathsf{SBit} = b_{28}\quad [174]$

$a:\ \mathsf{RQ} = q_{28}|\mathsf{msg}(\mathsf{SFile}(n_{28}), b_{28})\quad [175]$

$a:\ \mathsf{ProcAck} = \mathsf{true}\quad [158]$

$\hookrightarrow$ S. 134

$\Box$ $a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)\quad [32]$	$b:\ \mathsf{RQ} = q_{28}\quad [172]$
$a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\quad [94]$	$b:\ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}'\quad [151]$
$\rightarrow\ b_1 = b_5$	$a:\ \mathsf{RQ} = q_{28}|\mathsf{msg}(\mathsf{SFile}(n_{28}), b_{28})\quad [175]$
	$\rightarrow\ a:\ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}'|\mathsf{msg}(\mathsf{SFile}(n_{28}), b_{28})$
	$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1')\quad [37]$
	$\rightarrow\ b_1 \neq b_5$
	$\{D_1' \leftarrow \mathsf{SFile}(n_{28}),\ Q_1' \leftarrow q_{28}\}$

$$\vdots$$

von [156] (S. 131):

$$a: \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [32]$$
$$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1') \quad [37]$$
$$a: \ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [40]$$
$$a: \ \mathsf{RIM} = \mathsf{msg}(d_4, b_5) \quad [94]$$
$$b: \ b_5 = \mathsf{SBit} \quad [102]$$
$$b: \ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}' \quad [151]$$
$$a: \ \mathsf{RLose} = \mathsf{true} \quad [156]$$

$$b: \ \mathsf{SQ} \neq \varepsilon \quad [161]$$

$$b: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_{26}, B_{26})|Q_{26})) \quad [162]$$
$$\square \ \{D_{26} \leftarrow d_2, \ B_{26} \leftarrow b_2, \ Q_{26} \leftarrow q_2\}(40, 162)$$

$$b: \ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_{26}' \quad [163]$$

$$\boxed{\begin{array}{l} \square \ b: \ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_{26}' \quad [163] \\ \quad b: \ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}' \quad [151] \\ \hline \quad \rightarrow b_2 = b_5 \\ \quad a: \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [32] \\ \quad a: \ \mathsf{RIM} = \mathsf{msg}(d_4, b_5) \quad [94] \\ \hline \quad \rightarrow b_1 = b_5 \\ \quad a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1') \quad [37] \\ \quad a: \ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2 \quad [40] \\ \hline \quad \rightarrow b_1 \neq b_2 \\ \quad \{D_1' \leftarrow d_2, \ Q_1' \leftarrow q_2\} \end{array}}$$

$$b: \ \mathsf{RQ} = \mathsf{msg}(d_{26}', b_{26}')|\mathsf{msg}(d_2, b_2)|q_2 \quad [164]$$

↪ S. 133

$$\vdots$$

von [164] (S. 132):

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)\quad [32]$

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1')\quad [37]$

$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2\quad [40]$

$a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\quad [94]$

$b:\ b_5 = \mathsf{SBit}\quad [102]$

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}'\quad [151]$

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{26}', b_{26}')|\mathsf{msg}(d_2, b_2)|q_2\quad [164]$

Induktionsvoraussetzung A5:

$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \to (B = \mathsf{SBit} \to B' = \mathsf{SBit})\quad [165]$

$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{27})|Q'|\mathsf{msg}(D', B_{27}')|Q'') \to (B_{27} = \mathsf{SBit} \to B_{27}' = \mathsf{SBit})\quad [166]$

$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{27})|Q'|\mathsf{msg}(D', B_{27}')|Q'')\quad [167]$

$b:\ \neg(\mathsf{RQ} = Q_{27}|\mathsf{msg}(D_{27}, B_{27})|Q_{27}'|\mathsf{msg}(D_{27}', B_{27}')|Q_{27}'')\quad [169]$

$\square\ Q_{27},\ Q_{27}' \leftarrow \varepsilon,\ D_{27} \leftarrow d_{26}',\ B_{27} \leftarrow b_{26}',$
$D_{27}' \leftarrow d_2,\ B_{27}' \leftarrow b_2,\ Q_{27}'' \leftarrow q_2\}(164, 169)$

$b:\ b_{26}' = \mathsf{SBit} \to b_2 = \mathsf{SBit}\quad [168]$

$b:\ \neg(b_{26}' = \mathsf{SBit})\quad [170]$

$\square\ b:\ \mathsf{RQ} = \mathsf{msg}(d_{24}', b_5)|q_{24}'\quad [151]$
$b:\ \mathsf{RQ} = \mathsf{msg}(d_{26}', b_{26}')|\mathsf{msg}(d_2, b_2)|q_2\quad [164]$

$\to\ b_5 = b_{26}$

$b:\ b_5 = \mathsf{SBit}\quad [102]$
$b:\ \neg(b_{26}' = \mathsf{SBit})\quad [170]$

$\to\ b_5 \neq b_{26}$

$b:\ b_2 = \mathsf{SBit}\quad [171]$

$\square\ b:\ b_2 = \mathsf{SBit}\quad [171]$
$b:\ b_5 = \mathsf{SBit}\quad [102]$

$\to\ b_2 = b_5$

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)\quad [32]$
$a:\ \mathsf{RIM} = \mathsf{msg}(d_4, b_5)\quad [94]$

$\to\ b_1 = b_5$

$a:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_1', b_1)|Q_1')\quad [37]$
$a:\ \mathsf{RQ} = \mathsf{msg}(d_2, b_2)|q_2\quad [40]$

$\to b_1 \neq b_2$

$\{D_1' \leftarrow d_2,\ Q_1' \leftarrow q_2\}$

$\vdots$

von [158] (S. 131):

$a: \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [32]$

$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D'_1, b_1)|Q'_1) \quad [37]$

$b: \ \mathsf{RIM} = \mathsf{msg}(d_4, b_5) \quad [91]$

$b: \ \mathsf{RQ} = \mathsf{msg}(d'_{24}, b_5)|q'_{24} \quad [151]$

$a: \ \mathsf{ProcAck} = \mathsf{true} \quad [158]$

|

aus Tab. 0.7:

$b: \ \mathsf{SIM} = \mathsf{msg}(d_{29}, b_{29}) \quad [176]$

$b: \ \mathsf{SBit} = b_{29} \quad [177]$

$b: \ \mathsf{RQ} = q_{30} \quad [178]$

$b: \ \mathsf{SNo} = n_{30} \quad [179]$

Linker Zweig:

$a: \ (\mathsf{SFile}(s(n_{30})) = d_{31} \quad [180]$

$a: \ \mathsf{RQ} = q_{30}|\mathsf{msg}(\mathsf{SFile}(s(n_{30})), \mathsf{flip}(b_{29})) \quad [181]$

$a: \ \mathsf{SNo} = s(n_{30}) \quad [182]$

$a: \ \mathsf{SBit} = \mathsf{flip}(b_{29}) \quad [183]$

$\Box$ $a: \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [32]$
$b: \ \mathsf{RIM} = \mathsf{msg}(d_4, b_5) \quad [91]$

$\rightarrow \ b_1 = b_5$

$b: \ \mathsf{RQ} = q_{30} \quad [178]$
$b: \ \mathsf{RQ} = \mathsf{msg}(d'_{24}, b_5)|q'_{24} \quad [151]$
$a: \ \mathsf{RQ} = q_{30}|\mathsf{msg}(\mathsf{SFile}(s(n_{30})), \mathsf{flip}(b_{29})) \quad [181]$

$\rightarrow \ a: \mathsf{RQ} = \mathsf{msg}(d'_{24}, b_5)|q'_{24}|\mathsf{msg}(\mathsf{SFile}(s(n_{30})), \mathsf{flip}(b_{29}))$
$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D'_1, b_1)|Q'_1) \quad [37]$

$\rightarrow \ b_1 \neq b_5$

$\{D'_1 \leftarrow d'_{24}, \ Q'_1 \leftarrow q'_{24}|\mathsf{msg}(\mathsf{SFile}(s(n_{30})), \mathsf{flip}(b_{29}))\}$

Rechter Zweig:

$a: \ \mathsf{SFile}(s(n_{30})) = \perp \quad [184]$

$a: \ \mathsf{RQ} = q_{30} \quad [185]$

$a: \ \mathsf{SNo} = n_{30} \quad [186]$

$a: \ \mathsf{SBit} = b_{29} \quad [187]$

$a: \ \mathsf{ready} = \mathsf{true} \quad [188]$

$\Box$ $a: \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [32]$
$b: \ \mathsf{RIM} = \mathsf{msg}(d_4, b_5) \quad [91]$

$\rightarrow \ b_1 = b_5$

$b: \ \mathsf{RQ} = q_{30} \quad [178]$
$b: \ \mathsf{RQ} = \mathsf{msg}(d'_{24}, b_5)|q'_{24} \quad [151]$
$a: \ \mathsf{RQ} = q_{30} \quad [185]$

$\rightarrow \ a: \mathsf{RQ} = \mathsf{msg}(d'_{24}, b_5)|q'_{24}$
$a: \ \neg(\mathsf{RQ} = \mathsf{msg}(D'_1, b_1)|Q'_1) \quad [37]$

$\rightarrow \ b_1 \neq b_5$

$\{D'_1 \leftarrow d'_{24}, \ Q'_1 \leftarrow q'_{24}\}$

An dieser Stelle ist der Beweis von Teilaussage A4 beendet.

5.8 5. Teilaussage

Der Beweis von Teilaussage 5 wird ähnlich dem von Teilaussage 2 geführt.

Er setzt an Knoten [27] an, die Indizes werden bei 1 beginnend numeriert.

Beweisskizze:

Situation: $\mathsf{RQ}_a \neq \varepsilon$, es gibt eine Nachricht $m_1 = \mathsf{msg}(d_1, b_1)$ in RQ_a, deren Kontrollbit $b_1 = \mathsf{SBit}_a$ ist, sowie eine weitere, in RQ neuere Nachricht $m_2 = \mathsf{msg}(d_2, b_2)$, deren Kontrollbit $b_2 \neq SBit_a$ ist.

In diesem Fall wird – unter intensiver Einbeziehung der Gleichheit – "rückblickend" betrachtet, wie RQ vorher ausgesehen haben kann, und alle diese Situationen als unmöglich erkannt.

Wurde RecCom angewendet, ergibt sich, daß alle Nachrichten, die in RQ_a enthalten sind, auch schon in RQ_b enthalten waren. Damit liefert A5 als Induktionsvoraussetzung den gewünschten Widerspruch – falls $\mathsf{SBit}_b = b_1 = \mathsf{SBit}_a$ ist.

Es ergibt sich an dieser Stelle, daß ProcAck SBit nicht verändert haben kann: Dazu müßte $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ und somit nach A1 das erste sowie nach A5 alle Kontrollbits von RQ_b gleich $\mathsf{SBit}_b \neq \mathsf{SBit}_a$ sein.

Somit ist also $\mathsf{SBit}_a = \mathsf{SBit}_b$.

Wurde RLose angewendet, so sind ebenfalls alle Nachrichten aus RQ_a schon in RQ_b enthalten gewesen. Vorgehen analog dem eben betrachteten Fall.

Nachdem oben bereits festgestellt wurde, daß ProcAck SBit nicht verändert hat, bleibt hier nur der Fall zu betrachten, in dem SBit unverändert bleibt. Dabei bleibt allerdings auch RQ unverändert, sodaß A5 den Widerspruch liefert.
Wurde ReTrans angewendet, wird unterschieden, ob m_2 die letzte – also durch ReTrans angehängte – Nachricht ist, oder ob m_1 und m_2 beide bereits in RQ_b enthalten waren. Da ReTrans immer eine Nachricht mit dem aktuellen SBit – also SBit_b – anhängt, und $\mathsf{SBit}_a = \mathsf{SBit}_b$ gilt, erhält man in ersten Fall direkt eine Widerspruch. Im zweiten Fall geht man analog den bereits betrachteten Fällen vor.

In allen Fällen ergibt sich die Anwendbarkeit der Induktionsvoraussetzung aus $\mathsf{SBit}_a = \mathsf{SBit}_b$ wie oben.

Ist RQ nicht verändert worden, erhält man den Beweis sofort aus A5.

$$\vdots$$

von [27] (S. 123):

$a:\ \neg A5$ [27]

$a:\ \neg(\forall B, B':\ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'')$ [28]
$\rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit})$

$a:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,b_1)|Q'|\mathsf{msg}(D',b_1')|Q'') \rightarrow (b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit})$ [29]

$a:\ \exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,b_1)|Q'|\mathsf{msg}(D',b_1')|Q''$ [30]

$a:\ \neg(b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit})$ [31]

$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1''$ [32]
$a:\ b_1 = \mathsf{SBit}$ [33]
$a:\ \neg(b_1' = \mathsf{SBit})$ [34]

aus EA: $b:\ \exists Q : \mathsf{RQ} = Q$ [35]

$b:\ \mathsf{RQ} = q_2$ [36]

aus RQ:

$b:\ \forall Q : \mathsf{RQ} = Q \rightarrow$ [37]
$\mathsf{A}(\mathsf{RQ} = Q \text{ unless}^+ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$

aus Tab. 0.11, $\{Q \leftarrow q_2\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}$ [38]

$a:\ \mathsf{RQ} = q_2$ [39]
↪ S. 148

$a:\ \mathsf{RecCom} = \mathsf{true}$ [40]
aus Tab. 0.1:
$b:\ \mathsf{RIM} = \perp$ [44]
$b:\ \mathsf{RQ} = \mathsf{msg}(d_3,b_3)|q_3$ [45]
$a:\ \mathsf{RQ} = q_3$ [46]
$a:\ \mathsf{RIM} = \mathsf{msg}(d_3,b_3)$ [47]
↪ S. 138

$a:\ \mathsf{RLose} = \mathsf{true}$ [41]
↪ S. 143

$a:\ \mathsf{ReTrans} = \mathsf{true}$ [42]
$b:\ \mathsf{RQ} = q_{15}$ [113]
$b:\ \mathsf{SNo} = n_{15}$ [114]
$b:\ \mathsf{SBit} = b_{15}$ [115]
$a:\ \mathsf{RQ} = q_{15}|\mathsf{msg}(\mathsf{SFile}(n_{15}), b_{15})$ [116]
↪ S. 144

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [43]
↪ S. 147

$\vdots$

von [47] (S. 137):

$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1''$ [32]

$a:\ b_1 = \mathsf{SBit}$ [33]

$a:\ \neg(b_1' = \mathsf{SBit})$ [34]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_3,b_3)|q_3$ [45]

$a:\ \mathsf{RQ} = q_3$ [46]

$|$

Induktionsvoraussetzung A5:

aus $b:\ A5$ [17] :

$b:\ \forall B,B' : (\exists D,D',Q,Q',Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit})$ [48]

$|$

$b:\ (\exists D,D',Q,Q',Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B_4)|Q'|\mathsf{msg}(D',B_4')|Q'') \rightarrow (B_4 = \mathsf{SBit} \rightarrow B_4' = \mathsf{SBit})$ [49]

$b:\ \neg(\exists D,D',Q,Q',Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B_4)|Q'|\mathsf{msg}(D',B_4')|Q'')$ [50]

$b:\ \neg(\mathsf{RQ} = Q_4|\mathsf{msg}(D_4,B_4)|Q_4'|\mathsf{msg}(D_4',B_4')|Q_4'')$ [53]

□ $a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1''$ [32]
$a:\ \mathsf{RQ} = q_3$ [46]

$q_3 = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1''$
$b:\ \mathsf{RQ} = \mathsf{msg}(d_3,b_3)|q_3$ [45]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_3,b_3)|q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1''$

$b:\ \neg(\mathsf{RQ} = Q_4|\mathsf{msg}(D_4,B_4)|Q_4'|\mathsf{msg}(D_4',B_4')|Q_4'')$ [53]

$\{Q_4 \leftarrow \mathsf{msg}(d_3,b_3)|q_1, D_4 \leftarrow d_1, B_4 \leftarrow b_1, Q_4' \leftarrow q_1', D_4' \leftarrow d_1', B_4' \leftarrow b_1', Q_4'' \leftarrow q_1''\}$

B_4, B_4' einsetzen:

LG : $b:\ \exists D,D',Q,Q',Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,b_1)|Q'|\mathsf{msg}(D',b_1')|Q''$ [51]

$b:\ b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit}$ [52]

$b:\ \mathsf{RQ} = q_5|\mathsf{msg}(d_5,b_1)|q_5'|\mathsf{msg}(d_5',b_1')|q_5''$ [54]

$\boxed{b:\ \neg(b_1 = \mathsf{SBit})\ [55]}$

$\hookrightarrow$ S. 139

LG : $b:\ b_1 = \mathsf{SBit}$ [56]

$b:\ b_1' = \mathsf{SBit}$ [57]

□ $b:\ b_1 = \mathsf{SBit}$ [56]	$a:\ b_1 = \mathsf{SBit}$ [33]
$b:\ b_1' = \mathsf{SBit}$ [57]	$a:\ \neg(b_1' = \mathsf{SBit})$ [34]
$\rightarrow b_1 = b_1'$	$\rightarrow b_1 \neq b_1'$

Das folgende Tableau zeigt prinzipiell die Inkonsistenz der folgenden Formeln. Es wird im Verlauf des Beweises mehrfach benötigt.

$$b:\ \mathsf{RQ} = q|\mathsf{msg}(d,b_1)|q' \quad , \quad b:\ \neg(b_1 = \mathsf{SBit}) \quad , \quad a:\ b_1 = \mathsf{SBit}$$

$\vdots$

von [55] (S. 138):

$a:\ b_1 = \mathsf{SBit}$ [33]

$b:\ \mathsf{RQ} = q_5|\mathsf{msg}(d_5,b_1)|q_5'|\mathsf{msg}(d_5',b_1')|q_5''$ [54]

$b:\ \neg(b_1 = \mathsf{SBit})$ [55]

aus EA: $b:\ \exists B : \mathsf{SBit} = B$ [58]

$b:\ \mathsf{SBit} = b_6$ [59]

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [60]

mit Tab. 0.11, $\{B \leftarrow b_6\}$:

Linker Zweig:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [61]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_7,b_7)$ [63]

$b:\ \mathsf{SBit} = b_7$ [64]

$b:\ \mathsf{RQ} = q_8$ [65]

$b:\ \mathsf{SNo} = n_8$ [66]

Linker Unterzweig:

$a:\ \mathsf{SFile}(s(n_8)) = d_9$ [67]

$a:\ \mathsf{RQ} = q_8|\mathsf{msg}(\mathsf{SFile}(s(n_8)),\mathsf{flip}(b_7))$ [68]

$a:\ \mathsf{SNo} = s(n_8)$ [69]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_7)$ [70]

$\hookrightarrow$ S. 140

Rechter Unterzweig:

$a:\ \mathsf{SFile}(s(n_8)) = \bot$ [71]

$a:\ \mathsf{RQ} = q_8$ [72]

$a:\ \mathsf{SNo} = n_8$ [73]

$a:\ \mathsf{SBit} = b_7$ [74]

$a:\ \mathsf{ready} = \mathsf{true}$ [75]

$$\Box:\ \begin{array}{l} a:\ b_1 = \mathsf{SBit}\ [33] \\ a:\ \mathsf{SBit} = b_7\ [74] \\ \hline \rightarrow\ b_1 = b_7 \\ b:\ \neg(b_1 = \mathsf{SBit})\ [55] \\ b:\ \mathsf{SBit} = b_7\ [64] \\ \hline \rightarrow\ b_1 \neq b_7 \end{array}$$

Rechter Zweig:

$a:\ \mathsf{SBit} = b_6$ [62]

$$\Box:\ \begin{array}{l} a:\ b_1 = \mathsf{SBit}\ [33] \\ a:\ \mathsf{SBit} = b_6\ [62] \\ \hline \rightarrow\ b_1 = b_6 \\ b:\ \neg(b_1 = \mathsf{SBit})\ [55] \\ b:\ \mathsf{SBit} = b_6\ [59] \\ \hline \rightarrow\ b_1 \neq b_6 \end{array}$$

$\vdots$

von [70] (S. 139):

$b:\ \mathsf{RQ} = q_5|\mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5'' \quad [54]$

$b:\ \neg(b_1 = \mathsf{SBit}) \quad [55]$

$b:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7) \quad [63]$

$b:\ \mathsf{SBit} = b_7 \quad [64]$

Induktionsvoraussetzung A1:

$b:\ A1 \quad [13]:$

$$\begin{aligned} b:\ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow & \qquad [76] \\ (B = \mathsf{SBit} \rightarrow\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{RQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge \\ & (\mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge \\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3))) \end{aligned}$$

$$\begin{aligned} b:\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{10})) \rightarrow & \qquad [77] \\ (B_{10} = \mathsf{SBit} \rightarrow\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{RQ} = \mathsf{msg}(D^1, B_{10})|Q^1)) \wedge \\ & (\mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B_{10})) \wedge \\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B_{10})|Q^3))) \end{aligned}$$

$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{10})) \quad [78]$

$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{10}, B_{10})) \quad [79]$

$\Box\ \{D_{10} \leftarrow d_7,\ B_{10} \leftarrow b_7\}(63, 79)$

B_{10} einsetzen, weiter auflösen:

$b:\ \neg(b_7 = \mathsf{SBit}) \quad [80]$

$\Box\ (64, 80)$

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_7)|Q^1) \quad [81]$

$b:\ \mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_7) \quad [82]$

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_7)|Q^3) \quad [83]$

aus [83]:

$b:\ \mathsf{RQ} = \varepsilon \quad [84]$

$\Box\ (\mathrm{E}2, 54, 79)$

$b:\ \exists D^1, Q^1 : \mathsf{RQ} = \mathsf{msg}(D^1, b_7)|Q^1 \quad [85]$

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{10}^1, b_7)|q_{10}^1 \quad [86]$

$\hookrightarrow$ S. 141

$$\vdots$$

von [86] (S. 140):

$$b:\ \mathsf{RQ} = q_5|\mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5'' \quad [54]$$
$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [55]$$
$$b:\ \mathsf{SBit} = b_7 \quad [64]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_{10}^1, b_7)|q_{10}^1 \quad [86]$$

"Fallunterscheidung":

Q4: $$b:\ \forall Q, Q' : (\exists D, B : Q = Q'|\mathsf{msg}(D, B)) \rightarrow Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = \mathsf{msg}(D', B')|Q'') \quad [87]$$
$$b:\ (\exists D, B : Q_{11} = Q_{11}'|\mathsf{msg}(D, B)) \rightarrow Q_{11}' = \varepsilon \vee (\exists D', B', Q'' : Q_{11}' = \mathsf{msg}(D', B')|Q'') \quad [88]$$

$$b:\ \neg(\exists D, B : Q_{11} = Q_{11}'|\mathsf{msg}(D, B)) \quad [89]$$
$$b:\ \neg(Q_{11} = Q_{11}'|\mathsf{msg}(D_{11}, B_{11})) \quad [91]$$
$$\square\ \{Q_{11} \leftarrow q_5|\mathsf{msg}(d_5, b_1)\ , Q_{11}' \leftarrow q_5, \ldots\}(54, 91)$$

Q_{11}' einsetzen:

$$b:\ q_5 = \varepsilon \vee (\exists D', B', Q'' : q_5 = \mathsf{msg}(D', B')|Q'') \quad [90]$$

$$b:\ q_5 = \varepsilon \quad [92]$$

$$\boxed{\begin{array}{l}
\square\ b:\ q_5 = \varepsilon \quad [92] \\
\quad b:\ \mathsf{RQ} = q_5|\mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5'' \quad [54] \\
\hline
\quad b:\ \mathsf{RQ} = \mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5'' \\
\quad b:\ \mathsf{RQ} = \mathsf{msg}(d_{10}^1, b_7)|q_{10}^1 \quad [86] \\
\hline
\quad \rightarrow\ b_1 = b_7 \\
\quad b:\ \neg(b_1 = \mathsf{SBit}) \quad [55] \\
\quad b:\ \mathsf{SBit} = b_7 \quad [64] \\
\hline
\quad \rightarrow\ b_1 \neq b_7
\end{array}}$$

$$b:\ \exists D', B', Q'' : q_5 = Q''|\mathsf{msg}(D', B') \quad [93]$$
$$b:\ q_5 = \mathsf{msg}(d_{11}', b_{11}')|q_{11}'' \quad [94]$$

$\hookrightarrow$ S. 142

$$\vdots$$

von [94] (S. 141):

$$b:\ \mathsf{RQ} = q_5|\mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5'' \quad [54]$$
$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [55]$$
$$b:\ \mathsf{SBit} = b_7 \quad [64]$$
$$b:\ \mathsf{RQ} = \mathsf{msg}(d_{10}^1, b_7)|q_{10}^1 \quad [86]$$
$$b:\ q_5 = \mathsf{msg}(d_{11}', b_{11}')|q_{11}'' \quad [94]$$

Induktionsvoraussetzung A5:

$$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}) \quad [95]$$

$$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{12})|Q'|\mathsf{msg}(D', B_{12}')|Q'') \rightarrow (B_{12} = \mathsf{SBit} \rightarrow B_{12}' = \mathsf{SBit}) \quad [96]$$

$$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{12})|Q'|\mathsf{msg}(D', B_{12}')|Q'') \quad [97]$$
$$b:\ \neg(\mathsf{RQ} = Q_{12}|\mathsf{msg}(D_{12}, B_{12})|Q_{12}'|\mathsf{msg}(D_{12}', B_{12}')|Q_{12}'') \quad [99]$$

$$\boxed{\begin{array}{l} \Box\ b:\ \mathsf{RQ} = q_5|\mathsf{msg}(d_5, b_1)|q_5'|\mathsf{msg}(d_5', b_1')|q_5'' \quad [54] \\ \quad b:\ q_5 = \mathsf{msg}(d_{11}', b_{11}')|q_{11}'' \quad [94] \\ \quad b:\ \mathsf{RQ} = \mathsf{msg}(d_{10}^1, b_7)|q_{10}^1 \quad [86] \\ \quad \{Q_{12} \leftarrow \epsilon, D_{12} \leftarrow d_{10}^1, B_{12} \leftarrow b_7, Q_{12}' \leftarrow q_{11}'', D_{12}' \leftarrow d_5, \\ \quad\ B_{12}' \leftarrow b_1, Q_{12}'' \leftarrow q_5'|\mathsf{msg}(d_5', b_1')|q_5''\} \end{array}}$$

B_{12}, B_{12}' einsetzen:

$$b:\ b_7 = \mathsf{SBit} \rightarrow b_1 = \mathsf{SBit} \quad [98]$$

$$b:\ \neg(b_7 = \mathsf{SBit}) \quad [100] \qquad\qquad b:\ b_1 = \mathsf{SBit} \quad [101]$$
$$\Box\ (64, 100) \qquad\qquad \Box(55, 101)$$

$$\vdots$$

von [41] (S. 137):

$$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1,b_1)|q_1'|\mathsf{msg}(d_1',b_1')|q_1'' \quad [32]$$
$$a:\ b_1 = \mathsf{SBit} \quad [33]$$
$$a:\ \neg(b_1' = \mathsf{SBit}) \quad [34]$$
$$a:\ \mathsf{RLose} = \mathsf{true} \quad [41]$$

aus Tab. 0.3 mit SL2':

$$b:\ \mathsf{RQ} \neq \varepsilon \quad [102]$$

$$a:\ \neg(\mathsf{RQ} = Q_{13}|\mathsf{msg}(D_{13},B_{13})|Q_{13}'|\mathsf{msg}(D_{13}',B_{13}')|Q_{13}'') \quad [103]$$
$$\Box\ \{Q_{13} \leftarrow q_1, D_{13} \leftarrow d_1, B_{13} \leftarrow b_1, Q_{13}' \leftarrow q_1', D_{13}' \leftarrow d_1', B_{13}' \leftarrow b_1', Q_{13}'' \leftarrow q_1''\}(32,103)$$

$$b:\ \mathsf{RQ} = r_{13}|\mathsf{msg}(d_1,b_1)|r_{13}'|\mathsf{msg}(d_1',b_1')|r_{13}'' \quad [104]$$

Induktionsvoraussetzung A5:

aus $b:\ A5$ [17] :

$$b:\ \forall B,B' : (\exists D,D',Q,Q',Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q'|\mathsf{msg}(D',B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit}) \quad [105]$$

$$b:\ (\exists D,D',Q,Q',Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B_{14})|Q'|\mathsf{msg}(D',B_{14}')|Q'') \rightarrow (B_{14} = \mathsf{SBit} \rightarrow B_{14}' = \mathsf{SBit}) \quad [106]$$

$$b:\ \neg(\exists D,D',Q,Q',Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D,B_{14})|Q'|\mathsf{msg}(D',B_{14}')|Q'') \quad [107]$$
$$b:\ \neg(\mathsf{RQ} = Q_{14}|\mathsf{msg}(D_{14},B_{14})|Q_{14}'|\mathsf{msg}(D_{14}',B_{14}')|Q_{14}'') \quad [109]$$
$$\Box\ \{Q_{14} \leftarrow r_{13}, D_{14} \leftarrow d_1, B_{14} \leftarrow b_1,$$
$$Q_{14}' \leftarrow r_{13}', D_{14}' \leftarrow d_1', B_{14}' \leftarrow b_1', Q_{14}'' \leftarrow r_{13}''\}(104,109)$$

B_{14}, B_{14}' einsetzen:

$$b:\ b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit} \quad [108]$$

$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [110]$$

wie [55] mit
[104] anstelle [54],
[110] anstelle [55]

LG : $b:\ b_1 = \mathsf{SBit}$ [111]

$$b:\ b_1' = \mathsf{SBit} \quad [112]$$

$$\Box \quad \begin{array}{ll} b:\ b_1 = \mathsf{SBit}\ \ [111] & a:\ b_1 = \mathsf{SBit}\ \ [33] \\ b:\ b_1' = \mathsf{SBit}\ \ [112] & a:\ \neg(b_1' = \mathsf{SBit})\ \ [34] \\ \hline \rightarrow b_1 = b_1' & \rightarrow b_1 = b_1' \end{array}$$

$$\vdots$$

von [116] (S. 137):

$$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [32]$$

$$a:\ b_1 = \mathsf{SBit} \quad [33]$$

$$a:\ \neg(b_1' = \mathsf{SBit}) \quad [34]$$

$$b:\ \mathsf{RQ} = q_{15} \quad [113]$$

$$b:\ \mathsf{SBit} = b_{15} \quad [115]$$

$$a:\ \mathsf{RQ} = q_{15}|\mathsf{msg}(\mathsf{SFile}(n_{15}), b_{15}) \quad [116]$$

“Fallunterscheidung“ Q2:

$$a:\ \forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)|Q') \rightarrow Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B') \quad [117]$$

$$a:\ (\exists D, B : Q_{16} = \mathsf{msg}(D, B)|Q_{16}') \rightarrow Q_{16}' = \varepsilon \vee (\exists D', B', Q'' : Q_{16}' = Q''|\mathsf{msg}(D', B') \quad [118]$$

$$a:\ \neg(\exists D, B : Q_{16} = \mathsf{msg}(D, B)|Q_{16}') \quad [119]$$

$$a:\ \neg(Q_{16} = \mathsf{msg}(D_{16}, B_{16})|Q_{16}') \quad [121]$$

$$\Box\ \{Q_{16} \leftarrow \mathsf{msg}(d_1', b_1')|q_1'', Q_{16}' \leftarrow q_1''\}$$

Q_{16}' einsetzen:

$$a:\ q_1'' = \varepsilon \vee (\exists D', B', Q'' : q_1'' = Q''|\mathsf{msg}(D', B') \quad [120]$$

$$a:\ q_1'' = \varepsilon \quad [122]$$

↪ S. 145

$$a:\ \exists D', B', Q'' : q_1'' = Q''|\mathsf{msg}(D', B') \quad [123]$$

$$\boxed{a:\ q_1'' = q_{16}''|\mathsf{msg}(d_{16}', b_{16}') \quad [140]}$$

↪ S. 146

$$\vdots$$

von [122] (S. 144):

$$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [32]$$
$$a:\ b_1 = \mathsf{SBit} \quad [33]$$
$$a:\ \neg(b_1' = \mathsf{SBit}) \quad [34]$$
$$b:\ \mathsf{RQ} = q_{15} \quad [113]$$
$$b:\ \mathsf{SBit} = b_{15} \quad [115]$$
$$a:\ \mathsf{RQ} = q_{15}|\mathsf{msg}(\mathsf{SFile}(n_{15}), b_{15}) \quad [116]$$
$$a:\ q_1'' = \varepsilon \quad [122]$$

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \text{ unless}^+ \mathsf{ProcAck} = \mathsf{true}) \quad [124]$

mit Tab. 0.11, $\{B \leftarrow b_{15}\}$:

$$a:\ \mathsf{ProcAck} = \mathsf{true} \quad [125]$$

mit Tab. 0.7:

$$b:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_{17}) \quad [127]$$
$$b:\ \mathsf{SBit} = b_{17} \quad [128]$$
$$b:\ \mathsf{RQ} = q_{18} \quad [129]$$
$$b:\ \mathsf{SNo} = n_{18} \quad [130]$$

$$a:\ \mathsf{SBit} = b_{15} \quad [126]$$

□ : $a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [32]$
$a:\ q_1'' = \varepsilon \quad [122]$
$\rightarrow\ a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')$
$a:\ \mathsf{RQ} = q_{15}|\mathsf{msg}(\mathsf{SFile}(n_{15}), b_{15}) \quad [116]$
$\rightarrow\ b_1' = b_{15}$
$a:\ \neg(b_1' = \mathsf{SBit}) \quad [34]$
$a:\ \mathsf{SBit} = b_{15} \quad [126]$
$\rightarrow\ b_1' \neq b_{15}$

$$a:\ \mathsf{SFile}(s(n_{18})) = d_{19} \quad [131]$$
$$a:\ \mathsf{RQ} = q_{18}|\mathsf{msg}(\mathsf{SFile}(s(n_{18})), \mathsf{flip}(b_{17})) \quad [132]$$
$$a:\ \mathsf{SNo} = s(n_{18}) \quad [133]$$
$$a:\ \mathsf{SBit} = \mathsf{flip}(b_{17}) \quad [134]$$

$b:\ \mathsf{RQ} = q_{15} \quad [113]$
$b:\ \mathsf{RQ} = q_{18} \quad [129]$
$\rightarrow\ q_{15} = q_{18} b:\ \mathsf{SBit} = b_{15} \quad [115]$
$b:\ \mathsf{SBit} = b_{17} \quad [128]$
$\rightarrow\ b_{15} = b_{17}$
$a:\ \mathsf{RQ} = q_{15}|\mathsf{msg}(\mathsf{SFile}(n_{15}), b_{15}) \quad [116]$
$a:\ \mathsf{RQ} = q_{18}|\mathsf{msg}(\mathsf{SFile}(s(n_{18})), \mathsf{flip}(b_{17})) \quad [132]$
$\rightarrow\ b_{15} = \mathsf{flip}(b_{17})$

$$a:\ \mathsf{SFile}(s(n_{18})) = \bot \quad [135]$$
$$a:\ \mathsf{RQ} = q_{18} \quad [136]$$
$$a:\ \mathsf{SNo} = n_{18} \quad [137]$$
$$a:\ \mathsf{SBit} = b_{17} \quad [138]$$
$$a:\ \mathsf{ready} = \mathsf{true} \quad [139]$$

□ : wie [126]: SBit unverändert.

$\vdots$

von [140] (S. 144):

$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1''$ [32]

$a:\ b_1 = \mathsf{SBit}$ [33]

$a:\ \neg(b_1' = \mathsf{SBit})$ [34]

$b:\ \mathsf{RQ} = q_{15}$ [113]

$a:\ \mathsf{RQ} = q_{15}|\mathsf{msg}(\mathsf{SFile}(n_{15}), b_{15})$ [116]

$a:\ q_1'' = q_{16}''|\mathsf{msg}(d_{16}', b_{16}')$ [140]

|

Induktionsvoraussetzung A5:

aus $b:\ A5$ [17] :

$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \rightarrow (B = \mathsf{SBit} \rightarrow B' = \mathsf{SBit})$ [141]

|

$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{20})|Q'|\mathsf{msg}(D', B_{20}')|Q'') \rightarrow (B_{20} = \mathsf{SBit} \rightarrow B_{20}' = \mathsf{SBit})$ [142]

$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{20})|Q'|\mathsf{msg}(D', B_{20}')|Q'')$ [143]

$b:\ \neg(\mathsf{RQ} = Q_{20}|\mathsf{msg}(D_{20}, B_{20})|Q_{20}'|\mathsf{msg}(D_{20}', B_{20}')|Q_{20}'')$ [146]

□ $a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1''$ [32]
$a:\ q_1'' = q_{16}''|\mathsf{msg}(d_{16}', b_{16}')$ [140]

$\rightarrow$ $a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_{16}''|\mathsf{msg}(d_{16}', b_{16}')$
$b:\ \mathsf{RQ} = q_{15}$ [113]
$a:\ \mathsf{RQ} = q_{15}|\mathsf{msg}(\mathsf{SFile}(n_{15}), b_{15})$ [116]

$\rightarrow$ $b:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_{16}''$
$b:\ \neg(\mathsf{RQ} = Q_{20}|\mathsf{msg}(D_{20}, B_{20})|Q_{20}'|\mathsf{msg}(D_{20}', B_{20}')|Q_{20}'')$ [146]

$\{Q_{20} \leftarrow q_1, D_{20} \leftarrow d_1, B_{20} \leftarrow b_1, Q_{20}' \leftarrow q_1', D_{20}' \leftarrow d_1', B_{20}' \leftarrow b_1', Q_{20}'' \leftarrow q_{16}''\}$

B_{20}, B_{20}' einsetzen:

LG : $b:\ \exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, b_1)|Q'|\mathsf{msg}(D', b_1')|Q''$ [144]

$b:\ b_1 = \mathsf{SBit} \rightarrow b_1' = \mathsf{SBit}$ [145]

$b:\ \mathsf{RQ} = q_{21}|\mathsf{msg}(d_{21}, b_1)|q_{21}'|\mathsf{msg}(d_{21}', b_1')|q_{21}''$ [147]

$b:\ \neg(b_1 = \mathsf{SBit})$ [148]

wie [55]

LG : $b:\ b_1 = \mathsf{SBit}$ [149]

$b:\ b_1' = \mathsf{SBit}$ [150]

□ $b:\ b_1 = \mathsf{SBit}$ [149]	$a:\ b_1 = \mathsf{SBit}$ [33]
$b:\ b_1' = \mathsf{SBit}$ [150]	$a:\ \neg(b_1' = \mathsf{SBit})$ [34]
$\rightarrow b_1 = b_1'$	$\rightarrow b_1 = b_1'$

$\vdots$

von [43] (S. 137):

$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1''$ [32]

$a:\ b_1 = \mathsf{SBit}$ [33]

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [43]

|

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{22}, b_{22})$ [151]

$b:\ \mathsf{SBit} = b_{22}$ [152]

$b:\ \mathsf{RQ} = q_{23}$ [153]

$b:\ \mathsf{SNo} = n_{23}$ [154]

Linker Zweig:

$a:\ \mathsf{SFile}(s(n_{23})) = d_3$ [155]

$a:\ \mathsf{RQ} = q_{23}|\mathsf{msg}(\mathsf{SFile}(s(n_{23})), \mathsf{flip}(b_{22}))$ [156]

$a:\ \mathsf{SNo} = s(n_{23})$ [157]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{22})$ [158]

wie [70] (S. 140) mit :

$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1''$ [32]

$a:\ \mathsf{RQ} = q_{23}|\mathsf{msg}(\mathsf{SFile}(s(n_{23})), \mathsf{flip}(b_{22}))$ [156]

$b:\ \mathsf{RQ} = q_{23}$ [153]

$\rightarrow\ b:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_0$

$a:\ b_1 = \mathsf{SBit}$ [33]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_{22})$ [158]

$b:\ \mathsf{SBit} = b_{22}$ [152]

$\rightarrow\ b:\ \mathsf{SBit} = \mathsf{flip}(b_1)\ ;\ b: \neg(b_1 = \mathsf{SBit})$

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{22}, b_{22})$ [151]

$b:\ \mathsf{SBit} = b_{22}$ [152]

Rechter Zweig:

$a:\ \mathsf{SFile}(s(n_{23})) = \perp$ [159]

$a:\ \mathsf{RQ} = q_{23}$ [160]

$a:\ \mathsf{SNo} = n_{23}$ [161]

$a:\ \mathsf{SBit} = b_{22}$ [162]

$a:\ \mathsf{ready} = \mathsf{true}$ [163]

wie [39] (S. 148) mit :

$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1''$ [32]

$a:\ b_1 = \mathsf{SBit}$ [33]

$a:\ \neg(b_1' = \mathsf{SBit})$ [34]

$b:\ \mathsf{RQ} = q_{23}$ [153]

$a:\ \mathsf{RQ} = q_{23}$ [160]

$$\vdots$$

von [39] (S. 137):

$$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'|\mathsf{msg}(d_1', b_1')|q_1'' \quad [32]$$
$$a:\ b_1 = \mathsf{SBit} \quad [33]$$
$$a:\ \neg(b_1' = \mathsf{SBit}) \quad [34]$$
$$b:\ \mathsf{RQ} = q_2 \quad [36]$$
$$a:\ \mathsf{RQ} = q_2 \quad [39]$$

Induktionsvoraussetzung A5:

aus $b:\ A5$ [17] :

$$b:\ \forall B, B' : (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q'|\mathsf{msg}(D', B')|Q'') \to (B = \mathsf{SBit} \to B' = \mathsf{SBit}) \quad [164]$$

$$b:\ (\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{24})|Q'|\mathsf{msg}(D', B_{24}')|Q'') \to (B_{24} = \mathsf{SBit} \to B_{24}' = \mathsf{SBit}) \quad [165]$$

$$b:\ \neg(\exists D, D', Q, Q', Q'' : \mathsf{RQ} = Q|\mathsf{msg}(D, B_{24})|Q'|\mathsf{msg}(D', B_{24}')|Q'') \quad [166]$$
$$b:\ \neg(\mathsf{RQ} = Q_{24}|\mathsf{msg}(D_{24}, B_{24})|Q_{24}'|\mathsf{msg}(D_{24}', B_{24}')|Q_{24}'') \quad [168]$$

□ $a:\ \mathsf{RQ} = q_1\|\mathsf{msg}(d_1, b_1)\|q_1'\|\mathsf{msg}(d_1', b_1')\|q_1''$ [32]
$a:\ \mathsf{RQ} = q_2$ [35]
$b:\ \mathsf{RQ} = q_2$ [36]
$b:\ \neg(\mathsf{RQ} = Q_{24}\|\mathsf{msg}(D_{24}, B_{24})\|Q_{24}'\|\mathsf{msg}(D_{24}', B_{24}')\|Q_{24}'')$ [168]
$\{Q_{24} \leftarrow q_1, D_{24} \leftarrow d_1, B_{24} \leftarrow b_1, Q_{24}' \leftarrow q_1',$ $D_{24}' \leftarrow d_1', B_{24}' \leftarrow b_1', Q_{24}'' \leftarrow q_1''\}$

B_{24}, B_{24}' einsetzen:

$$b:\ b_1 = \mathsf{SBit} \to b_1' = \mathsf{SBit} \quad [167]$$

$$b:\ \neg(b_1 = \mathsf{SBit}) \quad [169]$$

wie [55]

LG : $b:\ b_1 = \mathsf{SBit}$ [170]

$$b:\ b_1' = \mathsf{SBit} \quad [171]$$

□ $b:\ b_1 = \mathsf{SBit}$ [170]	$a:\ b_1 = \mathsf{SBit}$ [33]
$b:\ b_1' = \mathsf{SBit}$ [171]	$a:\ \neg(b_1' = \mathsf{SBit})$ [34]
$\to b_1 = b_1'$	$\to b_1 = b_1'$

Damit ist der Beweis von Lemma 1 abgeschlossen.

6 Lemma 2: Quittung

$$\forall B : ((\exists D : \mathsf{SIM} = \mathsf{msg}(D,B)) \vee (\exists Q,Q',D' : \mathsf{SQ} = Q|\mathsf{msg}(D',B)|Q')) \rightarrow (\mathsf{SBit} = B \rightarrow \mathsf{RBit} = \mathsf{flip}(B))$$

Ist eine Nachricht (Quittung) mit Kontrollbit SBit auf dem (Rück)weg zum Sender, so erwartet der Empfänger bereits die nächste Nachricht.

Beweis:

Situation in a:

$\mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{SBit}$ oder SQ_a enthält eine Nachricht m mit $\mathsf{Bit}(m) = \mathsf{SBit}_a$ und $\mathsf{SBit}_a = \mathsf{RBit}_a$.

Man schließt zuerst $\mathsf{SBit}_a \neq \mathsf{SBit}_b$ aus: Dies könnte nur durch $\mathsf{ProcAck}$ geschehen, dessen Vorbedingung $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ ist, woraus mit Lemma 1, A1 folgt, daß alle in b existierenden Nachrichten ebenfalls SBit_b als Kontrollbit haben. Damit ist die in a beschriebene Situation unmöglich:
Wäre $\mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{SBit}_a = \mathsf{flip}(\mathsf{SBit}_b)$, so wäre $\mathsf{SIM}_a = \mathsf{SIM}_b$ (weder $\mathsf{SendCom}$ noch ClMsg angewendet) und so $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{SBit}_a = \mathsf{flip}(\mathsf{SBit}_b)$ gewesen. Enthielte SQ_a eine Nachricht mit Kontrollbit SBit_a, so wäre diese entweder auch schon in SQ_b enthalten gewesen, oder (AckMsg) $\mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_a)) = \mathsf{Bit}(\mathsf{RIM}_b) \neq \mathsf{SBit}_b$ gewesen.
Somit ist also $\mathsf{SBit}_a = \mathsf{SBit}_b$.

Im Weiteren unterscheidet man, ob die in a ausschlaggebende Nachricht in SIM oder SQ enthalten ist.

Sei also $\mathsf{SIM}_a \neq \bot$, $\mathsf{Bit}(\mathsf{SIM}_a) = \mathsf{SBit}_a$ und $\mathsf{SBit}_a = \mathsf{RBit}_a$. Durch Anwendung des EA-Axioms SIM und des entsprechenden Invarianzaxioms stellt man fest, daß entweder (keine Veränderung an SIM) $\mathsf{SIM}_b \neq \bot$ und $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ oder ($\mathsf{SendCom}$) $\mathsf{SQ}_b \neq \varepsilon$ und $\mathsf{Bit}(\mathsf{head}(\mathsf{SQ}_b)) = \mathsf{SBit}_b$, womit in beiden Fällen aus der Induktionsvoraussetzung $\mathsf{RBit}_a = \mathsf{SBit}_a = \mathsf{SBit}_b = \mathsf{flip}(\mathsf{RBit}_b)$ und aus Lemma 1, A1 oder A2, A3 $\mathsf{RIM}_b = \varepsilon \vee \mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{SBit}_b$ folgt.
Es müßte also RBit verändert, d.h. AccDat angewendet worden sein, dessen Vorbedingung $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{RBit}_b$ aber wegen $\mathsf{Bit}(\mathsf{RIM}) = \mathsf{SBit}_b = \mathsf{flip}(\mathsf{RBit}_b)$ nicht erfüllt ist.

Sei als zweite Möglichkeit $\mathsf{SQ}_a \neq \varepsilon$ und für eine Nachricht m in SQ ist $\mathsf{Bit}(m) = \mathsf{SBit}_a$ und $\mathsf{SBit}_a = \mathsf{RBit}_a$. Analog zu oben stellt man fest, daß diese Nachricht entweder schon in SQ_b enthalten war, oder durch AckMsg entstanden ist.
Im ersten Fall ergibt sich dasselbe Ergebnis, wie oben im Fall $\mathsf{SendCom}$.

Im zweiten Fall ergibt sich wegen der Vorbedingung $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{flip}(\mathsf{RBit}_b)$ für AccDat die Gleichungskette $\mathsf{RBit}_a = \mathsf{SBit}_a = \mathsf{Bit}(\mathsf{last}(\mathsf{SQ}_a)) = \mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{flip}(\mathsf{RBit}_b)$. Wieder müßte AccDat angewendet worden sein, dessen Vorbedingung aber wieder nicht erfüllt ist.

Der Beweis basiert auf dem Schema zur Durchführung eines Induktionsbeweises. Der Induktionsanfang ist trivial.

$$\vdots$$

$$p : [\,0, \{\neg(\neg A)\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$

$$a:\ \neg A \quad [9]$$

$$b:\ \neg(\neg A) \quad [12]$$

$$|$$

$$a:\ \neg(\forall B:\ ((\exists D : \mathsf{SIM} = \mathsf{msg}(D,B)) \vee (\exists Q,Q',D' : \mathsf{SQ} = Q|\mathsf{msg}(D',B)|Q')) \rightarrow (\mathsf{SBit} = B \rightarrow \mathsf{RBit} = \mathsf{flip}(B))) \quad [9]$$

$$|$$

$$b:\ \forall B:\ ((\exists D : \mathsf{SIM} = \mathsf{msg}(D,B)) \vee (\exists Q,Q',D' : \mathsf{SQ} = Q|\mathsf{msg}(D',B)|Q')) \rightarrow (\mathsf{SBit} = B \rightarrow \mathsf{RBit} = \mathsf{flip}(B)) \quad [12]$$

$$|$$

$b:$ Lemma 1 [13]

$$|$$

aus [9]:

$$a:\ \neg\ (((\exists D : \mathsf{SIM} = \mathsf{msg}(D,b_1)) \vee (\exists Q,Q',D' : \mathsf{SQ} = Q|\mathsf{msg}(D',b_1)|Q')) \rightarrow (\mathsf{SBit} = b_1 \rightarrow \mathsf{RBit} = \mathsf{flip}(b_1))) \quad [20]$$

$$|$$

$$a:\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D,b_1)) \vee (\exists Q,Q',D' : \mathsf{SQ} = Q|\mathsf{msg}(D',b_1)|Q') \quad [21]$$

$$a:\ \neg(\mathsf{SBit} = b_1 \rightarrow \mathsf{RBit} = \mathsf{flip}(b_1)) \quad [22]$$

$$a:\ \mathsf{SBit} = b_1 \quad [23]$$

$$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$$

$$|$$

aus EA:

$$b:\ \exists B : \mathsf{SBit} = B \quad [25]$$

$$b:\ \mathsf{SBit} = b_2 \quad [26]$$

$$|$$

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [27]

mit Tab. 0.11, $\{B \leftarrow b_2\}$:

Linker Zweig:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [28]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_3, b_3)$ [30]

$b:\ \mathsf{SBit} = b_3$ [31]

- $a:\ \mathsf{SBit} = \mathsf{flip}(b_3)$ [32]
  $\hookrightarrow$ S. 152
- $a:\ \mathsf{SBit} = b_3$ [33]
  wie [29] ff., da SBit unverändert

Rechter Zweig:

$a:\ \mathsf{SBit} = b_2$ [29]

$\hookrightarrow$ S. 156

$\vdots$

von [32] (S. 151):

$a: \ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, b_1)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', b_1)|Q') \quad [21]$

$a: \ \mathsf{SBit} = b_1 \quad [23]$

$b: \ \mathsf{SIM} = \mathsf{msg}(d_3, b_3) \quad [30]$

$b: \ \mathsf{SBit} = b_3 \quad [31]$

$a: \ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [32]$

aus Lemma 1, A1 für b:

$$\begin{aligned} b: \ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow & \qquad [34] \\ (B = \mathsf{SBit} \rightarrow \ & ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge \\ & (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge \\ & (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3)))) \end{aligned}$$

$b: \ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_4)) \rightarrow (B_4 = \mathsf{SBit} \rightarrow \ldots) \quad [35]$

$b: \ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_4)) \quad [36]$

$b: \ \neg(\mathsf{SIM} = \mathsf{msg}(D_4, B_4)) \quad [37]$

$\Box \ \{D_4 \leftarrow d_3, \ B_4 \leftarrow b_3\}(30, 37)$

[35] auflösen:

$b: \ \neg(b_3 = \mathsf{SBit}) \quad [38]$

$\Box \ (31, 38)$

$b: \ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_3)|Q^1) \quad [39]$

$b: \ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3) \quad [40]$

$b: \ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_3)|Q^3) \quad [41]$

aus [21]:

$a: \ \exists D : \mathsf{SIM} = \mathsf{msg}(D, b_1) \quad [42]$

$a: \ \mathsf{SIM} = \mathsf{msg}(d_5, b_1) \quad [44]$

$a: \ \exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', b_1)|Q' \quad [43]$

$a: \ \mathsf{SQ} = q_5|\mathsf{msg}(d_5', b_1)|q_5' \quad [54]$

$\hookrightarrow$ S. 153

$b: \ \forall M : \mathsf{SIM} = M \rightarrow \mathsf{A}(\mathsf{SIM} = M \ \mathsf{unless}^+ \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true}) \quad [45]$

mit Tab. 0.11, $\{M \leftarrow \mathsf{msg}(d_3, b_3)\}$:

$a: \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true} \quad [46]$

$a: \ \mathsf{SendCom} = \mathsf{true} \quad [48]$

aus Tab. 0.1:

$b: \ \mathsf{SIM} = \bot \quad [50]$

$b: \ \mathsf{SQ} = \mathsf{msg}(d_6, b_6)|q_6 \quad [51]$

$\Box \ (30, 50)$

$a: \ \mathsf{ClMsg} = \mathsf{true} \quad [49]$

aus Tab. 0.8:

$a: \ \mathsf{SIM} = \bot \quad [52]$

$b: \ \mathsf{SIM} = \mathsf{msg}(d_7, b_7) \quad [53]$

$\Box \ (\mathrm{E3}, 44, 52)$

$a: \ \mathsf{SIM} = \mathsf{msg}(d_3, b_3) \quad [47]$

$$\boxed{\begin{array}{ll} \Box : & a: \ \mathsf{SIM} = \mathsf{msg}(d_5, b_1) \quad [44] \\ & a: \ \mathsf{SIM} = \mathsf{msg}(d_3, b_3) \quad [47] \\ \hline & \rightarrow \ b_1 = b_3 \\ & a: \ \mathsf{SBit} = b_1 \quad [23] \\ & a: \ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [32] \\ \hline & \rightarrow \ b_1 = \mathsf{flip}(b_3) \end{array}}$$

$\vdots$

von [54] (S. 152):

$a:\ \mathsf{SBit} = b_1$ [23]

$b:\ \mathsf{SBit} = b_3$ [31]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_3)$ [32]

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_3)|Q^1)$ [39]

$b:\ \mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3)$ [40]

$a:\ \mathsf{SQ} = q_5|\mathsf{msg}(d_5', b_1)|q_5'$ [54]

aus EA:

$b:\ \exists Q : \mathsf{SQ} = Q$ [55]

$b:\ \mathsf{SQ} = q_8$ [56]

aus SQ:

$b:\ \forall Q : \mathsf{SQ} = Q \to \mathsf{A}(\mathsf{SQ} = Q \ \mathsf{unless}^+ \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [57]

aus Tab. 0.11, $\{Q \leftarrow q_8\}$:

$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [58]

$a:\ \mathsf{SQ} = q_8$ [59]

wie [68] mit
$a:\ \mathsf{SQ} = q_5\|\mathsf{msg}(d_5', b_1)\|q_5'$ [54]
$a:\ \mathsf{SQ} = q_8$ [59]
$b:\ q_8$ [56]
$\to\ b : \mathsf{SQ} = q_5\|\mathsf{msg}(d_5', b_1)\|q_5'$

$a:\ \mathsf{SendCom} = \mathsf{true}$ [60]

aus Tab. 0.1:

$b:\ \mathsf{SIM} = \perp$ [63]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_9, b_9)|q_9$ [64]

$a:\ \mathsf{SQ} = q_9$ [65]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_9, b_9)$ [66]

wie [68] mit
$a:\ \mathsf{SQ} = q_5\|\mathsf{msg}(d_5', b_1)\|q_5'$ [54]
$a:\ \mathsf{SQ} = q_9$ [65]
$b:\ \mathsf{SQ} = \mathsf{msg}(d_9, b_9)\|q_9$ [64]
$\to\ b : \mathsf{SQ} = \mathsf{msg}(d_9, b_9)\|q_5\|\mathsf{msg}(d_5', b_1)\|q_5'$

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [62]

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{13}, b_{13})$ [81]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{13})$ [82]

$b:\ \mathsf{SQ} = q_{14}$ [83]

$a:\ \mathsf{SQ} = q_{14}|\mathsf{msg}(\lambda, b_{13})$ [84]

$a:\ \mathsf{RIM} = \perp$ [85]

$\hookrightarrow$ S. 155

$a:\ \mathsf{SLose} = \mathsf{true}$ [61]

$a:\ \neg(\mathsf{SQ} = Q_{10}|\mathsf{msg}(D_{10}, B_{10})|Q_{10}')$ [67]

$\square\ \{Q_{10} \leftarrow q_5,\ D_{10} \leftarrow d_5',$
$B_{10} \leftarrow b_1, Q_{10}' \leftarrow q_5'\}$ (54, 67)

$b:\ \mathsf{SQ} = r_{10}|\mathsf{msg}(d_5', b_1)|r_{10}'$ [68]

$\hookrightarrow$ S. 154

$$\vdots$$

von [68] (S. 153):

$$a:\ \mathsf{SBit} = b_1 \quad [23]$$
$$b:\ \mathsf{SBit} = b_3 \quad [31]$$
$$a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [32]$$
$$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_3)|Q^1) \quad [39]$$
$$b:\ \mathsf{SQ} = r_{10}|\mathsf{msg}(d'_5, b_1)|r'_{10} \quad [68]$$

aus [39]:

$$b:\ \mathsf{SQ} = \varepsilon \quad [69]$$
$$\square\ (68, 69)$$

$$b:\ \exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_3)|Q^1 \quad [70]$$
$$b:\ \mathsf{SQ} = \mathsf{msg}(d^1_{11}, b_3)|q^1_{11} \quad [71]$$

mit Lemma1, A7:

$$b:\ \forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \rightarrow$$
$$(B = \mathsf{SBit} \rightarrow (\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit})) \quad [72]$$

$$b:\ (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{12})|Q) \rightarrow$$
$$(B_{12} = \mathsf{SBit} \rightarrow (\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit})) \quad [73]$$

$$b:\ \neg(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{12})|Q) \quad [74]$$
$$b:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_{12}, B_{12})|Q_{12}) \quad [75]$$
$$\square\ \{D_{12} \leftarrow d^1_{11},\ B_{12} \leftarrow b_3,\ Q_{12} \leftarrow q^1_{11}\}(71, 75)$$

[73] auflösen:

$$b:\ \neg(b_3 = \mathsf{SBit}) \quad [76]$$
$$\square\ (31, 76)$$

$$b:\ \forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit} \quad [77]$$
$$b:\ \mathsf{SQ} = Q'_{12}|\mathsf{msg}(D'_{12}, B'_{12})|Q''_{12} \rightarrow B'_{12} = \mathsf{SBit} \quad [78]$$

$$b:\ \neg(\mathsf{SQ} = Q'_{12}|\mathsf{msg}(D'_{12}, B'_{12})|Q''_{12}) \quad [79]$$
$$\square\ \{Q'_{12} \leftarrow r_{10},\ D'_{12} \leftarrow d'_5,\ B'_{12} \leftarrow b_1,\ Q''_{12} \leftarrow r'_{10}\}(68, 79)$$

$$b:\ b_1 = \mathsf{SBit} \quad [80]$$

$$\boxed{\begin{array}{ll} \square : & a:\ \mathsf{SBit} = b_1 \quad [23] \\ & a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [32] \\ \hline & \rightarrow\ b_1 = \mathsf{flip}(b_3) \\ & b:\ b_1 = \mathsf{SBit} \quad [80] \\ & b:\ \mathsf{SBit} = b_3 \quad [31] \\ \hline & \rightarrow\ b_1 = b_3 \end{array}}$$

$$\vdots$$

von [85] (S. 153):

$a:\ \mathsf{SBit} = b_1 \quad [23]$

$b:\ \mathsf{SBit} = b_3 \quad [31]$

$a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [32]$

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_3)|Q^1) \quad [39]$

$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3) \quad [40]$

$a:\ \mathsf{SQ} = q_5|\mathsf{msg}(d'_5, b_1)|q'_5 \quad [54]$

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{13}, b_{13}) \quad [81]$

$b:\ \mathsf{SQ} = q_{14} \quad [83]$

$a:\ \mathsf{SQ} = q_{14}|\mathsf{msg}(\lambda, b_{13}) \quad [84]$

mit Q2:

$a:\ \forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)|Q') \rightarrow Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B')) \quad [86]$

$a:\ (\exists D, B : Q_{15} = \mathsf{msg}(D, B)|Q'_{15}) \rightarrow Q'_{15} = \varepsilon \vee (\exists D', B', Q'' : Q'_{15} = Q''|\mathsf{msg}(D', B')) \quad [87]$

$a:\ \neg(\exists D, B : Q_{15} = \mathsf{msg}(D, B)|Q'_{15}) \quad [88]$

$a:\ \neg(Q_{15} = \mathsf{msg}(D_{15}, B_{15})|Q'_{15}) \quad [90]$

$\Box\ \{Q_{15} \leftarrow \mathsf{msg}(d'_5, b_1)|q'_5,\ Q'_{15} \leftarrow q'_5\}(54, 90)$

$a:\ q'_5 = \varepsilon \vee (\exists D', B', Q'' : q'_5 = Q''|\mathsf{msg}(D', B')) \quad [89]$

$a:\ q'_5 = \varepsilon \quad [91]$

aus [40]:

$b:\ \mathsf{RIM} = \bot \quad [93]$

$\Box\ (81, 93)$

$b:\ \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3) \quad [94]$

$b:\ \mathsf{RIM} = \mathsf{msg}(d^2_{16}, b_3) \quad [95]$

$$\Box : \quad \begin{array}{l} b:\ \mathsf{RIM} = \mathsf{msg}(d_{13}, b_{13}) \quad [81] \\ b:\ \mathsf{RIM} = \mathsf{msg}(d^2_{16}, b_3) \quad [95] \\ \hline \rightarrow b_{13} = b_3 \\ a:\ \mathsf{SBit} = b_1 \quad [23] \\ a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [32] \\ \hline \rightarrow b_1 = \mathsf{flip}(b_3) \end{array} \qquad \begin{array}{l} a:\ \mathsf{SQ} = q_5|\mathsf{msg}(d'_5, b_1)|q'_5 \quad [54] \\ a:\ q'_5 = \varepsilon \quad [91] \\ a:\ \mathsf{SQ} = q_{14}|\mathsf{msg}(\lambda, b_{13}) \quad [84] \\ \hline \rightarrow\ b_5 = b_{13} \end{array}$$

$a:\ \exists D', B', Q'' : q'_5 = Q''|\mathsf{msg}(D', B') \quad [92]$

$a:\ q'_5 = q''_{15}|\mathsf{msg}(d'_{15}, b'_{15}) \quad [96]$

$$\boxed{\begin{array}{l} \text{wie [68] mit} \\ a:\ \mathsf{SQ} = q_5|\mathsf{msg}(d'_5, b_1)|q'_5 \quad [54] \\ a:\ q'_5 = q''_{15}|\mathsf{msg}(d'_{15}, b'_{15}) \quad [96] \\ a:\ \mathsf{SQ} = q_{14}|\mathsf{msg}(\lambda, b_{13}) \quad [84] \\ b:\ \mathsf{SQ} = q_{14} \quad [83] \\ \hline \rightarrow\ b : \mathsf{SQ} = q_5|\mathsf{msg}(d'_5, b_1)|q''_{15} \end{array}}$$

$\vdots$

von [29] (S. 151):

$$a:\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, b_1)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', b_1)|Q') \quad [21]$$
$$a:\ \mathsf{SBit} = b_1 \quad [23]$$
$$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$$
$$b:\ \mathsf{SBit} = b_2 \quad [26]$$
$$a:\ \mathsf{SBit} = b_2 \quad [29]$$

aus [21]:

$$a:\ \exists D : \mathsf{SIM} = \mathsf{msg}(D, b_1) \quad [97]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1) \quad [99]$$

$$a:\ \exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', b_1)|Q' \quad [98]$$
$$a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17} \quad [164]$$

$\hookrightarrow$ S. 162

aus EA:

$$b:\ \exists M : \mathsf{SIM} = M \quad [100]$$
$$b:\ \mathsf{SIM} = m_{18} \quad [101]$$

aus SIM:

$$b:\ \forall M : \mathsf{SIM} = M \rightarrow \mathsf{A}(\mathsf{SIM} = M \ \mathsf{unless}^{+}\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true}) \quad [102]$$

mit Tab. 0.11, $\{M \leftarrow m_{18}\}$:

$$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true} \quad [103]$$

$$a:\ \mathsf{SIM} = m_{18} \quad [104]$$

$\hookrightarrow$ S. 160

$$a:\ \mathsf{SendCom} = \mathsf{true} \quad [105]$$

aus Tab. 0.1:

$$b:\ \mathsf{SIM} = \perp \quad [107]$$
$$b:\ \mathsf{SQ} = \mathsf{msg}(d_{19}, b_{19})|q_{19} \quad [108]$$
$$a:\ \mathsf{SQ} = q_{19} \quad [109]$$
$$a:\ \mathsf{SIM} = \mathsf{msg}(d_{19}, b_{19}) \quad [110]$$

$\hookrightarrow$ S. 157

$$a:\ \mathsf{CIMsg} = \mathsf{true} \quad [106]$$

aus Tab. 0.8:

$$a:\ \mathsf{SIM} = \perp \quad [146]$$
$$b:\ \mathsf{SIM} = \mathsf{msg}(d_{26}, b_{26}) \quad [147]$$
$$\square\ (\mathrm{E3}, 99, 146)$$

$\vdots$

von [110] (S. 156):

$a: \ \mathsf{SBit} = b_1$ [23]

$a: \ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$b: \ \mathsf{SBit} = b_2$ [26]

$a: \ \mathsf{SBit} = b_2$ [29]

$a: \ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1)$ [99]

$b: \ \mathsf{SQ} = \mathsf{msg}(d_{19}, b_{19})|q_{19}$ [108]

$a: \ \mathsf{SIM} = \mathsf{msg}(d_{19}, b_{19})$ [110]

aus Ind.Vor.:

$b: \ \forall B : ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B)|Q')) \rightarrow$ [111]
$(\mathsf{SBit} = B \rightarrow \mathsf{RBit} = \mathsf{flip}(B))$

$b: \ ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{20})) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{20})|Q')) \rightarrow$ [112]
$(\mathsf{SBit} = B_{20} \rightarrow \mathsf{RBit} = \mathsf{flip}(B_{20}))$

$b: \ \neg((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{20})) \vee$ [113]
$(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{20})|Q'))$

$b: \ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{20}))$ [114]

$b: \ \neg(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{20})|Q')$ [115]

$b: \ \neg(\mathsf{SQ} = Q_{20}|\mathsf{msg}(D'_{20}, B_{20})|Q'_{20})$ [116]

$\square \ \{Q_{20} \leftarrow \varepsilon, \ D'_{20} \leftarrow d_{19},$
$B_{20} \leftarrow b_{19}, \ Q'_{20} \leftarrow q_{19}\}(108, 116)$

[112] auflösen:

$b: \ \neg(\mathsf{SBit} = b_{19})$ [117]

$\square$:	$a: \ \mathsf{SBit} = b_1$ [23]
	$a: \ \mathsf{SBit} = b_2$ [29]
	$\rightarrow \ b_1 = b_2$
	$a: \ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1)$ [99]
	$a: \ \mathsf{SIM} = \mathsf{msg}(d_{19}, b_{19})$ [110]
	$\rightarrow \ b_1 = b_{19}$
	$b: \ \mathsf{SBit} = b_2$ [26]
	$b: \ \neg(\mathsf{SBit} = b_{19})$ [117]
	$\rightarrow \ b_2 \neq b_{19}$

$b: \ \mathsf{RBit} = \mathsf{flip}(b_{19})$ [118]

$\hookrightarrow$ S. 158

$\vdots$

von [118] (S. 157):

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1)$ [99]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{19}, b_{19})|q_{19}$ [108]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{19}, b_{19})$ [110]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{19})$ [118]

|

mit Lemma 1, A6:

$b:\ \forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \to (B = \mathsf{SBit} \to (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B)))$ [119]

$b:\ (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{21})|Q) \to (B_{21} = \mathsf{SBit} \to (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B_{21})))$ [120]

$b:\ \neg(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{21})|Q)$ [121]

$b:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_{21}, B_{21})|Q_{21})$ [123]

$\square\ \{D_{21} \leftarrow d_{19},\ B_{21} \leftarrow b_{19},\ Q_{21} \leftarrow q_{19}\}(108, 123)$

|

$b:\ B_{21} = \mathsf{SBit} \to (\exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B_{21}))$ [122]

$b:\ \neg(b_{19} = \mathsf{SBit})$ [124]

$\boxed{\text{wie [117]}}$

$b:\ \exists D', Q' : \mathsf{SQ} = Q'|\mathsf{msg}(D', b_{19})$ [125]

$b:\ \mathsf{SQ} = q'_{21}|\mathsf{msg}(d'_{21}, b_{19})$ [126]

Lemma 1, A3:

$$\begin{aligned} b:\ & \forall B : (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \to && [127]\\ & (B = \mathsf{SBit} \to\ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge \\ & \qquad (\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q'')))) \end{aligned}$$

|

$$\begin{aligned} b:\ & (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{22})) \to && [128]\\ & (B_{22} = \mathsf{SBit} \to\ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B_{22})) \wedge \\ & \qquad (\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B_{22})|Q'')))) \end{aligned}$$

$b:\ \neg(\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{22}))$ [129]

$b:\ \neg(\mathsf{SQ} = Q_{22}|\mathsf{msg}(D_{22}, B_{22}))$ [130]

$\square\ \{Q_{22} \leftarrow q'_{21},\ D_{22} \leftarrow d'_{21},\ B_{22} \leftarrow b_{19}\}(126, 130)$

[128] auflösen:

|

$b:\ \neg(b_{19} = \mathsf{SBit})$ [131]

$\boxed{\text{wie [117]}}$

$b:\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_{19})$ [132]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_{19})|Q'')$ [133]

$\hookrightarrow$ S. 159

$\vdots$

von [133] (S. 158):

$a: \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$a: \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1)$ [99]

$a: \mathsf{SIM} = \mathsf{msg}(d_{19}, b_{19})$ [110]

$b: \mathsf{RBit} = \mathsf{flip}(b_{19})$ [118]

$b: \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_{19})$ [132]

aus RBit: $b: \forall B : \mathsf{RBit} = B \to \mathsf{A}(\mathsf{RBit} = B \text{ unless}^{+} \mathsf{AccDat} = \mathsf{true})$ [134]

mit Tab. 0.11, $\{B \leftarrow \mathsf{flip}(b_{19})\}$:

$a: \mathsf{AccDat} = \mathsf{true}$ [135]

mit Tab. 0.9:

$b: \mathsf{RIM} = \mathsf{msg}(d_{23}, b_{23})$ [137]

$b: \mathsf{RBit} = b_{23}$ [138]

$b: \mathsf{RNo} = n_{24}$ [139]

$a: \mathsf{RFile}(n_{24}) = d_{23}$ [140]

$a: \mathsf{RNo} = s(n_{24})$ [141]

$a: \mathsf{RBit} = \mathsf{flip}(b_{23})$ [142]

aus [132]:

$b: \mathsf{RIM} = \bot$ [143]

$\Box$ (E3, 137, 143)

$b: \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_{19})$ [144]

$b: \mathsf{RIM} = \mathsf{msg}(d'_{25}, b_{19})$ [145]

$$\boxed{\begin{array}{ll} \Box : & b: \mathsf{RIM} = \mathsf{msg}(d'_{25}, b_{19}) \quad [145] \\ & b: \mathsf{RIM} = \mathsf{msg}(d_{23}, b_{23}) \quad [137] \\ \hline & \to b_{19} = b_{23} \\ & b: \mathsf{RBit} = b_{23} \quad [138] \\ & b: \mathsf{RBit} = \mathsf{flip}(b_{19}) \quad [118] \\ \hline & \to b_{23} = \mathsf{flip}(b_{19}) \end{array}}$$

$a: \mathsf{RBit} = \mathsf{flip}(b_{19})$ [136]

$$\boxed{\begin{array}{ll} \Box : & a: \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1) \quad [99] \\ & a: \mathsf{SIM} = \mathsf{msg}(d_{19}, b_{19}) \quad [110] \\ \hline & \to b_1 = b_{19} \\ & a: \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24] \\ & a: \mathsf{RBit} = \mathsf{flip}(b_{19}) \quad [136] \\ \hline & \to b_1 \neq b_{19} \end{array}}$$

$\vdots$

von [104] (S. 156):

$a:\ \mathsf{SBit} = b_1$ [23]

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$b:\ \mathsf{SBit} = b_2$ [26]

$a:\ \mathsf{SBit} = b_2$ [29]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1)$ [99]

$b:\ \mathsf{SIM} = m_{18}$ [101]

$a:\ \mathsf{SIM} = m_{18}$ [104]

|

aus Ind.Vor.:

$b:\ \forall B : ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B)|Q')) \rightarrow$ [148]
$(\mathsf{SBit} = B \rightarrow \mathsf{RBit} = \mathsf{flip}(B))$

|

$b:\ ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{27})) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{27})|Q')) \rightarrow$ [149]
$(\mathsf{SBit} = B_{27} \rightarrow \mathsf{RBit} = \mathsf{flip}(B_{27}))$

$b:\ \neg((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{27})) \vee$ [150]
$(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{27})|Q'))$

|

$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{27}))$ [151]

$b:\ \neg(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{27})|Q')$ [152]

$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{27}, B_{27}))$ [153]

$\square:$ $a:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1)$ [99]
$a:\ \mathsf{SIM} = m_{18}$ [104]
$b:\ \mathsf{SIM} = m_{18}$ [101]
$\{D_{27} \leftarrow d_{17},\ B_{27} \leftarrow b_1\}$

[149] auflösen:

$b:\ \neg(\mathsf{SBit} = b_1)$ [154]

$\square:$ $a:\ \mathsf{SBit} = b_1$ [23]
$a:\ \mathsf{SBit} = b_2$ [29]
$\rightarrow\ b_1 = b_2$
$b:\ \mathsf{SBit} = b_2$ [26]
$b:\ \neg(\mathsf{SBit} = b_1)$ [154]
$\rightarrow\ b_2 \neq b_1$

$b:\ \mathsf{RBit} = \mathsf{flip}(b_1)$ [155]

$\hookrightarrow$ S. 161

$\vdots$

von [155] (S. 160):

$a:\ \mathsf{SBit} = b_1$ [23]

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$b:\ \mathsf{SBit} = b_2$ [26]

$a:\ \mathsf{SBit} = b_2$ [29]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1)$ [99]

$b:\ \mathsf{SIM} = m_{18}$ [101]

$a:\ \mathsf{SIM} = m_{18}$ [104]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_1)$ [155]

$$\begin{aligned} b:\ &\forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow & [156]\\ &(B = \mathsf{SBit} \rightarrow ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge\\ &\quad (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge\\ &\quad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3))))\end{aligned}$$

$$\begin{aligned} b:\ &(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{28})) \rightarrow & [157]\\ &(B_{28} = \mathsf{SBit} \rightarrow ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B_{28})|Q^1)) \wedge\\ &\quad (\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B_{28})) \wedge\\ &\quad (\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B_{28})|Q^3))))\end{aligned}$$

$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{28}))$ [158]

$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{28}, B_{28}))$ [159]

$\Box:$ $a:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1)$ [99]
$a:\ \mathsf{SIM} = m_{18}$ [104]
$b:\ \mathsf{SIM} = m_{18}$ [101]
$\{D_{28} \leftarrow d_{17},\ B_{28} \leftarrow b_1\}$

[157] auflösen:

$b:\ \neg(\mathsf{SBit} = b_1)$ [160]

wie [154]

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B_{28})|Q^1)$ [161]

$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B_{28})$ [162]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B_{28})|Q^3)$ [163]

$\Box:$ wie [133] (S.159) mit
$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]
$a:\ \mathsf{SIM} = \mathsf{msg}(d_{17}, b_1)$ [99]
$b:\ \mathsf{RBit} = \mathsf{flip}(b_1)$ [155]
$b:\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_{19})$ [162]

$\vdots$

von [164] (S. 156):

$a:\ \mathsf{SBit} = b_1$ [23]

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$b:\ \mathsf{SBit} = b_2$ [26]

$a:\ \mathsf{SBit} = b_2$ [29]

$a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17}$ [164]

aus EA:

$b:\ \exists Q : \mathsf{SQ} = Q$ [165]

$b:\ \mathsf{SQ} = q_{29}$ [166]

aus SQ:

$b:\ \forall Q : \mathsf{SQ} = Q \rightarrow \mathsf{A}(\mathsf{SQ} = Q\ \mathsf{unless}^+\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [167]

aus Tab. 0.11:

$a:\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [168]

$a:\ \mathsf{SQ} = q_{29}$ [169]

$\hookrightarrow$ S. 164

relevant ist nur

$a:\ \mathsf{SQ} = q_2$ [169]

$b:\ \mathsf{SQ} = q_{29}$ [166]

$a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17}$ [164]

$\rightarrow b : \mathsf{SQ} = q|\mathsf{msg}(d'_{17}, b_1)|\bar{q}$

$a:\ \mathsf{SendCom} = \mathsf{true}$ [170]

aus Tab. 0.1:

$b:\ \mathsf{SIM} = \perp$ [173]

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{30}, b_{30})|q_{30}$ [174]

$a:\ \mathsf{SQ} = q_{30}$ [175]

$a:\ \mathsf{SIM} = \mathsf{msg}(d_{30}, b_{30})$ [176]

wie [169] mit

$b:\ \mathsf{SQ} = \mathsf{msg}(d_{30}, b_{30})|q_{30}$ [174]

$a:\ \mathsf{SQ} = q_{30}$ [175]

$a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17}$ [164]

$\rightarrow b : \mathsf{SQ} = \mathsf{msg}(d_{30}, b_{30})|q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17}$

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [172]

aus Tab. 0.10:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{32}, b_{32})$ [179]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{32})$ [180]

$b:\ \mathsf{SQ} = q_{33}$ [181]

$a:\ \mathsf{SQ} = q_{33}|\mathsf{msg}(\lambda, b_{32})$ [182]

$a:\ \mathsf{RIM} = \perp$ [183]

$\hookrightarrow$ S. 163

$a:\ \mathsf{SLose} = \mathsf{true}$ [171]

$a:\ \neg(\mathsf{SQ} = Q_{31}|\mathsf{msg}(D_{31}, B_{31})|Q'_{31})$ [177]

$\square\ \{Q_{31} \leftarrow q_{17},\ D_{31} \leftarrow d'_{17},$
$B_{31} \leftarrow b_1, Q'_{31} \leftarrow q'_{17}\}\ (164, 177)$

$b:\ \mathsf{SQ} = r_{31}|\mathsf{msg}(d'_{17}, b_1)|r'_{31}$ [178]

wie [169] mit

$b:\ \mathsf{SQ} = r_{31}|\mathsf{msg}(d'_{17}, b_1)|r'_{31}$ [178]

$\vdots$

von [183] (S. 162):

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17}$ [164]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{32}, b_{32})$ [179]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{32})$ [180]

$b:\ \mathsf{SQ} = q_{33}$ [181]

$a:\ \mathsf{SQ} = q_{33}|\mathsf{msg}(\lambda, b_{32})$ [182]

aus Q2:

$b:\ \forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)|Q') \rightarrow Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B'))$ [184]

$b:\ (\exists D, B : Q_{34} = \mathsf{msg}(D, B)|Q'_{34}) \rightarrow Q'_{34} = \varepsilon \vee (\exists D', B', Q'' : Q'_{34} = Q''|\mathsf{msg}(D', B'))$ [185]

$b:\ \neg(\exists D, B : Q_{34} = \mathsf{msg}(D, B)|Q'_{34})$ [186]

$b:\ \neg(Q_{34} = \mathsf{msg}(D_{34}, B_{34})|Q'_{34})$ [188]

$\Box\ \{Q_{34} \leftarrow \mathsf{msg}(d'_{17}, b_1)|q'_{17},\ Q'_{34} \leftarrow q'_{17}\}(164, 188)$

$b:\ q'_{17} = \varepsilon \vee (\exists D', B', Q'' : q'_{17} = Q''|\mathsf{msg}(D', B'))$ [187]

$b:\ q'_{17} = \varepsilon$ [189]

aus RBit:

$b:\ \forall B : \mathsf{RBit} = B \rightarrow$ [191]

$\mathsf{A}(\mathsf{RBit} = B\ \mathsf{unless}^{+}\ \mathsf{AccDat} = \mathsf{true})$

mit Tab. 0.11, $\{B \leftarrow \mathsf{flip}(b_{32})\}$:

$a:\ \mathsf{AccDat} = \mathsf{true}$ [192]

mit Tab. 0.9:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{35}, b_{35})$ [194]

$b:\ \mathsf{RBit} = b_{35}$ [195]

$a:\ \mathsf{RBit} = \mathsf{flip}(b_{35})$ [196]

$\Box:$
$b:\ \mathsf{RIM} = \mathsf{msg}(d_{32}, b_{32})$ [179]
$b:\ \mathsf{RIM} = \mathsf{msg}(d_{35}, b_{35})$ [194]
$\rightarrow\ b_{32} = b_{35}$
$b:\ \mathsf{RBit} = \mathsf{flip}(b_{32})$ [180]
$b:\ \mathsf{RBit} = b_{35}$ [195]
$\rightarrow\ \mathsf{flip}(b_{32}) = b_{35}$

$a:\ \mathsf{RBit} = \mathsf{flip}(b_{32})$ [193]

$\Box:$
$a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17}$ [164]
$b:\ q'_{17} = \varepsilon$ [189]
$a:\ \mathsf{SQ} = q_{33}|\mathsf{msg}(\lambda, b_{32})$ [182]
$\rightarrow b_1 = b_{32}$
$a:\ \mathsf{RBit} = \mathsf{flip}(b_{32})$ [186]
$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]
$\rightarrow b_1 \neq b_{32}$

$b:\ \exists D', B', Q'' : q'_{17} = Q''|\mathsf{msg}(D', B')$ [190]

$b:\ q'_{17} = q''_{34}|\mathsf{msg}(D'_{34}, B'_{34})$ [197]

wie [169] mit
$a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17}$ [164]
$b:\ q'_{17} = q''_{34}|\mathsf{msg}(D'_{34}, B'_{34})$ [197]
$a:\ \mathsf{SQ} = q_{33}|\mathsf{msg}(\lambda, b_{32})$ [182]
$b:\ \mathsf{SQ} = q_{33}$ [181]
$\rightarrow b : \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q''_{34}$

$\vdots$

von [169] (S. 162):

$a:\ \mathsf{SBit} = b_1 \quad [23]$

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$

$b:\ \mathsf{SBit} = b_2 \quad [26]$

$a:\ \mathsf{SBit} = b_2 \quad [29]$

$a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17} \quad [164]$

$b:\ \mathsf{SQ} = q_{29} \quad [166]$

$a:\ \mathsf{SQ} = q_{29} \quad [169]$

aus Ind.Vor.:

$b:\ \forall B : ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B)|Q')) \rightarrow$ [198]
$(\mathsf{SBit} = B \rightarrow \mathsf{RBit} = \mathsf{flip}(B))$

$b:\ ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{36})) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{36})|Q')) \rightarrow$ [199]
$(\mathsf{SBit} = B_{36} \rightarrow \mathsf{RBit} = \mathsf{flip}(B_{36}))$

$b:\ \neg((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{36})) \vee$ [200]
$(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{36})|Q'))$

$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{36})) \quad [201]$

$b:\ \neg(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{36})|Q') \quad [202]$

$b:\ \neg(\mathsf{SQ} = Q_{36}|\mathsf{msg}(D'_{36}, B_{36})|Q'_{36}) \quad [203]$

$\square:\ a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17} \quad [164]$
$b:\ \mathsf{SQ} = q_{29} \quad [166]$
$a:\ \mathsf{SQ} = q_{29} \quad [169]$
$\rightarrow\ b:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17}$
$\{Q_{36} \leftarrow q_{17},\ D'_{36} \leftarrow d'_{17},\ B_{36} \leftarrow b_1,\ Q'_{36} \leftarrow q'_{17}\}$

[199] auflösen:

$b:\ \neg(\mathsf{SBit} = b_1) \quad [204]$

$\square:\ a:\ \mathsf{SBit} = b_1 \quad [23]$
$a:\ \mathsf{SBit} = b_2 \quad [29]$
$\rightarrow\ b_1 = b_2$
$b:\ \mathsf{SBit} = b_2 \quad [26]$
$b:\ \neg(\mathsf{SBit} = b_1) \quad [204]$
$\rightarrow\ b_2 \neq b_1$

$b:\ \mathsf{RBit} = \mathsf{flip}(b_1) \quad [205]$

$\hookrightarrow$ S. 165

$\vdots$

von [205] (S. 164):

$a:\ \mathsf{SBit} = b_1 \quad [23]$

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$

$b:\ \mathsf{SBit} = b_2 \quad [26]$

$a:\ \mathsf{SBit} = b_2 \quad [29]$

$a:\ \mathsf{SQ} = q_{17}|\mathsf{msg}(d'_{17}, b_1)|q'_{17} \quad [164]$

$b:\ \mathsf{SQ} = q_{29} \quad [166]$

$a:\ \mathsf{SQ} = q_{29} \quad [169]$

$b:\ \mathsf{RBit} = \mathsf{flip}(b_1) \quad [205]$

aus Lemma 1, A8:

$b:\ \forall B : (\exists D, Q, Q' : \mathsf{SQ} = Q|\mathsf{msg}(D, B)|Q') \to (B = \mathsf{SBit} \to (\exists D', Q'' : \mathsf{SQ} = Q''|\mathsf{msg}(D', B))) \quad [206]$

$b:\ (\exists D, Q, Q' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{37})|Q') \to (B_{37} = \mathsf{SBit} \to (\exists D', Q'' : \mathsf{SQ} = Q''|\mathsf{msg}(D', B_{37}))) \quad [207]$

$b:\ \neg(\exists D, Q, Q' : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{37})|Q') \quad [208]$

$b:\ \neg(\mathsf{SQ} = Q_{37}|\mathsf{msg}(D_{37}, B_{37})|Q'_{37}) \quad [209]$

$\square$ wie [203]: $\{Q_{37} \leftarrow q_{17},\ D_{37} \leftarrow d'_{17},$
$B_{37} \leftarrow b_1,\ Q'_{37} \leftarrow q'_{17}\}$

[207] auflösen:

$b:\ \neg(b_1 = \mathsf{SBit}) \quad [210]$

$\square$ wie [204]

$b:\ \exists D', Q'' : \mathsf{SQ} = Q''|\mathsf{msg}(D', b_1) \quad [211]$

$b:\ \mathsf{SQ} = q''_{37}|\mathsf{msg}(d'_{37}, b_1) \quad [212]$

Lemma 1, A3:

$b:\ \forall B : (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B)) \to \quad [213]$
$(B = \mathsf{SBit} \to \ ((\mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', B)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', B)|Q''))))$

$b:\ (\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{38})) \to (B_{38} = \mathsf{SBit} \to (\ldots)) \quad [214]$

$b:\ \neg(\exists D, Q : \mathsf{SQ} = Q|\mathsf{msg}(D, B_{38})) \quad [215]$

$b:\ \neg(\mathsf{SQ} = Q_{38}|\mathsf{msg}(D_{38}, B_{38})) \quad [216]$

$\square\ \{Q_{38} \leftarrow q''_{37},\ D_{38} \leftarrow d'_{37},\ B_{38} \leftarrow b_1\}(212, 216)$

$b:\ \neg(b_1 = \mathsf{SBit}) \quad [217]$

$\square$ wie [204]

[214] auflösen:

$b:\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1) \quad [218]$

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D'', Q'' : \mathsf{RQ} = \mathsf{msg}(D'', b_1)|Q'') \quad [219]$

$\square$: wie [133] (S.159) mit
$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$
$b:\ \mathsf{RBit} = \mathsf{flip}(b_1) \quad [205]$
$b:\ \mathsf{RIM} = \bot \vee \exists D' : \mathsf{RIM} = \mathsf{msg}(D', b_1) \quad [218]$

7 Lemma 3: Alte Nachrichten

$$\mathsf{A}\Box(\forall B : ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B)|Q')) \rightarrow$$
$$(\mathsf{SBit} = \mathsf{flip}(B) \rightarrow \mathsf{RBit} = \mathsf{flip}(B)))$$

Sind noch Nachrichten unterwegs, deren Kontrollbit nicht mit dem Kontrollbit des Senders übereinstimmt, so interessieren sie den Empfänger ebenfalls nicht mehr.

Beweis: Induktionsbeweis. Der Induktionsanfang ist trivial.

Situation in a: $\mathsf{Bit}(\mathsf{RIM}_a) = \mathsf{flip}(\mathsf{SBit}_a)$ oder RQ_a enthält eine Nachricht m mit $\mathsf{Bit}(m) = \mathsf{flip}(\mathsf{SBit}_a)$ und $\mathsf{SBit}_a = \mathsf{flip}(\mathsf{RBit}_a)$.

Wieder schließt man zuerst $\mathsf{SBit}_a \neq \mathsf{SBit}_b$ aus: Dies könnte nur durch $\mathsf{ProcAck}$ geschehen, dessen Vorbedingung $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ ist, woraus mit Lemma 1, A1 folgt, daß alle in b existierenden Nachrichten ebenfalls SBit_b als Kontrollbit haben. Insbesondere ist RIM_b leer, oder $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{SBit}_b$.
Aus der genannten Bedingung folgt mit Lemma 2 weiterhin, daß $\mathsf{SBit}_b = \mathsf{flip}(\mathsf{RBit}_b)$, also $\mathsf{SBit}_a = \mathsf{flip}(\mathsf{SBit}_b) = \mathsf{RBit}_b$.
Aufgrund der für a angenommenen Situation ist also $\mathsf{RBit}_a = \mathsf{flip}(\mathsf{RBit}_b)$, woraus folgt, daß AccDat angewendet wurde. Dazu müßte $\mathsf{RIM}_b \neq \perp$ und $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{RBit}_b = \mathsf{flip}(\mathsf{SBit}_b)$ sein.

Im Weiteren unterscheidet man, ob die in a ausschlaggebende Nachricht in RIM oder RQ enthalten ist.

Sei also $\mathsf{RIM}_a \neq \perp$, $\mathsf{Bit}(\mathsf{RIM}_a) = \mathsf{flip}(\mathsf{SBit}_a)$ und $\mathsf{SBit}_a = \mathsf{flip}(\mathsf{RBit}_a)$. Durch Anwendung des EA-Axioms RIM und des entsprechenden Invarianzaxioms stellt man fest, daß entweder (keine Veränderung an RIM) $\mathsf{RIM}_b \neq \perp$ und $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{flip}(\mathsf{SBit}_b)$ oder (RecCom) RIM_b leer und $\mathsf{RQ}_b \neq \varepsilon$ mit $\mathsf{Bit}(\mathsf{head}(\mathsf{RQ}_b)) = \mathsf{flip}(\mathsf{SBit}_b)$ ist, womit in beiden Fällen aus der Induktionsvoraussetzung $\mathsf{flip}(\mathsf{SBit}_b) = \mathsf{flip}(\mathsf{RBit}_b)$ folgt. Damit hat man für a $\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a) = \mathsf{flip}(\mathsf{SBit}_b) = \mathsf{flip}(\mathsf{RBit}_b)$. Andererseits kann sich RBit nicht verändert haben, da AccDat nicht anwendbar ist: RIM_b ist leer, oder es ist $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{flip}(\mathsf{SBit}_b) = \mathsf{flip}(\mathsf{RBit}_b)$.

Sei als zweite Möglichkeit $\mathsf{RQ}_a \neq \varepsilon$ und für eine Nachricht m in RQ ist $\mathsf{Bit}(m) = \mathsf{flip}(\mathsf{SBit}_a)$ und $\mathsf{SBit}_a = \mathsf{RBit}_a$. Analog zu oben stellt man fest, daß diese Nachricht entweder schon in RQ_b enthalten war, oder durch $\mathsf{ReTrans}$ oder $\mathsf{ProcAck}$ entstanden ist. $\mathsf{ProcAck}$ kann ausgeschlossen werden, da es nur eine Nachricht anhängt, wenn es auch SBit verändert. Im Falle von $\mathsf{ReTrans}$ ist das Kontrollbit der neuen Nachricht $\mathsf{SBit}_b = \mathsf{SBit}_a$, also kann auch dieser Fall ausgeschlossen werden.
War die Nachricht schon in RQ_b enthalten, so erhält man wegen $\mathsf{SBit}_a = \mathsf{SBit}_b$ aus der Induktionsvoraussetzung $\mathsf{RBit}_b = \mathsf{SBit}_b$, also $\mathsf{RBit}_a \neq \mathsf{RBit}_b$. Folglich ist RBit verändert worden, was nur durch AccDat geschehen kann. Man erhält die Vorbedingung $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{RBit}_b = \mathsf{SBit}_b$, womit nach Lemma 1, A4 alle Nachrichten in RQ_b ebenfalls SBit_b als Kontrollbit haben. Insbesondere also $\mathsf{Bit}(m) = \mathsf{SBit}_b = \mathsf{SBit}_a$ im Widerspruch zur Annahme.

$$\vdots$$

$$p : [\,0, \{\neg(\neg A)\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$

$$a : \ \neg A \quad [9]$$

$$b : \ \neg(\neg A) \quad [12]$$

$$a : \ \neg(\forall B : \ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B)) \lor (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B)|Q')) \to \quad [9]$$
$$(\mathsf{SBit} = \mathsf{flip}(B) \to \mathsf{RBit} = \mathsf{flip}(B)))$$

$$b : \ \forall B : \ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B)) \lor (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B)|Q')) \to \quad [12]$$
$$(\mathsf{SBit} = \mathsf{flip}(B) \to \mathsf{RBit} = \mathsf{flip}(B))$$

$b :$ Lemma 1 [13]

$b :$ Lemma 2 [14]

aus [9]:

$$a : \ \neg \ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, b_1)) \lor (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', b_1)|Q')) \to \quad [20]$$
$$(\mathsf{SBit} = \mathsf{flip}(b_1) \to \mathsf{RBit} = \mathsf{flip}(b_1)))$$

$$a : \ (\exists D : \mathsf{RIM} = \mathsf{msg}(D, b_1)) \lor (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', b_1)|Q') \quad [21]$$

$$a : \ \neg(\mathsf{SBit} = \mathsf{flip}(b_1) \to \mathsf{RBit} = \mathsf{flip}(b_1)) \quad [22]$$

$$a : \ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [23]$$

$$a : \ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$$

aus EA:

$$b : \ \exists B : \mathsf{SBit} = B \quad [25]$$

$$b : \ \mathsf{SBit} = b_2 \quad [26]$$

aus SBit: $b : \ \forall B : \mathsf{SBit} = B \to \mathsf{A}(\mathsf{SBit} = B \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true})$ [27]

mit Tab. 0.11, $\{B \leftarrow b_2\}$:

$a : \ \mathsf{ProcAck} = \mathsf{true}$ [28]

mit Tab. 0.7:

$b : \ \mathsf{SIM} = \mathsf{msg}(d_3, b_3)$ [30]

$b : \ \mathsf{SBit} = b_3$ [31]

$a : \ \mathsf{SBit} = \mathsf{flip}(b_3)$ [32]

$\hookrightarrow$ S. 168

$a : \ \mathsf{SBit} = b_3$ [33]

wie [29] ff., da SBit unverändert

$a : \ \mathsf{SBit} = b_2$ [29]

$\hookrightarrow$ S. 170

$\vdots$

von [32] (S. 167):

$a: \ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [23]$

$a: \ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$

$b: \ \mathsf{SIM} = \mathsf{msg}(d_3, b_3) \quad [30]$

$b: \ \mathsf{SBit} = b_3 \quad [31]$

$a: \ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [32]$

aus Lemma 1, A1 für b:

$$b: \ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \rightarrow \quad [34]$$
$$(B = \mathsf{SBit} \rightarrow \ ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge$$
$$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge$$
$$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3))))$$

$b: \ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_4)) \rightarrow (B_4 = \mathsf{SBit} \rightarrow \ldots) \quad [35]$

$b: \ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_4)) \quad [36]$

$b: \ \neg(\mathsf{SIM} = \mathsf{msg}(D_4, B_4)) \quad [37]$

$\square \ \{D_4 \leftarrow d_3, \ B_4 \leftarrow b_3\}(30, 37)$

[35] auflösen:

$b: \ \neg(b_3 = \mathsf{SBit}) \quad [38]$

$\square \ (31, 38)$

$b: \ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_3)|Q^1) \quad [39]$

$b: \ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3) \quad [40]$

$b: \ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_3)|Q^3) \quad [41]$

aus Lemma 2:

$$b: \ \forall B : \ ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B)|Q')) \rightarrow \quad [42]$$
$$(\mathsf{SBit} = B \rightarrow \mathsf{RBit} = \mathsf{flip}(B))$$

$$b: \ ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_5)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_5)|Q')) \rightarrow \quad [43]$$
$$(\mathsf{SBit} = B_5 \rightarrow \mathsf{RBit} = \mathsf{flip}(B_5))$$

$$b: \ \neg((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_5)) \vee \quad [44]$$
$$(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_5)|Q'))$$

$b: \ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_5)) \quad [46]$

$b: \ \neg(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_5)|Q') \quad [47]$

$b: \ \neg(\mathsf{SIM} = \mathsf{msg}(D_5, B_5)) \quad [48]$

$\square \ \{D_5 \leftarrow d_3, \ B_5 \leftarrow b_3\}(28, 48)$

$b: \ \mathsf{SBit} = b_3 \rightarrow \mathsf{RBit} = \mathsf{flip}(b_3) \quad [45]$

$b: \ \neg(\mathsf{SBit} = b_3) \quad [49]$

$\square \ (29, 49)$

$b: \ \mathsf{RBit} = \mathsf{flip}(b_3) \quad [50]$

$\hookrightarrow$ S. 169

$\vdots$

von [50] (S. 168):

$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [23]

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_3)$ [30]

$b:\ \mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3)$ [40]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_3)$ [50]

aus RBit: $b:\ \forall B : \mathsf{RBit} = B \rightarrow \mathsf{A}(\mathsf{RBit} = B \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true})$ [51]

mit Tab. 0.11, $\{B \leftarrow \mathsf{flip}(b_3)\}$:

$a:\ \mathsf{AccDat} = \mathsf{true}$ [52]

mit Tab. 0.9:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_6, b_6)$ [54]

$b:\ \mathsf{RBit} = b_6$ [55]

$b:\ \mathsf{RNo} = n_7$ [56]

$a:\ \mathsf{RFile}(n_7) = d_6$ [57]

$a:\ \mathsf{RNo} = s(n_7)$ [58]

$a:\ \mathsf{RBit} = \mathsf{flip}(b_6)$ [59]

aus [40]:

$b:\ \mathsf{RIM} = \perp$ [60]

$\square$ (E3, 54, 60)

$b:\ \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3)$ [61]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_8^2, b_3)$ [62]

$\square:$

$b:\ \mathsf{RIM} = \mathsf{msg}(d_6, b_6)$ [54]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_3^2, b_3)$ [62]

$\rightarrow\ b_6 = b_3$

$b:\ \mathsf{RBit} = b_6$ [55]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_3)$ [50]

$\rightarrow\ b_6 = \mathsf{flip}(b_3)$

$a:\ \mathsf{RBit} = \mathsf{flip}(b_3)$ [53]

$\square:$

$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [23]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_3)$ [30]

$\rightarrow\ b_1 = b_3$

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$a:\ \mathsf{RBit} = \mathsf{flip}(b_3)$ [53]

$\rightarrow\ b_1 \neq b_3$

$\vdots$

von [29] (S. 167):

$a: \ (\exists D : \mathsf{RIM} = \mathsf{msg}(D, b_1)) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', b_1)|Q') \quad [21]$

$a: \ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [23]$

$a: \ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$

$b: \ \mathsf{SBit} = b_2 \quad [26]$

$a: \ \mathsf{SBit} = b_2 \quad [29]$

aus [21]:

$a: \ \exists D : \mathsf{RIM} = \mathsf{msg}(D, b_1) \quad [63]$

$a: \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [65]$

aus EA:

$b: \ \exists M : \mathsf{RIM} = M \quad [66]$

$b: \ \mathsf{RIM} = m_8 \quad [67]$

$a: \ \exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', b_1)|Q' \quad [64]$

$a: \ \mathsf{RQ} = q_1|\mathsf{msg}(d_1', b_1)|q_1' \quad [106]$

$\hookrightarrow$ S. 173

aus RIM: $b: \ \forall M : \mathsf{RIM} = M \rightarrow \mathsf{A}(\mathsf{RIM} = M \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}) \quad [68]$

mit Tab. 0.11, $\{M \leftarrow m_8\}$:

$a: \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true} \quad [69]$

$a: \ \mathsf{RecCom} = \mathsf{true} \quad [71]$

aus Tab. 0.1:

$b: \ \mathsf{RIM} = \perp \quad [73]$

$b: \ \mathsf{RQ} = \mathsf{msg}(d_9, b_9)|q_9 \quad [74]$

$a: \ \mathsf{RQ} = q_9 \quad [75]$

$a: \ \mathsf{RIM} = \mathsf{msg}(d_9, b_9) \quad [76]$

$\hookrightarrow$ S. 171

$a: \ \mathsf{AckMsg} = \mathsf{true} \quad [72]$

aus Tab. 0.8:

$a: \ \mathsf{RIM} = \perp \quad [91]$

$b: \ \mathsf{RIM} = \mathsf{msg}(d_{13}, b_{13}) \quad [92]$

$\Box \ (\mathrm{E3}, 65, 91)$

$a: \ \mathsf{RIM} = m_8 \quad [70]$

$\hookrightarrow$ S. 172

$\vdots$

von [76] (S. 170):

$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [23]

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$b:\ \mathsf{SBit} = b_2$ [26]

$a:\ \mathsf{SBit} = b_2$ [29]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [65]

$b:\ \mathsf{RIM} = \perp$ [73]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_9, b_9)$ [76]

aus Ind.Vor. [12]:

$b:\ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{10})) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_{10})|Q')) \rightarrow$ [77]
$(\mathsf{SBit} = \mathsf{flip}(B_{10}) \rightarrow \mathsf{RBit} = \mathsf{flip}(B_{10}))$

$b:\ \neg((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{10})) \vee$ [78]
$(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_{10})|Q'))$

$b:\ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{10}))$ [80]

$b:\ \neg(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_{10})|Q')$ [81]

$b:\ \neg(\mathsf{RQ} = Q_{10}|\mathsf{msg}(D'_{10}, B_{10})|Q'_{10})$ [82]

$\square\ \{Q_{10} \leftarrow \varepsilon,\ D'_{10} \leftarrow d_9,\ B_{10} \leftarrow b_9,\ Q'_{10} \leftarrow q_9\}(74, 82)$

$b:\ \mathsf{SBit} = \mathsf{flip}(b_9) \rightarrow \mathsf{RBit} = \mathsf{flip}(b_9)$ [79]

$b:\ \neg(\mathsf{SBit} = \mathsf{flip}(b_9))$ [83]

$\square:$
$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [65]
$a:\ \mathsf{RIM} = \mathsf{msg}(d_9, b_9)$ [76]
$\rightarrow\ b_1 = b_9$
$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [23]
$a:\ \mathsf{SBit} = b_2$ [29]
$\rightarrow\ b_2 = \mathsf{flip}(b_1)$
$b:\ \mathsf{SBit} = b_2$ [26]
$b:\ \neg(\mathsf{SBit} = \mathsf{flip}(b_9))$ [83]
$\rightarrow\ b_2 \neq \mathsf{flip}(b_9)$

$b:\ \mathsf{RBit} = \mathsf{flip}(b_9)$ [84]

aus RBit: $b:\ \forall B : \mathsf{RBit} = B \rightarrow$ [85]
$\mathsf{A}(\mathsf{RBit} = B \ \mathsf{unless}^+\ \mathsf{AccDat} = \mathsf{true})$
mit Tab. 0.11, $\{B \leftarrow \mathsf{flip}(b_9)\}$:

$a:\ \mathsf{AccDat} = \mathsf{true}$ [86]
mit Tab. 0.9:
$b:\ \mathsf{RIM} = \mathsf{msg}(d_{11}, b_{11})$ [88]
$b:\ \mathsf{RBit} = b_{11}$ [89]
$b:\ \mathsf{RNo} = n_{12}$ [90]
$\square$ (E3, 73, 88)

$a:\ \mathsf{RBit} = \mathsf{flip}(b_9)$ [87]

$\square:$
$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [65]
$a:\ \mathsf{RIM} = \mathsf{msg}(d_9, b_9)$ [76]
$\rightarrow\ b_1 = b_9$
$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]
$a:\ \mathsf{RBit} = \mathsf{flip}(b_9)$ [87]
$\rightarrow\ b_1 \neq b_9$

$\vdots$

von [70] (S. 170):

$a:$ $\mathsf{SBit} = \mathsf{flip}(b_1)$ [23]

$b:$ $\mathsf{SBit} = b_2$ [26]

$a:$ $\mathsf{SBit} = b_2$ [29]

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [65]

$b:$ $\mathsf{RIM} = m_8$ [67]

$a:$ $\mathsf{RIM} = m_8$ [70]

aus Ind.Vor. [12]:

$b:$ $((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{14})) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_{14})|Q')) \rightarrow$ [93]
$(\mathsf{SBit} = \mathsf{flip}(B_{14}) \rightarrow \mathsf{RBit} = \mathsf{flip}(B_{14}))$

$b:$ $\neg((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{14})) \vee$ [94]
$(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_{14})|Q'))$

$b:$ $\neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{14}))$ [96]

$b:$ $\neg(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_{14})|Q')$ [97]

$b:$ $\neg(\mathsf{RIM} = \mathsf{msg}(D_{14}, B_{14}))$ [98]

$\square$: $a:$ $\mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [65]
$a:$ $\mathsf{RIM} = m_8$ [70]
$b:$ $\mathsf{RIM} = m_8$ [67]
$\{D_{14} \leftarrow d_1, B_{14} \leftarrow b_1\}$

$b:$ $\mathsf{SBit} = \mathsf{flip}(b_1) \rightarrow \mathsf{RBit} = \mathsf{flip}(b_1)$ [95]

$b:$ $\mathsf{RBit} = \mathsf{flip}(b_1)$ [100]

aus RBit:

$b:$ $\forall B : \mathsf{RBit} = B \rightarrow$ [101]
$\mathsf{A}(\mathsf{RBit} = B \ \mathsf{unless}^{+} \ \mathsf{AccDat} = \mathsf{true})$

mit Tab. 0.11, $\{B \leftarrow \mathsf{flip}(b_1)\}$:

$b:$ $\neg(\mathsf{SBit} = \mathsf{flip}(b_1))$ [99]

$\square$: $a:$ $\mathsf{SBit} = \mathsf{flip}(b_1)$ [23]
$a:$ $\mathsf{SBit} = b_2$ [29]
$\rightarrow$ $b_2 = \mathsf{flip}(b_1)$
$b:$ $\mathsf{SBit} = b_2$ [26]
$b:$ $\neg(\mathsf{SBit} = \mathsf{flip}(b_1))$ [99]
$\rightarrow$ $b_2 \neq \mathsf{flip}(b_1)$

$a:$ $\mathsf{AccDat} = \mathsf{true}$ [102]

mit Tab. 0.9:

$b:$ $\mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15})$ [104]

$b:$ $\mathsf{RBit} = b_{15}$ [105]

$b:$ $\mathsf{RNo} = n_{16}$ [106]

$a:$ $\mathsf{RBit} = \mathsf{flip}(b_1)$ [103]

$\square$ (24, 103)

$\square$: $b:$ $\mathsf{RIM} = \mathsf{msg}(d_{15}, b_{15})$ [104]
$b:$ $\mathsf{RIM} = m_8$ [67]
$a:$ $\mathsf{RIM} = m_8$ [70]
$a:$ $\mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [65]
$\rightarrow$ $b_1 = b_{15}$
$b:$ $\mathsf{RBit} = b_{15}$ [105]
$b:$ $\mathsf{RBit} = \mathsf{flip}(b_1)$ [100]
$\rightarrow$ $b_{15} = \mathsf{flip}(b_1)$

$\vdots$

von [106] (S. 170):

$a:$ $\mathsf{SBit} = \mathsf{flip}(b_1)$ [23]

$a:$ $\neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$b:$ $\mathsf{SBit} = b_2$ [26]

$a:$ $\mathsf{SBit} = b_2$ [29]

$a:$ $\mathsf{RQ} = q_1|\mathsf{msg}(d'_1, b_1)|q'_1$ [106]

aus EA:

$b:$ $\exists Q : \mathsf{RQ} = Q$ [107]

$b:$ $\mathsf{RQ} = q_{17}$ [108]

aus RQ:

$b:$ $\forall Q : \mathsf{RQ} = Q \rightarrow$ [109]
$\mathsf{A}(\mathsf{RQ} = Q\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$

aus Tab. 0.11, $\{Q \leftarrow q_{17}\}$:

$a:$ $\mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee$ [110]
$\mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}$

$a:$ $\mathsf{RecCom} = \mathsf{true}$ [112]

aus Tab. 0.1:

$b:$ $\mathsf{RIM} = \perp$ [116]

$b:$ $\mathsf{RQ} = \mathsf{msg}(d_{18}, b_{18})|q_{18}$ [117]

$a:$ $\mathsf{RQ} = q_{18}$ [118]

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_{18}, b_{18})$ [119]

wie [111] mit
$a:$ $\mathsf{RQ} = q_1\|\mathsf{msg}(d'_1, b_1)\|q'_1$ [106]
$a:$ $\mathsf{RQ} = q_{18}$ [118]
$b:$ $\mathsf{RQ} = \mathsf{msg}(d_{18}, b_{18})\|q_{18}$ [117]
$b:$ $\mathsf{RQ} = \mathsf{msg}(d_{18}, b_{18})\|q_1\|\mathsf{msg}(d'_1, b_1)\|q'_1$

$a:$ $\mathsf{ReTrans} = \mathsf{true}$ [114] $\hookrightarrow$ S. 174

$a:$ $\mathsf{ProcAck} = \mathsf{true}$ [115] $\hookrightarrow$ S. 175

$a:$ $\mathsf{RLose} = \mathsf{true}$ [113]

aus Tab. 0.3:

$b:$ $\mathsf{RQ} \neq \varepsilon$ [120]

$a:$ $\neg(\mathsf{RQ} = Q_{19}|\mathsf{msg}(D_{19}, B_{19})|Q'_{19})$ [121]

$\square$ $\{Q_{19} \leftarrow q_1, D_{19} \leftarrow d'_1, B_{19} \leftarrow b_1, Q'_{19} \leftarrow q'_1\}(106, 121)$

$b:$ $\mathsf{SQ} = r_{19}|\mathsf{msg}(d'_1, b_1)|r'_{19}$ [122]

wie [111] mit
$b:$ $\mathsf{SQ} = r_{19}\|\mathsf{msg}(d'_1, b_1)\|r'_{19}$ [122]

$a:$ $\mathsf{RQ} = q_{17}$ [111]

relevant ist
$a:$ $\mathsf{RQ} = q_1\|\mathsf{msg}(d'_1, b_1)\|q'_1$ [106]
$a:$ $\mathsf{RQ} = q_{17}$ [111]
$b:$ $\mathsf{RQ} = q_{17}$ [108]
$b:$ $\mathsf{RQ} = q\|\mathsf{msg}(d'_1, b_1)\|\bar{q}$

$\hookrightarrow$ S. 176

$\vdots$

von [114] (S. 173):

$a: \ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [23]$

$a: \ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$

$b: \ \mathsf{SBit} = b_2 \quad [26]$

$a: \ \mathsf{SBit} = b_2 \quad [29]$

$a: \ \mathsf{RQ} = q_1|\mathsf{msg}(d_1', b_1)|q_1' \quad [106]$

$a: \ \mathsf{ReTrans} = \mathsf{true} \quad [114]$

aus Tab. 0.6:

$b: \ \mathsf{RQ} = q_{20} \quad [122]$

$b: \ \mathsf{SNo} = n_{20} \quad [123]$

$b: \ \mathsf{SBit} = b_{20} \quad [124]$

$a: \ \mathsf{RQ} = q_{20}|\mathsf{msg}(\mathsf{SFile}(n_{20}), b_{20}) \quad [125]$

aus Q2:

$a: \ \forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)|Q') \to Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B')) \quad [126]$

$a: \ (\exists D, B : Q_{21} = \mathsf{msg}(D, B)|Q_{21}') \to Q_{21}' = \varepsilon \vee (\exists D', B', Q'' : Q_{21}' = Q''|\mathsf{msg}(D', B')) \quad [127]$

$a: \ \neg(\exists D, B : Q_{21} = \mathsf{msg}(D, B)|Q_{21}') \quad [128]$

$a: \ \neg(Q_{21} = \mathsf{msg}(D_{21}, B_{21})|Q_{21}') \quad [130]$

$\Box \ \{Q_{21} \leftarrow \mathsf{msg}(d_1', b_1)|q_1', Q_{21}' \leftarrow q_1'\}$

$a: \ q_1' = \varepsilon \vee (\exists D', B', Q'' : q_1' = Q''|\mathsf{msg}(D', B')) \quad [129]$

$a: \ q_1' = \varepsilon \quad [131]$

$\Box: \ a: \ \mathsf{RQ} = q_1|\mathsf{msg}(d_1', b_1)|q_1' \quad [106]$

$a: \ q_1' = \varepsilon \quad [131]$

$a: \ \mathsf{RQ} = q_{20}|\mathsf{msg}(\mathsf{SFile}(n_{20}), b_{20}) \quad [125]$

$\to \ b_1 = b_{20}$

$b: \ \mathsf{SBit} = b_2 \quad [26]$

$b: \ \mathsf{SBit} = b_{20} \quad [124]$

$\to \ b_1 = b_2$

$a: \ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [23]$

$a: \ \mathsf{SBit} = b_2 \quad [29]$

$\to \ \mathsf{flip}(b_1) = b_2$

$a: \ \exists D', B', Q'' : q_1' = Q''|\mathsf{msg}(D', B') \quad [132]$

$a: \ q_1' = q_{21}''|\mathsf{msg}(d_{21}', b_{21}') \quad [133]$

wie [111], mit

$a: \ \mathsf{RQ} = q_1|\mathsf{msg}(d_1', b_1)|q_1' \quad [106]$

$a: \ q_1' = q_{21}''|\mathsf{msg}(d_{21}', b_{21}') \quad [133]$

$a: \mathsf{RQ} = q_1|\mathsf{msg}(d_1', b_1)|q_{21}''|\mathsf{msg}(d_{21}', b_{21}')$

$a: \ \mathsf{RQ} = q_{20}|\mathsf{msg}(\mathsf{SFile}(n_{20}), b_{20}) \quad [125]$

$b: \ \mathsf{RQ} = q_{20} \quad [122]$

$b: \ \mathsf{RQ} = q_1|\mathsf{msg}(d_1', b_1)|q_{21}''$

$\vdots$

von [115] (S. 173):

$a:$ $\mathsf{SBit} = \mathsf{flip}(b_1)$ [23]

$a:$ $\neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$b:$ $\mathsf{SBit} = b_2$ [26]

$a:$ $\mathsf{SBit} = b_2$ [29]

$a:$ $\mathsf{RQ} = q_1|\mathsf{msg}(d'_1, b_1)|q'_1$ [106]

$a:$ $\mathsf{ProcAck} = \mathsf{true}$ [115]

|

mit Tab. 0.7:

$b:$ $\mathsf{SIM} = \mathsf{msg}(d_{22}, b_{22})$ [134]

$b:$ $\mathsf{SBit} = b_{22}$ [135]

$b:$ $\mathsf{RQ} = q_{23}$ [136]

$b:$ $\mathsf{SNo} = n_{23}$ [137]

$a:$ $\mathsf{SFile}(s(n_{23})) = d_{24}$ [138]

$a:$ $\mathsf{RQ} = q_{23}|\mathsf{msg}(\mathsf{SFile}(s(n_{23})), \mathsf{flip}(b_{22}))$ [139]

$a:$ $\mathsf{SNo} = s(n_{23})$ [140]

$a:$ $\mathsf{SBit} = \mathsf{flip}(b_{22})$ [141]

$\Box:$ $a:$ $\mathsf{SBit} = b_2$ [29]

$a:$ $\mathsf{SBit} = \mathsf{flip}(b_{22})$ [141]

$\rightarrow$ $b_2 = \mathsf{flip}(b_{22})$

$b:$ $\mathsf{SBit} = b_2$ [26]

$b:$ $\mathsf{SBit} = b_{22}$ [135]

$\rightarrow$ $b_2 = b_{22}$

$a:$ $\mathsf{SFile}(s(n_{23})) = \perp$ [142]

$a:$ $\mathsf{RQ} = q_{23}$ [143]

$a:$ $\mathsf{SNo} = n_{23}$ [144]

$a:$ $\mathsf{SBit} = b_{22}$ [145]

$a:$ $\mathsf{ready} = \mathsf{true}$ [146]

wie [111], mit

$a:$ $\mathsf{RQ} = q_1|\mathsf{msg}(d'_1, b_1)|q'_1$ [106]

$a:$ $\mathsf{RQ} = q_{23}$ [143]

$b:$ $\mathsf{RQ} = q_{23}$ [136]

$b:$ $\mathsf{RQ} = q_1|\mathsf{msg}(d'_1, b_1)|q'_1$

$\vdots$

von [111] (S. 173):

$$a: \ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [23]$$
$$a: \ \neg(\mathsf{RBit} = \mathsf{flip}(b_1)) \quad [24]$$
$$b: \ \mathsf{SBit} = b_2 \quad [26]$$
$$a: \ \mathsf{SBit} = b_2 \quad [29]$$
$$a: \ \mathsf{RQ} = q_1|\mathsf{msg}(d_1', b_1)|q_1' \quad [106]$$
$$b: \ \mathsf{RQ} = q_{17} \quad [108]$$
$$a: \ \mathsf{RQ} = q_{17} \quad [111]$$

aus Ind.Vor. [12]:

$$b: \ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{25})) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_{25})|Q')) \rightarrow \quad [147]$$
$$(\mathsf{SBit} = \mathsf{flip}(B_{25}) \rightarrow \mathsf{RBit} = \mathsf{flip}(B_{25}))$$

$$b: \ \neg((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{25})) \vee \quad [148]$$
$$(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_{25})|Q'))$$

$$b: \ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{25})) \quad [150]$$
$$b: \ \neg(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_{25})|Q') \quad [151]$$
$$b: \ \neg(\mathsf{RQ} = Q_{25}|\mathsf{msg}(D_{25}', B_{25})|Q_{25}') \quad [152]$$

$$\boxed{\begin{array}{ll} \Box: & a: \ \mathsf{RQ} = q_1|\mathsf{msg}(d_1', b_1)|q_1' \quad [106] \\ & a: \ \mathsf{RQ} = q_{17} \quad [111] \\ & b: \ \mathsf{RQ} = q_{17} \quad [108] \\ & b: \ \neg(\mathsf{RQ} = Q_{25}|\mathsf{msg}(D_{25}', B_{25})|Q_{25}') \quad [152] \\ & \{Q_{25} \leftarrow q_1,\ D_{25}' \leftarrow d_1',\ B_{25} \leftarrow b_1,\ Q_{25}' \leftarrow q_1'\} \end{array}}$$

$$b: \ \mathsf{SBit} = \mathsf{flip}(b_1) \rightarrow \mathsf{RBit} = \mathsf{flip}(b_1) \quad [149]$$

$$b: \ \neg(\mathsf{SBit} = \mathsf{flip}(b_1)) \quad [153]$$

$$\boxed{\begin{array}{ll} \Box: & a: \ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [23] \\ & a: \ \mathsf{SBit} = b_2 \quad [29] \\ \hline & \rightarrow \ \mathsf{flip}(b_1) = b_2 \\ & b: \ \mathsf{SBit} = b_2 \quad [26] \\ & b: \ \neg(\mathsf{SBit} = \mathsf{flip}(b_1)) \quad [153] \\ \hline & \rightarrow \ b_2 \neq \mathsf{flip}(b_1) \end{array}}$$

$$b: \ \mathsf{RBit} = \mathsf{flip}(b_1) \quad [154]$$

$\hookrightarrow$ S. 177

$\vdots$

von [154] (S. 176):

$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [23]

$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(b_1))$ [24]

$b:\ \mathsf{SBit} = b_2$ [26]

$a:\ \mathsf{SBit} = b_2$ [29]

$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d'_1, b_1)|q'_1$ [106]

$b:\ \mathsf{RQ} = q_{17}$ [108]

$a:\ \mathsf{RQ} = q_{17}$ [111]

$b:\ \mathsf{RBit} = \mathsf{flip}(b_1)$ [154]

aus RBit: $b:\ \forall B : \mathsf{RBit} = B \rightarrow \mathsf{A}(\mathsf{RBit} = B \ \mathsf{unless}^+\ \mathsf{AccDat} = \mathsf{true})$ [155]

mit Tab. 0.11, $\{B \leftarrow \mathsf{flip}(b_1)\}$:

$a:\ \mathsf{AccDat} = \mathsf{true}$ [156]

mit Tab. 0.9:

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{26}, b_{26})$ [158]

$b:\ \mathsf{RBit} = b_{26}$ [159]

$a:\ \mathsf{RFile}(n_{27}) = d_{26}$ [160]

$a:\ \mathsf{RBit} = \mathsf{flip}(b_{26})$ [161]

Lemma1, A4:

$b:\ \forall B : (\exists D : \mathsf{RIM} = \mathsf{msg}(D, B)) \rightarrow (B = \mathsf{SBit} \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', B)|Q'))$ [162]

$b:\ (\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{28})) \rightarrow (B_{28} = \mathsf{SBit} \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', B_{28})|Q'))$ [163]

$b:\ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_{28}))$ [164]

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{28}, B_{28}))$ [165]

$\square\ \{D_{28} \leftarrow d_{26},\ B_{28} \leftarrow b_{26}\}(158, 165)$

[163] auflösen:

$b:\ \neg(b_{26} = \mathsf{SBit})$ [166]

$b:\ \mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_{26})|Q'$ [167]

$\hookrightarrow$ S. 178

$a:\ \mathsf{RBit} = \mathsf{flip}(b_1)$ [157]

$\square\ (24, 157)$

$\square$:

$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [23]
$a:\ \mathsf{SBit} = b_2$ [29]
$\rightarrow\ \mathsf{flip}(b_1) = b_2$

$b:\ \mathsf{RBit} = b_{26}$ [159]
$b:\ \mathsf{RBit} = \mathsf{flip}(b_1)$ [154]
$\rightarrow\ \mathsf{flip}(b_1) = b_{26}$

$b:\ \mathsf{SBit} = b_2$ [26]
$b:\ \neg(b_{26} = \mathsf{SBit})$ [168]
$\rightarrow\ b_2 \neq b_{26}$

$\vdots$

von [167] (S. 177):

$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [23]

$b:\ \mathsf{SBit} = b_2$ [26]

$a:\ \mathsf{SBit} = b_2$ [29]

$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1', b_1)|q_1'$ [106]

$b:\ \mathsf{RQ} = q_{17}$ [108]

$a:\ \mathsf{RQ} = q_{17}$ [111]

$b:\ \mathsf{RQ} = \varepsilon \vee \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_{26})|Q'$ [167]

$b:\ \mathsf{RQ} = \varepsilon$ [168]

$\Box:\ a:\ \mathsf{RQ} = q_1\vert\mathsf{msg}(d_1', b_1)\vert q_1'$ [106]
$a:\ \mathsf{RQ} = q_{17}$ [111]
$b:\ \mathsf{RQ} = q_{17}$ [108]
$b:\ \mathsf{RQ} = \varepsilon$ [168]

$b:\ \exists D', Q' : \mathsf{RQ} = \mathsf{msg}(D', b_{26})|Q'$ [169]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{26}', b_{26})|q_{26}'$ [170]

Lemma 1, A7 für RQ:

$b:\ \forall B : (\exists D, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q) \rightarrow$ [171]
$(B = \mathsf{SBit} \rightarrow (\forall Q', Q'', D', B' : \mathsf{RQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit}))$

$b:\ (\exists D, Q : \mathsf{RQ} = \mathsf{msg}(D, B_{29})|Q) \rightarrow$ [172]
$(B_{29} = \mathsf{SBit} \rightarrow (\forall Q', Q'', D', B' : \mathsf{RQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit}))$

$b:\ \neg(\exists D, Q : \mathsf{RQ} = \mathsf{msg}(D, B_{29})|Q)$ [173]

$b:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_{29}, B_{29})|Q_{29})$ [174]

$\Box\ \{D_{29} \leftarrow d_{26}',\ B_{29} \leftarrow b_{26},\ Q_{29} \leftarrow q_{29}'\}(170, 174)$

[172] auflösen:

$b:\ \neg(b_{26} = \mathsf{SBit})$ [175]

$\Box$ wie [166]

$b:\ \forall Q', Q'', D', B' : \mathsf{RQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit}$ [176]

$b:\ \mathsf{RQ} = Q_{29}'|\mathsf{msg}(D_{29}', B_{29}')|Q_{29}'' \rightarrow B_{29}' = \mathsf{SBit}$ [177]

$b:\ \neg(\mathsf{RQ} = Q_{29}'|\mathsf{msg}(D_{29}', B_{29}')|Q_{29}'')$ [178]

$\Box:\ a:\ \mathsf{RQ} = q_1\vert\mathsf{msg}(d_1', b_1)\vert q_1'$ [106]
$a:\ \mathsf{RQ} = q_{17}$ [111]
$b:\ \mathsf{RQ} = q_{17}$ [108]
$b:\ \neg(\mathsf{RQ} = Q_{29}'\vert\mathsf{msg}(D_{29}', B_{29}')\vert Q_{29}'')$ [178]
$\Box\ \{Q_{29}' \leftarrow q_1,\ D_{29}' \leftarrow d_1',\ B_{29}' \leftarrow b_1,\ Q_{29}'' \leftarrow q_1'\}$

$b:\ b_1 = \mathsf{SBit}$ [179]

$\Box:\ a:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [23]
$a:\ \mathsf{SBit} = b_2$ [29]
$\rightarrow\ \mathsf{flip}(b_1) = b_2$
$b:\ \mathsf{SBit} = b_2$ [26]
$b:\ b_1 = \mathsf{SBit}$ [179]
$\rightarrow\ b_2 = b_1$

8 Lemma 4: Synchronisierung durch die beiden Kontrollbits

$$\mathsf{A}\Box((\mathsf{SBit} = \mathsf{RBit} \to \mathsf{RNo} = \mathsf{SNo}) \wedge (\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \to \mathsf{RNo} = s(\mathsf{SNo})))$$

Sind die Kontrollbits von Sender und Empfänger gleich, arbeiten beide an dem gleichen Index, ansonsten ist der Empfänger schon bereit, den nächsten Index zu bearbeiten.

Beweis:

Der Beweis basiert auf dem Schema zur Durchführung eines Induktionsbeweises. Der Induktionsanfang ist trivial.

Situation in a:
Es ist $\mathsf{SBit}_a = \mathsf{RBit}_a$ und $\mathsf{RNo}_a \neq \mathsf{SNo}_a$ oder es ist $\mathsf{SBit}_a = \mathsf{flip}(\mathsf{RBit}_a)$ und $\mathsf{RNo}_a \neq s(\mathsf{SNo}_a)$.
In b ist – disjunkte Fallunterscheidung – $\mathsf{SBit}_b = \mathsf{RBit}_b$ und $\mathsf{RNo}_b = \mathsf{SNo}_b$ oder $\mathsf{SBit}_b = \mathsf{flip}(\mathsf{RBit}_b)$ und $\mathsf{RNo}_b = s(\mathsf{SNo}_b)$.

Der Beweis wird über eine Fallunterscheidung dieser beiden Alternativen geführt:

Ist in b nicht $\mathsf{SBit}_b = \mathsf{RBit}_b$, so muß $\mathsf{SBit}_b = \mathsf{flip}(\mathsf{RBit}_b)$ und $\mathsf{RNo}_b = s(\mathsf{SNo}_b)$ sein. Man stellt zuerst fest, daß dann in dem betrachteten Schritt AccDat nicht angewendet worden sein kann – also RBit unverändert bleibt: Sonst wäre $\mathsf{Bit}(\mathsf{RIM}_b) = \mathsf{RBit}_b = \mathsf{flip}(\mathsf{SBit}_b)$ und mit Lemma 3 müßte dann $\mathsf{SBit}_b = \mathsf{flip}(\mathsf{RBit}_b)$ sein. Somit ist also – ebenfalls da AccDat nicht angewendet wurde – $\mathsf{RNo}_a = \mathsf{RNo}_b$.

Hat $\mathsf{ProcAck}$ in dem betrachteten Schritt SBit nicht verändert, so ist $\mathsf{SBit}_a = \mathsf{SBit}_b = \mathsf{flip}(\mathsf{RBit}_b) = \mathsf{flip}(\mathsf{RBit}_a)$ und $\mathsf{RNo}_a = \mathsf{RNo}_b = s(\mathsf{SNo}_b) = s(\mathsf{SNo}_a)$ im Widerspruch zur Annahme. Anderenfalls ist $\mathsf{SBit}_a = \mathsf{flip}(\mathsf{SBit}_b) = \mathsf{flip}(\mathsf{flip}(\mathsf{RBit}_b)) = \mathsf{RBit}_a$ und $\mathsf{SNo}_a = s(\mathsf{SNo}_b) = \mathsf{RNo}_b = \mathsf{RNo}_a$ ebenfalls ein Widerspruch zur Annahme.

Bleibt der Fall zu betrachten, daß $\mathsf{SBit}_b = \mathsf{RBit}_b$ und $\mathsf{RNo}_b = \mathsf{SNo}_b$ ist. Diesmal kann man eine Anwendung von $\mathsf{ProcAck}$ im betreffenden Schritt ausschließen: Dazu müßte $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ und nach Lemma 2 $\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})$ sein. Somit ist $\mathsf{SBit}_a = \mathsf{RBit}_a$ und $\mathsf{SNo}_a = \mathsf{SNo}_b$.

Ist AccDat in dem betrachteten Schritt nicht angewendet worden, ist $\mathsf{SBit}_a = \mathsf{SBit}_b = \mathsf{RBit}_b = \mathsf{RBit}_a$ und $\mathsf{SNo}_a = \mathsf{SNo}_b = \mathsf{RNo}_b = \mathsf{RNo}_a$ im Widerspruch zur Annahme. Anderenfalls ist $\mathsf{RBit}_a = \mathsf{flip}(\mathsf{RBit}_b) = \mathsf{flip}(\mathsf{SBit}_b) = \mathsf{flip}(\mathsf{SBit}_a)$ und $\mathsf{RNo}_a = s(\mathsf{RNo}_b) = s(\mathsf{SNo}_b) = s(\mathsf{SNo}_a)$ ebenfalls ein Widerspruch zur Annahme.

$\vdots$

$p : [\,0, \{\neg(\neg A)\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$a :\ \neg A$ [9]

$b :\ \neg(\neg A)$ [12]

$a :\ \neg((\mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}) \wedge (\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo})))$ [9]

$b :\ (\mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}) \wedge (\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo}))$ [12]

$b :$ Lemma 1 [13]

$b :$ Lemma 2 [14]

$b :$ Lemma 3 [15]

$b :\ \mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}$ [20]

$b :\ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo})$ [21]

aus EA:

$b :\ \exists B : \mathsf{RBit} = B$ [22]

$b :\ \mathsf{RBit} = b_1$ [23]

aus [20]:

$b :\ \neg(\mathsf{SBit} = \mathsf{RBit})$ [24] | $b :\ \mathsf{RNo} = \mathsf{SNo}$ [25]

$\hookrightarrow$ S. 186

aus BR:

$b :\ \forall B : \mathsf{RBit} = B \rightarrow (\mathsf{SBit} = B \vee \mathsf{SBit} = \mathsf{flip}(B))$ [26]

$b :\ \mathsf{RBit} = B_2 \rightarrow (\mathsf{SBit} = B_2 \vee \mathsf{SBit} = \mathsf{flip}(B_2))$ [27]

$b :\ \neg(\mathsf{RBit} = B_2)$ [28] | $b :\ \mathsf{SBit} = b_1 \vee \mathsf{SBit} = \mathsf{flip}(b_1)$ [29]

$\Box\ \{B_2 \leftarrow b_1\}(23, 28)$

$b :\ \mathsf{SBit} = b_1$ [30] | $b :\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [31]

$\Box :\ b :\ \neg(\mathsf{SBit} = \mathsf{RBit})$ [24]
$b :\ \mathsf{RBit} = b_1$ [23]
$b :\ \mathsf{SBit} = b_1$ [30]

aus [21]:

$b :\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}))$ [32] | $b :\ \mathsf{RNo} = s(\mathsf{SNo})$ [33]

$\hookrightarrow$ S. 182

$\Box :\ b :\ \mathsf{RBit} = b_1$ [23]
$b :\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [31]
$b :\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}))$ [32]

$\vdots$

von [33] (S. 181):

$b:\ \mathsf{RBit} = b_1$ [23]

$b:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [31]

$b:\ \mathsf{RNo} = s(\mathsf{SNo})$ [33]

$|$

aus RBit: $b:\ \forall B : \mathsf{RBit} = B \rightarrow \mathsf{A}(\mathsf{RBit} = B \ \mathsf{unless}^+\ \mathsf{AccDat} = \mathsf{true})$ [34]

mit Tab. 0.11, $\{B \leftarrow b_1)\}$:

$a:\ \mathsf{AccDat} = \mathsf{true}$ [35] | $a:\ \mathsf{RBit} = b_1$ [36]

mit Tab. 0.9: | $a:\ \neg(\mathsf{AccDat} = \mathsf{true})$ [37]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_3, b_3)$ [38] | $\hookrightarrow$ S. 183

$b:\ \mathsf{RBit} = b_3$ [39]

$b:\ \mathsf{RNo} = n_4$ [40]

$|$

$b:\ \forall B:\ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B)|Q')) \rightarrow$ [41]
$(\mathsf{SBit} = \mathsf{flip}(B) \rightarrow \mathsf{RBit} = \mathsf{flip}(B))$

$|$

$b:\ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_5)) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_5)|Q')) \rightarrow$ [42]
$(\mathsf{SBit} = \mathsf{flip}(B_5) \rightarrow \mathsf{RBit} = \mathsf{flip}(B_5))$

$b:\ \neg((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_5)) \vee$ [43]
$(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_5)|Q'))$

$|$

$b:\ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_5))$ [45]

$b:\ \neg(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_5)|Q')$ [46]

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_5, B_5))$ [46]

$\square\ \{D_5 \leftarrow d_3,\ B_5 \leftarrow b_3\}(38, 46)$

$b:\ \mathsf{SBit} = \mathsf{flip}(b_3) \rightarrow \mathsf{RBit} = \mathsf{flip}(b_3)$ [44]

$b:\ \neg(\mathsf{SBit} = \mathsf{flip}(b_3))$ [45] | $b:\ \mathsf{RBit} = \mathsf{flip}(b_3)$ [46]

$\square:$ $b:\ \mathsf{RBit} = b_1$ [23]
$b:\ \mathsf{RBit} = b_3$ [39]
$\rightarrow\ b_1 = b_3$
$b:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [31]
$b:\ \neg(\mathsf{SBit} = \mathsf{flip}(b_3))$ [45]
$\rightarrow\ b_1 \neq b_3$

$\square:$ $b:\ \mathsf{RBit} = \mathsf{flip}(b_3)$ [46]
$b:\ \mathsf{RBit} = b_3$ [39]

$\vdots$

von [37] (S. 182):

$b:\ \mathsf{RBit} = b_1$ [23]

$b:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [31]

$b:\ \mathsf{RNo} = s(\mathsf{SNo})$ [33]

$a:\ \mathsf{RBit} = b_1$ [36]

$a:\ \neg(\mathsf{AccDat} = \mathsf{true})$ [37]

aus EA:

$b:\ \exists N : \mathsf{RNo} = N$ [47]

$b:\ \mathsf{RNo} = n_6$ [48]

aus RNo: $b:\ \forall N : \mathsf{RNo} = N \rightarrow \mathsf{A}(\mathsf{RNo} = N\ \mathsf{unless}^+\ \mathsf{AccDat} = \mathsf{true})$ [49]

mit Tab. 0.11, $\{N \leftarrow n_6\}$:

$a:\ \mathsf{AccDat} = \mathsf{true}$ [50]

$\square$ $(37, 50)$

$a:\ \mathsf{RNo} = n_6$ [51]

aus SBit:

$b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [52]

mit Tab. 0.11, $\{B \leftarrow \mathsf{flip}(b_1)\}$:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [53]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_7, b_7)$ [56]

$b:\ \mathsf{SBit} = b_7$ [57]

$b:\ \mathsf{RQ} = q_8$ [58]

$b:\ \mathsf{SNo} = n_8$ [59]

$a:\ \mathsf{SFile}(s(n_8)) = d_9$ [60]

$a:\ \mathsf{RQ} = q_8|\mathsf{msg}(\mathsf{SFile}(s(n_8)), \mathsf{flip}(b_7))$ [61]

$a:\ \mathsf{SNo} = s(n_8)$ [62]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_7)$ [63]

$\hookrightarrow$ S. 184

$a:\ \mathsf{SFile}(s(n_8)) = \bot$ [64]

$a:\ \mathsf{RQ} = q_8$ [65]

$a:\ \mathsf{SNo} = n_8$ [66]

$a:\ \mathsf{SBit} = b_7$ [67]

$a:\ \mathsf{ready} = \mathsf{true}$ [68]

wie [54], da SBit und SNo unverändert

$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [54]

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true}$ [55]

$\hookrightarrow$ S. 185

$\vdots$

von [63] (S. 183):

$b:\ \mathsf{RBit} = b_1 \quad [23]$

$b:\ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [31]$

$b:\ \mathsf{RNo} = s(\mathsf{SNo}) \quad [33]$

$a:\ \mathsf{RBit} = b_1 \quad [36]$

$b:\ \mathsf{RNo} = n_6 \quad [48]$

$a:\ \mathsf{RNo} = n_6 \quad [51]$

$b:\ \mathsf{SBit} = b_7 \quad [57]$

$b:\ \mathsf{SNo} = n_8 \quad [59]$

$a:\ \mathsf{SNo} = s(n_8) \quad [62]$

$a:\ \mathsf{SBit} = \mathsf{flip}(b_7) \quad [63]$

aus [9]:

$a:\ \neg(\mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}) \quad [69]$

$a:\ \mathsf{SBit} = \mathsf{RBit} \quad [71]$

$a:\ \neg(\mathsf{RNo} = \mathsf{SNo}) \quad [72]$

$$
\boxed{\begin{array}{ll}
\Box: & b:\ \mathsf{SNo} = n_8 \quad [59] \\
 & b:\ \mathsf{RNo} = s(\mathsf{SNo}) \quad [33] \\
 & b:\ \mathsf{RNo} = n_6 \quad [48] \\ \hline
 & \rightarrow\ n_6 = s(n_8) \\
 & a:\ \mathsf{RNo} = n_6 \quad [51] \\
 & a:\ \mathsf{SNo} = s(n_8) \quad [62] \\
 & a:\ \neg(\mathsf{RNo} = \mathsf{SNo}) \quad [72] \\ \hline
 & \rightarrow\ n_6 \neq s(n_8)
\end{array}}
$$

$a:\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo})) \quad [70]$

$a:\ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \quad [73]$

$a:\ \neg(\mathsf{RNo} = s(\mathsf{SNo})) \quad [74]$

$$
\boxed{\begin{array}{ll}
\Box: & b:\ \mathsf{RBit} = b_1 \quad [23] \\
 & b:\ \mathsf{SBit} = \mathsf{flip}(b_1) \quad [31] \\
 & b:\ \mathsf{SBit} = b_7 \quad [57] \\ \hline
 & \rightarrow\ b_1 = \mathsf{flip}(b_7) \\
 & a:\ \mathsf{RBit} = b_1 \quad [36] \\
 & a:\ \mathsf{SBit} = \mathsf{flip}(b_7) \quad [63] \\
 & a:\ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \quad [73] \\ \hline
 & \rightarrow\ \mathsf{flip}(b_7) = \mathsf{flip}(b_1)
\end{array}}
$$

$\vdots$

von [55] (S. 183):

$b:\ \mathsf{RNo} = s(\mathsf{SNo})\quad [33]$

$a:\ \mathsf{RBit} = b_1\quad [36]$

$b:\ \mathsf{RNo} = n_6\quad [48]$

$a:\ \mathsf{RNo} = n_6\quad [51]$

$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)\quad [54]$

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true}\quad [55]$

aus EA:

$b:\ \exists N : \mathsf{SNo} = N\quad [75]$

$b:\ \mathsf{SNo} = n_{10}\quad [76]$

aus SNo: $b:\ \forall N : \mathsf{SNo} = N \to \mathsf{A}(\mathsf{SNo} = N \text{ unless}^+ \mathsf{ProcAck} = \mathsf{true})\quad [77]$

mit Tab. 0.11, $\{N \leftarrow n_{10}\}$:

$a:\ \mathsf{ProcAck} = \mathsf{true}\quad [78]$

$\square\ (55, 78)$

$a:\ \mathsf{SNo} = n_{10}\quad [79]$

aus [9]:

$a:\ \neg(\mathsf{SBit} = \mathsf{RBit} \to \mathsf{RNo} = \mathsf{SNo})\quad [80]$

$a:\ \mathsf{SBit} = \mathsf{RBit}\quad [82]$

$a:\ \neg(\mathsf{RNo} = \mathsf{SNo})\quad [83]$

$\square:\ a:\ \mathsf{SBit} = \mathsf{RBit}\quad [82]$

$a:\ \mathsf{RBit} = b_1\quad [36]$

$a:\ \mathsf{SBit} = \mathsf{flip}(b_1)\quad [54]$

$a:\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \to \mathsf{RNo} = s(\mathsf{SNo}))\quad [81]$

$a:\ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit})\quad [84]$

$a:\ \neg(\mathsf{RNo} = s(\mathsf{SNo}))\quad [85]$

$\square:\ b:\ \mathsf{RNo} = s(\mathsf{SNo})\quad [33]$

$b:\ \mathsf{RNo} = n_6\quad [48]$

$b:\ \mathsf{SNo} = n_{10}\quad [76]$

$\to\ n_6 = n_{10}$

$a:\ \neg(\mathsf{RNo} = s(\mathsf{SNo}))\quad [85]$

$a:\ \mathsf{RNo} = n_6\quad [51]$

$a:\ \mathsf{SNo} = n_{10}\quad [79]$

$\to\ n_6 \neq n_{10}$

$\vdots$

von [25] (S. 181):

$b:\ \mathsf{RBit} = b_1$ [23]

$b:\ \mathsf{RNo} = \mathsf{SNo}$ [25]

aus [12]:

$b:\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}))$ [86]

$b:\ \mathsf{RNo} = s(\mathsf{SNo})$ [87]

$\square$ (NZ, 25, 87)

aus BR:

$b:\ \forall B : \mathsf{RBit} = B \rightarrow (\mathsf{SBit} = B \vee \mathsf{SBit} = \mathsf{flip}(B))$ [88]

$b:\ \mathsf{RBit} = B_{11} \rightarrow (\mathsf{SBit} = B_{11} \vee \mathsf{SBit} = \mathsf{flip}(B_{11}))$ [89]

$b:\ \neg(\mathsf{RBit} = B_{11})$ [90]

$\square\ \{B_{11} \leftarrow b_1\}(23, 90)$

$b:\ \mathsf{SBit} = b_1 \vee \mathsf{SBit} = \mathsf{flip}(b_1)$ [91]

$b:\ \mathsf{SBit} = b_1$ [92]

$b:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [93]

$\square:$ $b:\ \mathsf{SBit} = \mathsf{flip}(b_1)$ [93]
$b:\ \mathsf{RBit} = b_1$ [23]
$b:\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}))$ [86]

aus SBit:

$b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})$ [94]

mit Tab. 0.11, $\{B \leftarrow b_1\}$:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [95]

mit Tab. 0.7:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{12}, b_{12})$ [98]

$b:\ \mathsf{SBit} = b_{12}$ [99]

$\hookrightarrow$ S. 187

$a:\ \mathsf{SBit} = b_1$ [96]

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [97]

aus EA:

$b:\ \exists N : \mathsf{SNo} = N$ [109]

$b:\ \mathsf{SNo} = n_{14}$ [110]

aus SNo:

$b:\ \forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}(\mathsf{SNo} = N \ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})$ [111]

mit Tab. 0.11, $\{N \leftarrow n_{14}\}$:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [112]

$\square$ (97, 112)

$a:\ \mathsf{SNo} = n_{14}$ [113]

$\hookrightarrow$ S. 188

$\vdots$

von [99] (S. 186):

$b:\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}))$ [86]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_{12}, b_{12})$ [98]

$b:\ \mathsf{SBit} = b_{12}$ [99]

mit Lemma 2:

$b:\ \forall B:\ ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B)|Q')) \rightarrow$ [100]
$(\mathsf{SBit} = B \rightarrow \mathsf{RBit} = \mathsf{flip}(B))$

$b:\ ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{13})) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{13})|Q')) \rightarrow$ [101]
$(\mathsf{SBit} = B_{13} \rightarrow \mathsf{RBit} = \mathsf{flip}(B_{13}))$

$b:\ \neg((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{13})) \vee$ [102]
$(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{13})|Q'))$

$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_{13}))$ [104]

$b:\ \neg(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_{13})|Q')$ [105]

$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_{13}, B_{13}))$ [106]

$\square\ \{D_{13} \leftarrow d_{12},\ B_{13} \leftarrow b_{12}\}(98, 106)$

$b:\ \mathsf{SBit} = b_{12} \rightarrow \mathsf{RBit} = \mathsf{flip}(b_{12})$ [103]

$b:\ \neg(\mathsf{SBit} = b_{12})$ [107]

$\square\ (99, 107)$

$b:\ \mathsf{RBit} = \mathsf{flip}(b_{12})$ [108]

$\square$:	$b:\ \mathsf{RBit} = \mathsf{flip}(b_{12})$	[108]
	$b:\ \mathsf{SBit} = b_{12}$	[99]
	$b:\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}))$	[86]

$\vdots$

von [113] (S. 186):

$b:$ RBit $= b_1$ [23]

$b:$ RNo $=$ SNo [25]

$a:$ SBit $= b_1$ [96]

$b:$ SNo $= n_{14}$ [110]

$a:$ SNo $= n_{14}$ [113]

aus RBit: $b: \forall B:$ RBit $= B \rightarrow$ A(RBit $= B$ unless$^+$ AccDat $=$ true) [114]

mit Tab. 0.11, $\{B \leftarrow b_1\}$:

$a:$ AccDat $=$ true [115]

mit Tab. 0.9:

$b:$ RIM $=$ msg(d_{15}, b_{15}) [118]

$b:$ RBit $= b_{15}$ [119]

$b:$ RNo $= n_{16}$ [120]

$a:$ RFile$(n_{16}) = d_{15}$ [121]

$a:$ RNo $= s(n_{16})$ [122]

$a:$ RBit $=$ flip(b_{15}) [123]

$a:$ RBit $= b_1$ [116]

$a: \neg$(AccDat $=$ true) [117]

$\hookrightarrow$ S. 189

aus [9]:

$a: \neg$(SBit $=$ RBit $\rightarrow$ RNo $=$ SNo) [124]

$a:$ SBit $=$ RBit [126]

$a: \neg$(RNo $=$ SNo) [127]

$\square:$ $b:$ RBit $= b_1$ [23]
$b:$ RBit $= b_{15}$ [119]
$\rightarrow b_1 = b_{15}$
$a:$ SBit $= b_1$ [96]
$a:$ RBit $=$ flip(b_{15}) [123]
$a:$ SBit $=$ RBit [126]
$\rightarrow b_1 =$ flip(b_{15})

$a: \neg$(SBit $=$ flip(RBit) $\rightarrow$ RNo $= s$(SNo)) [125]

$a:$ SBit $=$ flip(RBit) [128]

$a: \neg$(RNo $= s$(SNo)) [129]

$\square:$ $b:$ SNo $= n_{14}$ [110]
$b:$ RNo $= n_{16}$ [120]
$b:$ RNo $=$ SNo [25]
$\rightarrow n_{14} = n_{16}$
$a:$ SNo $= n_{14}$ [113]
$a:$ RNo $= s(n_{16})$ [122]
$a: \neg$(RNo $= s$(SNo)) [129]
$\rightarrow s(n_{16}) \neq s(n_{14})$

$\vdots$

von [117] (S. 188):

$b:$ RNo = SNo [25]

$a:$ SBit = b_1 [96]

$b:$ SNo = n_{14} [110]

$a:$ SNo = n_{14} [113]

$a:$ RBit = b_1 [116]

$a:$ ¬(AccDat = true) [117]

|

aus EA:

$b:$ $\exists N$: RNo = N [130]

$b:$ RNo = n_{17} [131]

|

aus RNo: $b:$ $\forall N$: RNo = $N \rightarrow$ A(RNo = N unless$^+$ AccDat = true) [132]

mit Tab. 0.11, $\{N \leftarrow n_{17}\}$:

$a:$ AccDat = true [133]
$\square$ (117, 133)

$a:$ RNo = n_{17} [134]

|

aus [9]:

$a:$ ¬(SBit = RBit → RNo = SNo) [135]

$a:$ SBit = RBit [137]

$a:$ ¬(RNo = SNo) [138]

$$
\boxed{\begin{array}{ll}
\square : & b: \mathsf{SNo} = n_{14} \quad [110] \\
 & b: \mathsf{RNo} = n_{17} \quad [131] \\
 & b: \mathsf{RNo} = \mathsf{SNo} \quad [25] \\ \hline
 & \rightarrow n_{14} = n_{17} \\
 & a: \mathsf{SNo} = n_{14} \quad [113] \\
 & a: \mathsf{RNo} = n_{17} \quad [134] \\
 & a: \neg(\mathsf{RNo} = \mathsf{SNo}) \quad [138] \\ \hline
 & \rightarrow n_{14} \neq n_{17}
\end{array}}
$$

$a:$ ¬(SBit = flip(RBit) → RNo = s(SNo)) [136]

$a:$ SBit = flip(RBit) [139]

$a:$ ¬(RNo = s(SNo)) [140]

$$
\boxed{\begin{array}{ll}
\square : & a: \mathsf{SBit} = b_1 \quad [96] \\
 & a: \mathsf{RBit} = b_1 \quad [116] \\
 & a: \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \quad [139]
\end{array}}
$$

9 Lemma 5: Zusammenhang von SBit, SNo und Laufnummern

$$\mathsf{A}\Box(\forall D, B : (\mathsf{RIM} = \mathsf{msg}(D,B) \lor \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q') \rightarrow$$
$$((B = \mathsf{SBit} \rightarrow D = \mathsf{SFile}(\mathsf{SNo})) \land (B = \mathsf{flip}(\mathsf{SBit}) \rightarrow D = \mathsf{SFile}(p(\mathsf{SNo})))))$$

Nachrichten mit Kontrollbit SBit enthalten die aktuell zu übertragende Information, die anderen sind „alt“.

Beweis:

Der Beweis basiert auf dem Schema zur Durchführung eines Induktionsbeweises. Der Induktionsanfang ist trivial.

Situation in a:
RIM_a oder RQ_a enthalten eine Nachricht m, deren Kontrollbit SBit_a ist und deren Inhalt, $\mathsf{Data}(m)$ nicht $\mathsf{SFile}(\mathsf{SNo}_a)$ ist, oder deren Kontrollbit $\mathsf{flip}(\mathsf{SBit}_a)$ ist und $\mathsf{Data}(m)$ nicht $\mathsf{SFile}(p(\mathsf{SNo}_a))$ ist.

Man unterscheidet, ob in dem betreffenden Schritt SBit verändert wurde. SNo wird genau dann verändert, wenn auch SBit verändert wird.

Wurden SBit und SNo verändert, dies kann nur durch ProcAck geschehen sein, so ist $\mathsf{Bit}(\mathsf{SIM}_b) = \mathsf{SBit}_b$ und damit nach Lemma 1 für alle Nachrichten m' in RIM_b und RQ_b ebenfalls $\mathsf{Bit}(m') = \mathsf{SBit}_b = \mathsf{flip}(\mathsf{SBit}_a)$.

Als weiteres wird unterschieden, ob die ausschlaggebende Nachricht in RIM_a oder in RQ_a enthalten ist: Ist sie in RIM_a enthalten, so war sie entweder in RIM_b oder in RQ_b schon enthalten, womit nach Induktionsvoraussetzung $\mathsf{Data}(m) = \mathsf{SFile}_b(\mathsf{SNo}_b) = \mathsf{SFile}_b(p(\mathsf{SNo}_a))$ ist. Da sich SFile wird nie verändert, ist also $\mathsf{Data}(m) = \mathsf{SFile}_a(p(\mathsf{SNo}_a))$.

Ist die betreffende Nachricht in RQ_a enthalten, so war sie entweder schon in RQ_b enthalten, womit sich derselbe Beweis wie eben ergibt, oder sie ist die durch ProcAck angehängte Nachricht, dann ist $\mathsf{Bit}(m) = \mathsf{flip}(\mathsf{SBit}_b) = \mathsf{SBit}_a$ und $\mathsf{Data}(m) = \mathsf{SFile}(s(\mathsf{SNo}_b)) = \mathsf{SFile}(\mathsf{SNo}_a)$.

Bleiben SBit und SNo unverändert, trifft man dieselbe Fallunterscheidung: Ist die ausschlaggebende Nachricht in RIM_a enthalten, so war sie entweder in RIM_b oder in RQ_b schon enthalten, womit nach Induktionsvoraussetzung daß $\mathsf{Data}(m) = \mathsf{SFile}(X)$ für das entsprechende $X \in \{\mathsf{SNo}, p(\mathsf{SNo})\}$ ist. Da sich SFile wird nie verändert, übertragen sich diese Beziehungen unverändert nach a.

Ist die betreffende Nachricht in RQ_a enthalten, so war sie entweder schon in RQ_b enthalten, womit sich derselbe Beweis wie eben ergibt, oder sie ist durch ProcAck oder ReTrans angehängt worden. In diesem Fall kann ProcAck ausgeschlossen werden, da dabei nur eine Nachricht angehängt wird, wenn auch SBit verändert wird, im Falle von ReTrans ist $\mathsf{Bit}(m) = \mathsf{SBit}_b = \mathsf{SBit}_a$ und $\mathsf{Data}(m) = \mathsf{SFile}(\mathsf{SNo}_b) = \mathsf{SFile}(\mathsf{SNo}_a)$, beides im Widerspruch zur Annahme.

$$\vdots$$

$$p : [\,0, \{\neg(\neg A)\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$

$$a:\ \neg A \quad [9]$$

$$b:\ \neg(\neg A) \quad [12]$$

$$a:\ \neg(\forall D, B : (\mathsf{RIM} = \mathsf{msg}(D,B) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q') \rightarrow \quad [9]$$
$$((B = \mathsf{SBit} \rightarrow D = \mathsf{SFile}(\mathsf{SNo})) \wedge (B = \mathsf{flip}(\mathsf{SBit}) \rightarrow D = \mathsf{SFile}(p(\mathsf{SNo})))))$$

$$b:\ \forall D, B : (\mathsf{RIM} = \mathsf{msg}(D,B) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q') \rightarrow \quad [12]$$
$$((B = \mathsf{SBit} \rightarrow D = \mathsf{SFile}(\mathsf{SNo})) \wedge (B = \mathsf{flip}(\mathsf{SBit}) \rightarrow D = \mathsf{SFile}(p(\mathsf{SNo}))))$$

$$b:\ \text{Lemma 1} \quad [13]$$

aus [9]:

$$a:\ \neg((\mathsf{RIM} = \mathsf{msg}(d_1,b_1) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(d_1,b_1)|Q') \rightarrow \quad [20]$$
$$((b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo})))))$$

$$a:\ \mathsf{RIM} = \mathsf{msg}(d_1,b_1) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(d_1,b_1)|Q' \quad [21]$$
$$a:\ \neg((b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo})))) \quad [22]$$

aus EA:

$$b:\ \exists B : \mathsf{SBit} = B \quad [23]$$
$$b:\ \mathsf{SBit} = b_2 \quad [24]$$

aus SBit: $b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B \ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true}) \quad [25]$

mit Tab. 0.11, $\{B \leftarrow b_2\}$:

Linker Zweig:

$$a:\ \mathsf{ProcAck} = \mathsf{true} \quad [26]$$

mit Tab. 0.7:

$$b:\ \mathsf{SIM} = \mathsf{msg}(d_3,b_3) \quad [29]$$
$$b:\ \mathsf{SBit} = b_3 \quad [30]$$
$$b:\ \mathsf{RQ} = q_4 \quad [31]$$
$$b:\ \mathsf{SNo} = n_4 \quad [32]$$

Linker Unterzweig:

$$a:\ \mathsf{SFile}(s(n_4)) = d_5 \quad [33]$$
$$a:\ \mathsf{RQ} = q_4|\mathsf{msg}(\mathsf{SFile}(s(n_4)), \mathsf{flip}(b_3)) \quad [34]$$
$$a:\ \mathsf{SNo} = s(n_4) \quad [35]$$
$$a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [36]$$

↪ S. 192

Rechter Unterzweig:

$$a:\ \mathsf{SFile}(s(n_4)) = \perp \quad [37]$$
$$a:\ \mathsf{RQ} = q_4 \quad [38]$$
$$a:\ \mathsf{SNo} = n_4 \quad [39]$$
$$a:\ \mathsf{SBit} = b_3 \quad [40]$$
$$a:\ \mathsf{ready} = \mathsf{true} \quad [41]$$

analog [27], SBit und SNo unverändert

Rechter Zweig:

$$a:\ \mathsf{SBit} = b_2 \quad [27]$$
$$a:\ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [28]$$

↪ S. 202

$\vdots$

von [36] (S. 191):

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(d_1, b_1)|Q'$ [21]

$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_3, b_3)$ [29]

$b:\ \mathsf{SBit} = b_3$ [30]

$b:\ \mathsf{RQ} = q_4$ [31]

$b:\ \mathsf{SNo} = n_4$ [32]

$a:\ \mathsf{RQ} = q_4|\mathsf{msg}(\mathsf{SFile}(s(n_4)), \mathsf{flip}(b_3))$ [34]

$a:\ \mathsf{SNo} = s(n_4)$ [35]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_3)$ [36]

mit Lemma 1, A1:

$b:\ \forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \to$ [42]
$(B = \mathsf{SBit} \to (\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge$
$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3))))$

$b:\ (\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_6)) \to (B_6 = \mathsf{SBit} \to (\ \dots\ ))$ [55]

$b:\ \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_6))$ [43]
$b:\ \neg(\mathsf{SIM} = \mathsf{msg}(D_6, B_6))$ [45]
$\Box\ \{D_6 \leftarrow d_3, B_6 \leftarrow b_3\}(29, 45)$

B_6 einsetzen:
$b:\ (b_3 = \mathsf{SBit} \to$ [44]
$((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_3)|Q^1)) \wedge$
$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_3)|Q^3))))$

$b:\ \neg(b_3 = \mathsf{SBit})$ [46]
$\Box\ (30, 46)$

$b:\ \mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_3)|Q^1)$ [47]
$b:\ \mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3)$ [48]
$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_3)|Q^3)$ [49]

aus [21]:

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [50]
$\hookrightarrow$ S. 193

$a:\ \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(d_1, b_1)|Q'$ [51]
$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'$ [114]
$\hookrightarrow$ S. 198

$\vdots$

von [50] (S. 192):

$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b:\ \mathsf{SIM} = \mathsf{msg}(d_3, b_3)$ [29]

$b:\ \mathsf{SBit} = b_3$ [30]

$b:\ \mathsf{RQ} = q_4$ [31]

$b:\ \mathsf{SNo} = n_4$ [32]

$a:\ \mathsf{RQ} = q_4|\mathsf{msg}(\mathsf{SFile}(s(n_4)), \mathsf{flip}(b_3))$ [34]

$a:\ \mathsf{SNo} = s(n_4)$ [35]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_3)$ [36]

$b:\ \mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3)$ [48]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_3)|Q^3)$ [49]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [50]

|

aus EA:

$b:\ \exists M : \mathsf{RIM} = M$ [52]

$b:\ \mathsf{RIM} = m_8$ [53]

|

aus RIM: $b:\ \forall M : \mathsf{RIM} = M \to \mathsf{A}(\mathsf{RIM} = M \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [54]

mit Tab. 0.11, $\{M \leftarrow m_8\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [55] | $a:\ \mathsf{RIM} = m_8$ [56]

$\hookrightarrow$ S. 196

$a:\ \mathsf{RecCom} = \mathsf{true}$ [57]

aus Tab. 0.1:

$b:\ \mathsf{RIM} = \perp$ [59]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_9, b_9)|q_9$ [60]

$a:\ \mathsf{RQ} = q_9$ [61]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_9, b_9)$ [62]

$a:\ \mathsf{AckMsg} = \mathsf{true}$ [58]

aus Tab. 0.8:

$a:\ \mathsf{RIM} = \perp$ [88]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_{13}, b_{13})$ [89]

$\square$ (E3, 50, 88)

aus [49]:

$b:\ \mathsf{RQ} = \varepsilon$ [63]

$\square$ (E2, 60, 63)

$b:\ \exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_3)|Q^3$ [64]

$b:\ \mathsf{RQ} = \mathsf{msg}(d^3_{10}, b_3)|q^3_{10}$ [65]

$\hookrightarrow$ S. 194

$\vdots$

von [65] (S. 193):

$a: \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b: \mathsf{SBit} = b_3$ [30]

$b: \mathsf{SNo} = n_4$ [32]

$a: \mathsf{SNo} = s(n_4)$ [35]

$a: \mathsf{SBit} = \mathsf{flip}(b_3)$ [36]

$a: \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [50]

$b: \mathsf{RQ} = \mathsf{msg}(d_9, b_9)|q_9$ [60]

$a: \mathsf{RIM} = \mathsf{msg}(d_9, b_9)$ [62]

$b: \mathsf{RQ} = \mathsf{msg}(d^3_{10}, b_3)|q^3_{10}$ [65]

|

aus [12]:

$b: (\mathsf{RIM} = \mathsf{msg}(D_{11}, B_{11}) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{11}, B_{11})|Q') \to$ [66]
$((B_{11} = \mathsf{SBit} \to D_{11} = \mathsf{SFile}(\mathsf{SNo})) \wedge (B_{11} = \mathsf{flip}(\mathsf{SBit}) \to D_{11} = \mathsf{SFile}(p(\mathsf{SNo}))))$

$b: \neg(\mathsf{RIM} = \mathsf{msg}(D_{11}, B_{11}) \vee$ [67]
$\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{11}, B_{11})|Q')$

|

$b: \neg(\mathsf{RIM} = \mathsf{msg}(D_{11}, B_{11}))$ [69]

$b: \neg(\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{11}, B_{11})|Q')$ [70]

$b: \neg(\mathsf{RQ} = Q_{11}|\mathsf{msg}(D_{11}, B_{11})|Q'_{11})$ [71]

$\Box\{Q_{11} \leftarrow \varepsilon,\ D_{11} \leftarrow d_9,\ B_{11} \leftarrow b_9,\ Q_{11} \leftarrow q_9\}(60, 71)$

$b: (b_9 = \mathsf{SBit} \to d_9 = \mathsf{SFile}(\mathsf{SNo})) \wedge$ [68]
$(b_9 = \mathsf{flip}(\mathsf{SBit}) \to d_9 = \mathsf{SFile}(p(\mathsf{SNo}))))$

|

$b: b_3 = \mathsf{SBit} \to d_9 = \mathsf{SFile}(\mathsf{SNo})$ [72]

$b: b_3 = \mathsf{flip}(\mathsf{SBit}) \to d_9 = \mathsf{SFile}(p(\mathsf{SNo}))$ [73]

|

aus [72]:

$b: \neg(b_3 = \mathsf{SBit})$ [74]

$\Box\ (30, 74)$

$b: d_9 = \mathsf{SFile}(\mathsf{SNo})$ [75]

aus SData:

$b: \forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\Box(\mathsf{SFile}(N) = D)$ [76]

$b: \mathsf{SFile}(N_{12}) = D_{12} \to \mathsf{A}\Box(\mathsf{SFile}(N_{12}) = D_{12})$ [77]

$b: \neg(\mathsf{SFile}(N_{12}) = D_{12}$ [78]

$\Box$: $b: d_9 = \mathsf{SFile}(\mathsf{SNo})$ [75]
$b: \mathsf{SNo} = n_4$ [32]
$\{N_{12} \leftarrow n_4,\ D_{12} \leftarrow d_9\}$

$b: \mathsf{A}\Box(\mathsf{SFile}(n_4) = d_9)$ [79]

$a: \mathsf{SFile}(n_4) = d_9$ [80]

$a: \mathsf{A}\Box(\mathsf{SFile}(n_4) = d_9)$ [81]

$\hookrightarrow$ S. 195

$$\vdots$$

von [81] (S. 194):

$$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))) \quad [22]$$

$$a:\ \mathsf{SNo} = s(n_4) \quad [35]$$

$$a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [36]$$

$$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [50]$$

$$b:\ \mathsf{RQ} = \mathsf{msg}(d_9, b_9)|q_9 \quad [60]$$

$$a:\ \mathsf{RIM} = \mathsf{msg}(d_9, b_9) \quad [62]$$

$$b:\ \mathsf{RQ} = \mathsf{msg}(d_{10}^3, b_3)|q_{10}^3 \quad [65]$$

aus [22]:

$$a:\ \neg(b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \quad [82]$$

$$a:\ b_1 = \mathsf{SBit} \quad [84]$$

$$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo})) \quad [85]$$

$$\boxed{\begin{array}{ll}
\Box: & b:\ \mathsf{RQ} = \mathsf{msg}(d_{10}^3, b_3)|q_{10}^3 \quad [65] \\
& b:\ \mathsf{RQ} = \mathsf{msg}(d_9, b_9)|q_9 \quad [60] \\ \hline
& \to\ b_3 = b_1 \\
& a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [50] \\
& a:\ \mathsf{RIM} = \mathsf{msg}(d_9, b_9) \quad [62] \\ \hline
& \to\ b_1 = b_9 \\
& a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [36] \\
& a:\ b_1 = \mathsf{SBit} \quad [84] \\ \hline
& \to\ \mathsf{flip}(b_3) = b_1
\end{array}}$$

$$a:\ \neg(b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [83]$$

$$a:\ b_1 = \mathsf{flip}(\mathsf{SBit}) \quad [86]$$

$$a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [87]$$

$$\boxed{\begin{array}{ll}
\Box: & a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [50] \\
& a:\ \mathsf{RIM} = \mathsf{msg}(d_9, b_9) \quad [62] \\ \hline
& \to\ d_1 = d_9 \\
& a:\ \mathsf{SFile}(n_4) = d_9 \quad [80] \\
& a:\ \mathsf{SNo} = s(n_4) \quad [35] \\
& a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [87] \\ \hline
& \to\ d_9 \neq d_1
\end{array}}$$

$\vdots$

von [56] (S. 193):

$a: \neg((b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b: \mathsf{SBit} = b_3$ [30]

$b: \mathsf{SNo} = n_4$ [32]

$a: \mathsf{SNo} = s(n_4)$ [35]

$a: \mathsf{SBit} = \mathsf{flip}(b_3)$ [36]

$b: \mathsf{RIM} = \perp \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3)$ [48]

$a: \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [50]

$b: \mathsf{RIM} = m_8$ [53]

$a: \mathsf{RIM} = m_8$ [56]

aus [48]:

$b: \mathsf{RIM} = \perp$ [90]

$\Box: a: \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [50]
$a: \mathsf{RIM} = m_8$ [56]
$b: \mathsf{RIM} = m_8$ [53]
$b: \mathsf{RIM} = \perp$ [48]

$b: \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_3)$ [91]

$b: \mathsf{RIM} = \mathsf{msg}(d_{10}^2, b_3)$ [92]

aus [12]:

$b: (\mathsf{RIM} = \mathsf{msg}(D_{14}, B_{14}) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{14}, B_{14})|Q') \rightarrow$ [93]
$((B_{14} = \mathsf{SBit} \rightarrow D_{14} = \mathsf{SFile}(\mathsf{SNo})) \wedge (B_{14} = \mathsf{flip}(\mathsf{SBit}) \rightarrow D_{14} = \mathsf{SFile}(p(\mathsf{SNo}))))$

$b: \neg(\mathsf{RIM} = \mathsf{msg}(D_{14}, B_{14}) \vee$ [94]
$\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{14}, B_{14})|Q')$

$b: \neg(\mathsf{RIM} = \mathsf{msg}(D_{14}, B_{14}))$ [96]

$b: \neg(\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{14}, B_{14})|Q')$ [97]

$\Box: a: \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [50]
$b: \mathsf{RIM} = m_8$ [53]
$a: \mathsf{RIM} = m_8$ [56]
$b: \neg(\mathsf{RIM} = \mathsf{msg}(D_{14}, B_{14}))$ [96]
$\{D_{14} \leftarrow d_1,\ B_{14} \leftarrow b_1\}$

$b: (b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge$ [95]
$(b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$

$b: b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo})$ [98]

$b: b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo}))$ [99]

$b: \neg(b_1 = \mathsf{SBit})$ [100]

$\Box: a: \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [50]
$a: \mathsf{RIM} = m_8$ [56]
$b: \mathsf{RIM} = m_8$ [53]
$b: \mathsf{RIM} = \mathsf{msg}(d_{10}^2, b_3)$ [92]
$\rightarrow b_3 = b_1$
$b: \mathsf{SBit} = b_3$ [30]
$b: \neg(b_1 = \mathsf{SBit})$ [100]
$\rightarrow b_3 \neq b_1$

$b: d_1 = \mathsf{SFile}(\mathsf{SNo})$ [101]

$\hookrightarrow$ S. 197

$\vdots$

von [101] (S. 196):

$$a: \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \land (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))) \quad [22]$$
$$b: \mathsf{SNo} = n_4 \quad [32]$$
$$a: \mathsf{SNo} = s(n_4) \quad [35]$$
$$a: \mathsf{SBit} = \mathsf{flip}(b_3) \quad [36]$$
$$a: \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [50]$$
$$b: \mathsf{RIM} = m_8 \quad [53]$$
$$a: \mathsf{RIM} = m_8 \quad [56]$$
$$b: \mathsf{RIM} = \mathsf{msg}(d_{10}^2, b_3) \quad [92]$$
$$b: d_1 = \mathsf{SFile}(\mathsf{SNo}) \quad [101]$$

aus SData:

$$b: \forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\Box(\mathsf{SFile}(N) = D) \quad [102]$$
$$b: \mathsf{SFile}(N_{15}) = D_{15} \to \mathsf{A}\Box(\mathsf{SFile}(N_{15}) = D_{15}) \quad [103]$$

Linker Zweig:

$$b: \neg(\mathsf{SFile}(N_{15}) = D_{15} \quad [104]$$

$$\boxed{\begin{array}{ll} \Box: & b: d_1 = \mathsf{SFile}(\mathsf{SNo}) \quad [101] \\ & b: \mathsf{SNo} = n_4 \quad [32] \\ & \{N_{15} \leftarrow n_4,\ D_{15} \leftarrow d_1\} \end{array}}$$

Rechter Zweig:

$$b: \mathsf{A}\Box(\mathsf{SFile}(n_4) = d_1) \quad [105]$$
$$a: \mathsf{SFile}(n_4) = d_1 \quad [106]$$
$$a: \mathsf{A}\Box(\mathsf{SFile}(n_4) = d_1) \quad [107]$$

aus [22]:

$$a: \neg(b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \quad [108]$$
$$a: b_1 = \mathsf{SBit} \quad [110]$$
$$a: \neg(d_1 = \mathsf{SFile}(\mathsf{SNo})) \quad [111]$$

$$\boxed{\begin{array}{ll} \Box: & a: \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [50] \\ & a: \mathsf{RIM} = m_8 \quad [56] \\ & b: \mathsf{RIM} = m_8 \quad [53] \\ & b: \mathsf{RIM} = \mathsf{msg}(d_{10}^2, b_3) \quad [92] \\ \hline & \to\ b_3 = b_1 \\ & a: \mathsf{SBit} = \mathsf{flip}(b_3) \quad [36] \\ & a: b_1 = \mathsf{SBit} \quad [110] \\ & \to\ \mathsf{flip}(b_3) = b_1 \end{array}}$$

$$a: \neg(b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [109]$$
$$a: b_1 = \mathsf{flip}(\mathsf{SBit}) \quad [112]$$
$$a: \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [113]$$

$$\boxed{\begin{array}{ll} \Box: & a: \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [113] \\ & a: \mathsf{SNo} = s(n_4) \quad [35] \\ & a: \mathsf{SFile}(n_4) = d_1 \quad [106] \end{array}}$$

$\vdots$

von [114] (S. 192):

$a:\ \neg((b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b:\ \mathsf{SBit} = b_3$ [30]

$b:\ \mathsf{RQ} = q_4$ [31]

$b:\ \mathsf{SNo} = n_4$ [32]

$a:\ \mathsf{RQ} = q_4|\mathsf{msg}(\mathsf{SFile}(s(n_4)), \mathsf{flip}(b_3))$ [34]

$a:\ \mathsf{SNo} = s(n_4)$ [35]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_3)$ [36]

$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_3)|Q^3)$ [49]

$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1'$ [114]

aus Q2:

$a:\ \forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)|Q') \rightarrow Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B'))$ [115]

$a:\ (\exists D, B : Q_{16} = \mathsf{msg}(D, B)|Q_{16}') \rightarrow Q_{16}' = \varepsilon \vee (\exists D', B', Q'' : Q_{16}' = Q''|\mathsf{msg}(D', B'))$ [116]

Linker Zweig:

$a:\ \neg(\exists D, B : Q_{16} = \mathsf{msg}(D, B)|Q_{16}')$ [117]

$a:\ \neg(Q_{16} = \mathsf{msg}(D_{16}, B_{16})|Q_{16}')$ [119]

$\Box\ \{Q_{16} \leftarrow \mathsf{msg}(d_1', b_1)|q_1', Q_{16}' \leftarrow q_1'\}(114, 119)$

Rechter Zweig:

$a:\ q_1' = \varepsilon \vee (\exists D', B', Q'' : q_1' = Q''|\mathsf{msg}(D', B'))$ [118]

$a:\ q_1' = \varepsilon$ [120]

$a:\ \exists D', B', Q'' : q_1' = Q''|\mathsf{msg}(D', B')$ [121]

$a:\ q_1' = q_{16}''|\mathsf{msg}(d_{16}', b_{16}')$ [128]

$\hookrightarrow$ S. 199

aus [22]:

$a:\ \neg(b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [122]

$a:\ b_1 = \mathsf{SBit}$ [124]

$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [125]

$a:\ \neg(b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [123]

$a:\ b_1 = \mathsf{flip}(\mathsf{SBit})$ [126]

$a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [127]

$\Box$: $a:\ q_1' = \varepsilon$ [120]
$a:\ \mathsf{RQ} = q_1\|\mathsf{msg}(d_1, b_1)\|q_1'$ [114]
$a:\ \mathsf{RQ} = q_4\|\mathsf{msg}(\mathsf{SFile}(s(n_4)), \mathsf{flip}(b_3))$ [34]
$\rightarrow\ a:\ d_1 = \mathsf{SFile}(s(n_4))$
$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [125]
$a:\ \mathsf{SNo} = s(n_4)$ [35]

$\Box$: $a:\ q_1' = \varepsilon$ [120]
$a:\ \mathsf{RQ} = q_1\|\mathsf{msg}(d_1, b_1)\|q_1'$ [114]
$a:\ \mathsf{RQ} = q_4\|\mathsf{msg}(\mathsf{SFile}(s(n_4)), \mathsf{flip}(b_3))$ [34]
$\rightarrow\ \mathsf{flip}(b_3) = b_1$
$a:\ \mathsf{SBit} = \mathsf{flip}(b_3)$ [36]
$a:\ b_1 = \mathsf{flip}(\mathsf{SBit})$ [126]
$\rightarrow\ b_1 = b_3$

$$\vdots$$

von [128] (S. 198):

$$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))) \quad [22]$$
$$b:\ \mathsf{SBit} = b_3 \quad [30]$$
$$b:\ \mathsf{RQ} = q_4 \quad [31]$$
$$b:\ \mathsf{SNo} = n_4 \quad [32]$$
$$a:\ \mathsf{RQ} = q_4|\mathsf{msg}(\mathsf{SFile}(s(n_4)), \mathsf{flip}(b_3)) \quad [34]$$
$$a:\ \mathsf{SNo} = s(n_4) \quad [35]$$
$$a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [36]$$
$$b:\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_3)|Q^3) \quad [49]$$
$$a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1' \quad [114]$$
$$a:\ q_1' = q_{16}''|\mathsf{msg}(d_{16}', b_{16}')) \quad [128]$$

$$|$$

das folgende Gleichheitsresultat wird auf diesem Ast in vielen Abschlüssen verwendet:

$$\boxed{\begin{array}{l} a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_1' \quad [114] \\ a:\ q_1' = q_{16}''|\mathsf{msg}(d_{16}', b_{16}')) \quad [128] \\ \hline \to\ a:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_{16}''|\mathsf{msg}(d_{16}', b_{16}') \\ a:\ \mathsf{RQ} = q_4|\mathsf{msg}(\mathsf{SFile}(s(n_4)), \mathsf{flip}(b_3)) \quad [34] \\ b:\ \mathsf{RQ} = q_4 \quad [31] \\ \hline \to\ b:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q_{16}'' \quad [(*)] \end{array}}$$

$$|$$

aus [49]:

$b:\ \mathsf{RQ} = \varepsilon \quad [129]$	$b:\ \exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_3)\vert Q^3 \quad [130]$
$\Box\ ((*), 129)$	$b:\ \mathsf{RQ} = \mathsf{msg}(d_{17}^3, b_3)\vert q_{17}^3 \quad [131]$

Lemma 1, A7 für RQ:

$$b:\ \forall B : (\exists D, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q) \to \quad [132]$$
$$(B = \mathsf{SBit} \to (\forall Q', Q'', D', B' : \mathsf{RQ} = Q'|\mathsf{msg}(D', B')|Q'' \to B' = \mathsf{SBit}))$$

$$|$$

$$b:\ (\exists D, Q : \mathsf{RQ} = \mathsf{msg}(D, B_{18})|Q) \to \quad [133]$$
$$(B_{18} = \mathsf{SBit} \to (\forall Q', Q'', D', B' : \mathsf{RQ} = Q'|\mathsf{msg}(D', B')|Q'' \to B' = \mathsf{SBit}))$$

$b:\ \neg(\exists D, Q : \mathsf{RQ} = \mathsf{msg}(D, B_{18})\vert Q) \quad [134]$	$b:\ \forall Q', Q'', D', B' : \quad [135]$
$b:\ \neg(\mathsf{RQ} = \mathsf{msg}(D_{18}, B_{18})\vert Q_{18}) \quad [136]$	$\mathsf{RQ} = Q'\vert\mathsf{msg}(D', B')\vert Q'' \to B' = \mathsf{SBit})$
$\Box\ \{D_{18} \leftarrow d_{17}^3,\ B_{18} \leftarrow b_3,\ Q_{18} \leftarrow q_{17}^3\}(131, 134)$	$\hookrightarrow$ S. 200

$\vdots$

von [135] (S. 199):

$$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))\quad [22]$$
$$b:\ \mathsf{SBit} = b_3\quad [30]$$
$$b:\ \mathsf{SNo} = n_4\quad [32]$$
$$a:\ \mathsf{SNo} = s(n_4)\quad [35]$$
$$a:\ \mathsf{SBit} = \mathsf{flip}(b_3)\quad [36]$$
$$b:\ \mathsf{RQ} = q_1|\mathsf{msg}(d_1, b_1)|q''_{16}\quad [(*)]$$
$$b:\ \forall Q', Q'', D', B' : \mathsf{RQ} = Q'|\mathsf{msg}(D', B')|Q'' \to B' = \mathsf{SBit})\quad [135]$$

$$b:\ \neg(b_3 = \mathsf{SBit})\quad [137]$$
$$\square\ (30, 137)$$

$$b:\ \forall Q', Q'', D', B' : \mathsf{RQ} = Q'|\mathsf{msg}(D', B')|Q'' \to B' = \mathsf{SBit}\quad [138]$$
$$b:\ \mathsf{RQ} = Q'_{18}|\mathsf{msg}(D'_{18}, B'_{18})|Q''_{18} \to B'_{18} = \mathsf{SBit}\quad [139]$$

$$b:\ \neg(\mathsf{RQ} = Q'_{18}|\mathsf{msg}(D'_{18}, B'_{18})|Q''_{18})\quad [140]$$
$$\square\ \{Q'_{18} \leftarrow q_1,\ D'_{18} \leftarrow d_1,\ \ B'_{18} \leftarrow b_1,\ Q''_{18} \leftarrow q''_{16}\}((*), 140)$$

$$b:\ b_1 = \mathsf{SBit}\quad [141]$$

aus [12]:

$$b:\ (\mathsf{RIM} = \mathsf{msg}(D_{19}, B_{19}) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{19}, B_{19})|Q') \to \quad [142]$$
$$((B_{19} = \mathsf{SBit} \to D_{19} = \mathsf{SFile}(\mathsf{SNo})) \wedge (B_{19} = \mathsf{flip}(\mathsf{SBit}) \to D_{19} = \mathsf{SFile}(p(\mathsf{SNo}))))$$

$$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{19}, B_{19}) \vee \quad [143]$$
$$\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{19}, B_{19})|Q')$$
$$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{19}, B_{19}))\quad [145]$$
$$b:\ \neg(\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{19}, B_{19})|Q')\quad [146]$$
$$b:\ \mathsf{RQ} = Q_{19}|\mathsf{msg}(D_{19}, B_{19})|Q')_{19}\quad [147]$$
$$\square\ \{Q_{19} \leftarrow q_1,\ D_{19} \leftarrow d_1,$$
$$B_{19} \leftarrow b_1,\ Q'_{19} \leftarrow q''_{16}\}((*), 147)$$

$$b:\ (b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge \quad [144]$$
$$(b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$$
$$b:\ b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})\quad [148]$$
$$b:\ b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))\quad [149]$$

$$b:\ \neg(b_1 = \mathsf{SBit})\quad [150]$$
$$\square\ (141, 150)$$

$$b:\ d_1 = \mathsf{SFile}(\mathsf{SNo})\quad [151]$$

$\hookrightarrow$ S. 201

$$\vdots$$

von [151] (S. 200):

$$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \land (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))) \quad [22]$$
$$b:\ \mathsf{SBit} = b_3 \quad [30]$$
$$b:\ \mathsf{SNo} = n_4 \quad [32]$$
$$a:\ \mathsf{SNo} = s(n_4) \quad [35]$$
$$a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [36]$$
$$b:\ b_1 = \mathsf{SBit} \quad [141]$$
$$b:\ d_1 = \mathsf{SFile}(\mathsf{SNo}) \quad [151]$$

aus SData:

$$b:\ \forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\Box(\mathsf{SFile}(N) = D) \quad [152]$$
$$b:\ \mathsf{SFile}(N_{21}) = D_{21} \to \mathsf{A}\Box(\mathsf{SFile}(N_{21}) = D_{21}) \quad [153]$$

Linker Zweig:

$$b:\ \neg(\mathsf{SFile}(N_{21}) = D_{21} \quad [154]$$

$$\boxed{\begin{array}{ll} \Box: & b:\ d_1 = \mathsf{SFile}(\mathsf{SNo}) \quad [151] \\ & b:\ \mathsf{SNo} = n_4 \quad [32] \\ & \{N_{21} \leftarrow n_4,\ D_{21} \leftarrow d_1\} \end{array}}$$

Rechter Zweig:

$$b:\ \mathsf{A}\Box(\mathsf{SFile}(n_4) = d_1) \quad [155]$$
$$a:\ \mathsf{SFile}(n_4) = d_1 \quad [156]$$
$$a:\ \mathsf{A}\Box(\mathsf{SFile}(n_4) = d_1) \quad [157]$$

aus [22]:

$$a:\ \neg(b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \quad [158]$$
$$a:\ b_1 = \mathsf{SBit} \quad [160]$$
$$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo})) \quad [161]$$

$$\boxed{\begin{array}{ll} \Box: & b:\ b_1 = \mathsf{SBit} \quad [141] \\ & b:\ \mathsf{SBit} = b_3 \quad [30] \\ \hline & \to\ b_3 = b_1 \\ & a:\ \mathsf{SBit} = \mathsf{flip}(b_3) \quad [36] \\ & a:\ b_1 = \mathsf{SBit} \quad [160] \\ \hline & \to\ b_3 = \mathsf{flip}(b_1) \end{array}}$$

$$a:\ \neg(b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [159]$$
$$a:\ b_1 = \mathsf{flip}(\mathsf{SBit}) \quad [162]$$
$$a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [163]$$

$$\boxed{\begin{array}{ll} \Box: & a:\ \mathsf{SFile}(n_4) = d_1 \quad [156] \\ & a:\ \mathsf{SNo} = s(n_4) \quad [35] \\ & a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [163] \end{array}}$$

$\vdots$

von [28] (S. 191):

$a: \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(d_1, b_1)|Q'$ [21]

$a: \ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b: \ \mathsf{SBit} = b_2$ [24]

$a: \ \mathsf{SBit} = b_2$ [27]

$a: \ \neg(\mathsf{ProcAck} = \mathsf{true})$ [28]

aus EA:

$b: \ \exists N : \mathsf{SNo} = N$ [163]

$b: \ \mathsf{SNo} = n_{22}$ [164]

aus SNo: $b: \ \forall N : \mathsf{SNo} = N \to \mathsf{A}(\mathsf{SNo} = N \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true})$ [165]

mit Tab. 0.11, $\{N \leftarrow n_{22}\}$:

$a: \ \mathsf{ProcAck} = \mathsf{true}$ [166]

$\square$ $(28, 166)$

$a: \ \mathsf{SNo} = n_{22}$ [167]

aus [21]:

$a: \ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [168]

aus EA:

$b: \ \exists M : \mathsf{RIM} = M$ [170]

$b: \ \mathsf{RIM} = m_{23}$ [171]

aus RIM:

$b: \ \forall M : \mathsf{RIM} = M \to \mathsf{A}(\mathsf{RIM} = M \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [172]

mit Tab. 0.11, $\{M \leftarrow m_{23}\}$:

$a: \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [173]

$a: \ \mathsf{RecCom} = \mathsf{true}$ [175]

aus Tab. 0.1:

$b: \ \mathsf{RIM} = \perp$ [177]

$b: \ \mathsf{RQ} = \mathsf{msg}(d_{24}, b_{24})|q_{24}$ [178]

$a: \ \mathsf{RQ} = q_{24}$ [179]

$a: \ \mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})$ [180]

$\hookrightarrow$ S. 203

$a: \ \mathsf{AckMsg} = \mathsf{true}$ [176]

aus Tab. 0.8:

$a: \ \mathsf{RIM} = \perp$ []

$b: \ \mathsf{RIM} = \mathsf{msg}(d, b)$ []

$\square$ $(\mathrm{E3}, 161,)$

$a: \ \mathsf{RIM} = m_{23}$ [174]

$\hookrightarrow$ S. 206

$a: \ \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(d_1, b_1)|Q'$ [169]

$a: \ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30}$ [240]

$\hookrightarrow$ S. 209

$\vdots$

von [180] (S. 202):

$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \land (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b:\ \mathsf{SBit} = b_2$ [24]

$a:\ \mathsf{SBit} = b_2$ [27]

$b:\ \mathsf{SNo} = n_{22}$ [164]

$a:\ \mathsf{SNo} = n_{22}$ [167]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [168]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{24}, b_{24})|q_{24}$ [178]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})$ [180]

|

aus [12] :

$b:\ (\mathsf{RIM} = \mathsf{msg}(D_{25}, B_{25}) \lor \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{25}, B_{25})|Q') \to$ [181]
$((B_{25} = \mathsf{SBit} \to D_{25} = \mathsf{SFile}(\mathsf{SNo})) \land (B_{25} = \mathsf{flip}(\mathsf{SBit}) \to D_{25} = \mathsf{SFile}(p(\mathsf{SNo}))))$

Left branch:

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{25}, B_{25}) \lor$ [182]
$\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{25}, B_{25})|Q')$

|

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{25}, B_{25}))$ [184]

$b:\ \neg(\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{25}, B_{25})|Q')$ [185]

$b:\ \neg(\mathsf{RQ} = Q_{25}|\mathsf{msg}(D_{25}, B_{25})|Q'_{25})$ [186]

$\Box\ \{Q_{25} \leftarrow \varepsilon,\ D_{25} \leftarrow d_{24},$
$B_{25} \leftarrow b_{24},\ Q_{25} \leftarrow q_{24}\}(178, 186)$

Right branch:

$b:\ (b_{24} = \mathsf{SBit} \to d_{24} = \mathsf{SFile}(\mathsf{SNo})) \land$ [183]
$(b_{24} = \mathsf{flip}(\mathsf{SBit}) \to d_{24} = \mathsf{SFile}(p(\mathsf{SNo}))))$

|

$b:\ b_{24} = \mathsf{SBit} \to d_{24} = \mathsf{SFile}(\mathsf{SNo})$ [187]

$b:\ b_{24} = \mathsf{flip}(\mathsf{SBit}) \to d_{24} = \mathsf{SFile}(p(\mathsf{SNo}))$ [188]

|

aus [22]:

$a:\ \neg(b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [189]

$a:\ b_1 = \mathsf{SBit}$ [191]

$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [192]

$\hookrightarrow$ S. 204

$a:\ \neg(b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [190]

$a:\ b_1 = \mathsf{flip}(\mathsf{SBit})$ [193]

$a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [194]

$\hookrightarrow$ S. 205

$\vdots$

von [192] (S. 203):

$b:\ \mathsf{SBit} = b_2 \quad [24]$

$a:\ \mathsf{SBit} = b_2 \quad [27]$

$b:\ \mathsf{SNo} = n_{22} \quad [164]$

$a:\ \mathsf{SNo} = n_{22} \quad [167]$

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [168]$

$a:\ \mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24}) \quad [180]$

$b:\ b_{24} = \mathsf{SBit} \rightarrow d_{24} = \mathsf{SFile}(\mathsf{SNo}) \quad [187]$

$a:\ b_1 = \mathsf{SBit} \quad [191]$

$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo})) \quad [192]$

aus [187]:

$b:\ \neg(b_{24} = \mathsf{SBit}) \quad [195]$

$$\boxed{\begin{array}{ll} \Box: & \dfrac{a:\ b_1 = \mathsf{SBit}\ [191] \quad a:\ \mathsf{SBit} = b_2\ [27]}{\rightarrow\ b_1 = b_2} \qquad \dfrac{b:\ \mathsf{SBit} = b_2\ [24] \quad b:\ \neg(b_{24} = \mathsf{SBit})\ [195]}{\rightarrow\ b_2 \neq b_{24}} \\ & \dfrac{a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)\ [168] \quad a:\ \mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})\ [180]}{\rightarrow\ b_1 = b_{24}} \end{array}}$$

$b:\ d_{24} = \mathsf{SFile}(\mathsf{SNo}) \quad [196]$

aus SData:

$b:\ \forall D, N : \mathsf{SFile}(N) = D \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N) = D) \quad [197]$

$b:\ \mathsf{SFile}(N_{25}) = D_{25} \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N_{25}) = D_{25}) \quad [198]$

$b:\ \neg(\mathsf{SFile}(N_{25}) = D_{25} \quad [199]$

$$\boxed{\begin{array}{ll} \Box: & b:\ d_{24} = \mathsf{SFile}(\mathsf{SNo})\ [196] \\ & b:\ \mathsf{SNo} = n_{22}\ [164] \\ & \{N_{25} \leftarrow n_{22},\ D_{25} \leftarrow d_{24}\} \end{array}}$$

$b:\ \mathsf{A}\Box(\mathsf{SFile}(n_{22}) = d_{24}) \quad [200]$

$a:\ \mathsf{SFile}(n_{22}) = d_{24} \quad [201]$

$a:\ \mathsf{A}\Box(\mathsf{SFile}(n_{22}) = d_{24}) \quad [202]$

$$\boxed{\begin{array}{ll} \Box: & \dfrac{a:\ \mathsf{SFile}(n_{22}) = d_{24}\ [201] \quad a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo}))\ [192] \quad a:\ \mathsf{SNo} = n_{22}\ [167]}{\rightarrow\ d_1 \neq d_{24}} \\ & \dfrac{a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)\ [168] \quad a:\ \mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})\ [180]}{\rightarrow\ d_1 = d_{24}} \end{array}}$$

$\vdots$

von [194] (S. 203):

$b:$ $\mathsf{SBit} = b_2$ [24]

$a:$ $\mathsf{SBit} = b_2$ [27]

$b:$ $\mathsf{SNo} = n_{22}$ [164]

$a:$ $\mathsf{SNo} = n_{22}$ [167]

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [168]

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})$ [180]

$b:$ $b_{24} = \mathsf{flip}(\mathsf{SBit}) \to d_{24} = \mathsf{SFile}(p(\mathsf{SNo}))$ [188]

$a:$ $b_1 = \mathsf{flip}(\mathsf{SBit})$ [193]

$a:$ $\neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [194]

aus [188]:

$b:$ $\neg(b_{24} = \mathsf{flip}(\mathsf{SBit}))$ [203]

$\Box:$

$a:$ $b_1 = \mathsf{flip}(\mathsf{SBit})$ [193]

$a:$ $\mathsf{SBit} = b_2$ [27]

$\to$ $\mathsf{flip}(b_1) = b_2$

$b:$ $\mathsf{SBit} = b_2$ [24]

$b:$ $\neg(b_{24} = \mathsf{flip}(\mathsf{SBit}))$ [203]

$\to$ $\mathsf{flip}(b_2) \neq b_{24}$

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [168]

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})$ [180]

$\to$ $b_1 = b_{24}$

$b:$ $d_{24} = \mathsf{SFile}(p(\mathsf{SNo}))$ [204]

aus SData:

$b:$ $\forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\Box(\mathsf{SFile}(N) = D)$ [205]

$b:$ $\mathsf{SFile}(N_{26}) = D_{26} \to \mathsf{A}\Box(\mathsf{SFile}(N_{26}) = D_{26})$ [206]

$b:$ $\neg(\mathsf{SFile}(N_{26}) = D_{26}$ [207]

$\Box:$ $b:$ $d_{24} = \mathsf{SFile}(p(\mathsf{SNo}))$ [204]

$b:$ $\mathsf{SNo} = n_{22}$ [164]

$\{N_{26} \leftarrow p(n_{22}),\ D_{26} \leftarrow d_{24}\}$

$b:$ $\mathsf{A}\Box(\mathsf{SFile}(p(n_{22})) = d_{24})$ [208]

$a:$ $\mathsf{SFile}(p(n_{22})) = d_{24}$ [209]

$a:$ $\mathsf{A}\Box(\mathsf{SFile}(p(n_{22})) = d_{24})$ [210]

$\Box:$ $a:$ $\mathsf{SFile}(p(n_{22})) = d_{24}$ [209]

$a:$ $\neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [194]

$a:$ $\mathsf{SNo} = n_{22}$ [167]

$\to$ $d_1 \neq d_{24}$

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [168]

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_{24}, b_{24})$ [180]

$\to$ $d_1 = d_{24}$

$\vdots$

von [174] (S. 202):

$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \land (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b:\ \mathsf{SBit} = b_2$ [24]

$a:\ \mathsf{SBit} = b_2$ [27]

$b:\ \mathsf{SNo} = n_{22}$ [164]

$a:\ \mathsf{SNo} = n_{22}$ [167]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [168]

$b:\ \mathsf{RIM} = m_{23}$ [171]

$a:\ \mathsf{RIM} = m_{23}$ [174]

aus [12] :

$b:\ (\mathsf{RIM} = \mathsf{msg}(D_{25}, B_{27}) \lor \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{27}, B_{27})|Q') \to$ [211]
$((B_{27} = \mathsf{SBit} \to D_{27} = \mathsf{SFile}(\mathsf{SNo})) \land (B_{27} = \mathsf{flip}(\mathsf{SBit}) \to D_{27} = \mathsf{SFile}(p(\mathsf{SNo}))))$

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{27}, B_{27}) \lor$ [212]
$\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{27}, B_{27})|Q')$

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{27}, B_{27}))$ [214]

$b:\ \neg(\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{27}, B_{27})|Q')$ [215]

$\Box:\ a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [168]
$a:\ \mathsf{RIM} = m_{23}$ [174]
$b:\ \mathsf{RIM} = m_{23}$ [171]
$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{27}, B_{27}))$ [214]
$\{D_{27} \leftarrow d_1,\ B_{27} \leftarrow b_1\}$

$b:\ (b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \land$ [213]
$(b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$

$b:\ b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})$ [216]

$b:\ b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))$ [217]

aus [22]:

$a:\ \neg(b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [218]

$a:\ b_1 = \mathsf{SBit}$ [220]

$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [221]

$\hookrightarrow$ S. 207

$a:\ \neg(b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [219]

$a:\ b_1 = \mathsf{flip}(\mathsf{SBit})$ [222]

$a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [223]

$\hookrightarrow$ S. 208

$\vdots$

von [221] (S. 206):

$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile(SNo)}) \land (b_1 = \mathsf{flip(SBit)} \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b:\ \mathsf{SBit} = b_2$ [24]

$a:\ \mathsf{SBit} = b_2$ [27]

$b:\ \mathsf{SNo} = n_{22}$ [164]

$a:\ \mathsf{SNo} = n_{22}$ [167]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [168]

$b:\ b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile(SNo)}$ [216]

$a:\ b_1 = \mathsf{SBit}$ [220]

$a:\ \neg(d_1 = \mathsf{SFile(SNo)})$ [221]

aus [216]:

$b:\ \neg(b_1 = \mathsf{SBit})$ [224]

$\Box:\ a:\ \mathsf{SBit} = b_2$ [27]
$a:\ b_1 = \mathsf{SBit}$ [220]
$\to\ b_2 = b_1$
$b:\ \mathsf{SBit} = b_2$ [24]
$b:\ \neg(b_1 = \mathsf{SBit})$ [224]
$\to\ b_2 \neq b_1$

$b:\ d_1 = \mathsf{SFile(SNo)}$ [225]

aus SData:

$b:\ \forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\Box(\mathsf{SFile}(N) = D)$ [226]

$b:\ \mathsf{SFile}(N_{28}) = D_{28} \to \mathsf{A}\Box(\mathsf{SFile}(N_{28}) = D_{28})$ [227]

$b:\ \neg(\mathsf{SFile}(N_{28}) = D_{28}$ [228]

$\Box:\ b:\ d_1 = \mathsf{SFile(SNo)}$ [225]
$b:\ \mathsf{SNo} = n_{22}$ [164]
$\{N_{28} \leftarrow n_{22},\ D_{28} \leftarrow d_1\}$

$b:\ \mathsf{A}\Box(\mathsf{SFile}(n_{22}) = d_1)$ [229]

$a:\ \mathsf{SFile}(n_{22}) = d_1$ [230]

$a:\ \mathsf{A}\Box(\mathsf{SFile}(n_{22}) = d_1)$ [231]

$\Box:\ a:\ \neg(d_1 = \mathsf{SFile(SNo)})$ [221]
$a:\ \mathsf{SNo} = n_{22}$ [167]
$a:\ \mathsf{A}\Box(\mathsf{SFile}(n_{22}) = d_1)$ [231]

$$\vdots$$

von [223] (S. 206):

$$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))) \quad [22]$$
$$b:\ \mathsf{SBit} = b_2 \quad [24]$$
$$a:\ \mathsf{SBit} = b_2 \quad [27]$$
$$b:\ \mathsf{SNo} = n_{22} \quad [164]$$
$$a:\ \mathsf{SNo} = n_{22} \quad [167]$$
$$a:\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1) \quad [168]$$
$$b:\ b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})) \quad [217]$$
$$a:\ b_1 = \mathsf{flip}(\mathsf{SBit}) \quad [222]$$
$$a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [223]$$

aus [217]:

$$b:\ \neg(b_1 = \mathsf{flip}(\mathsf{SBit})) \quad [232]$$

$$\boxed{\begin{array}{ll} \square: & a:\ b_1 = \mathsf{flip}(\mathsf{SBit}) \quad [222] \\ & a:\ \mathsf{SBit} = b_2 \quad [27] \\ \hline & \to\ \mathsf{flip}(b_1) = b_2 b:\ \mathsf{SBit} = b_2 \quad [24] \\ & b:\ \neg(b_1 = \mathsf{flip}(\mathsf{SBit})) \quad [232] \\ \hline & \to\ b_2 \neq \mathsf{flip}(b_2) \end{array}}$$

$$b:\ d_1 = \mathsf{SFile}(p(\mathsf{SNo})) \quad [233]$$

aus SData:

$$b:\ \forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\square(\mathsf{SFile}(N) = D) \quad [234]$$
$$b:\ \mathsf{SFile}(N_{29}) = D_{29} \to \mathsf{A}\square(\mathsf{SFile}(N_{29}) = D_{29}) \quad [235]$$

$$b:\ \neg(\mathsf{SFile}(N_{29}) = D_{29} \quad [236]$$

$$\boxed{\begin{array}{ll} \square: & b:\ d_1 = \mathsf{SFile}(p(\mathsf{SNo})) \quad [233] \\ & b:\ \mathsf{SNo} = n_{22} \quad [164] \\ & \{N_{29} \leftarrow p(n_{22}),\ D_{29} \leftarrow d_1\} \end{array}}$$

$$b:\ \mathsf{A}\square(\mathsf{SFile}(p(n_{22})) = d_1) \quad [237]$$
$$a:\ \mathsf{SFile}(p(n_{22})) = d_1 \quad [238]$$
$$a:\ \mathsf{A}\square(\mathsf{SFile}(p(n_{22})) = d_1) \quad [239]$$

$$\boxed{\begin{array}{ll} \square: & a:\ \mathsf{SFile}(p(n_{22})) = d_1 \quad [238] \\ & a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [223] \\ & a:\ \mathsf{SNo} = n_{22} \quad [167] \end{array}}$$

$\vdots$

von [240] (S. 202):

$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile(SNo)}) \wedge (b_1 = \mathsf{flip(SBit)} \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b:\ \mathsf{SBit} = b_2$ [24]

$a:\ \mathsf{SBit} = b_2$ [27]

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [28]

$b:\ \mathsf{SNo} = n_{22}$ [164]

$a:\ \mathsf{SNo} = n_{22}$ [167]

$a:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30}$ [240]

aus EA:

$b:\ \exists Q : \mathsf{RQ} = Q$ [241]

$b:\ \mathsf{RQ} = q_{31}$ [242]

aus RQ: $b:\ \forall Q : \mathsf{RQ} = Q \to \mathsf{A}(\mathsf{RQ} = Q\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [243]

mit Tab. 0.11, $\{Q \leftarrow q_{31}\}$:

$a:\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}$ [244]

$a:\ \mathsf{RQ} = q_{31}$ [245]

relevant ist nur
$a:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30}$ [240]
$a:\ \mathsf{RQ} = q_{31}$ [245]
$b:\ \mathsf{RQ} = q_{31}$ [242]

$\to\ b:\ \mathsf{RQ} = q|\mathsf{msg}(d_1, b_1)|q'$ [(**)]

$\hookrightarrow$ S. 212

$a:\ \mathsf{RecCom} = \mathsf{true}$ [246]

aus Tab. 0.2:

$b:\ \mathsf{RIM} = \perp$ [250]

$b:\ \mathsf{RQ} = \mathsf{msg}(d_{32}, b_{32})|q_{32}$ [251]

$a:\ \mathsf{RQ} = q_{32}$ [252]

$a:\ \mathsf{RIM} = \mathsf{msg}(d_{32}, b_{32})$ [253]

wie [245] mit
$b:\ \mathsf{RQ} = \mathsf{msg}(d_{32}, b_{32})|q_{32}$ [251]
$a:\ \mathsf{RQ} = q_{32}$ [252]
$a:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30}$ [240]

$b : \mathsf{RQ} = \mathsf{msg}(d_{32}, b_{32})|q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30}$

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [249]

$\square$ (28, 249)

$a:\ \mathsf{ReTrans} = \mathsf{true}$ [248]

$\hookrightarrow$ S. 211

$a:\ \mathsf{RLose} = \mathsf{true}$ [247]

mit Tab. 0.3:

$a:\ \neg(\mathsf{RQ} = Q_{32}|\mathsf{msg}(D_{32}, B_{32})|Q'_{32})$ [254]

$\square\ \{Q_{32} \leftarrow q_{30},\ D_{32} \leftarrow d_1$
$B_{32} \leftarrow b_1,\ Q'_{32} \leftarrow q'_{30}\}(240, 254)$

$b:\ \mathsf{RQ} = r_{32}|\mathsf{msg}(d_1, b_1)|r'_{32}$ [255]

wie [245] mit
$b:\ \mathsf{RQ} = r_{32}|\mathsf{msg}(d_1, b_1)|r'_{32}$ [255]

$$\vdots$$

von [265] (S. 210):

$$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))) \quad [22]$$

$$b:\ \mathsf{SBit} = b_2 \quad [24]$$

$$a:\ \mathsf{SBit} = b_2 \quad [27]$$

$$a:\ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [28]$$

$$b:\ \mathsf{SNo} = n_{22} \quad [164]$$

$$a:\ \mathsf{SNo} = n_{22} \quad [167]$$

$$a:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30} \quad [240]$$

$$a:\ \mathsf{ReTrans} = \mathsf{true} \quad [248]$$

$$|$$

aus Tab. 0.6:

$$b:\ \mathsf{RQ} = q_{33} \quad [256]$$

$$b:\ \mathsf{SNo} = n_{33} \quad [257]$$

$$b:\ \mathsf{SBit} = b_{33} \quad [258]$$

$$a:\ \mathsf{RQ} = q_{33}|\mathsf{msg}(\mathsf{SFile}(n_{33}), b_{33}) \quad [259]$$

$$|$$

aus Q2:

$$a:\ \forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)|Q') \to Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B')) \quad [260]$$

$$a:\ (\exists D, B : Q_{34} = \mathsf{msg}(D, B)|Q'_{34}) \to Q'_{34} = \varepsilon \vee (\exists D', B', Q'' : Q'_{34} = Q''|\mathsf{msg}(D', B')) \quad [261]$$

$$a:\ \neg(\exists D, B : Q_{34} = \mathsf{msg}(D, B)|Q'_{34}) \quad [262]$$

$$a:\ \neg(Q_{34} = \mathsf{msg}(D_{34}, B_{34})|Q'_{34}) \quad [264]$$

$$\square\ \{Q_{34} \leftarrow \mathsf{msg}(d'_1, b_1)|q'_{30}, Q'_{34} \leftarrow q'_{30}\}(240, 264)$$

$$a:\ q'_{30} = \varepsilon \vee (\exists D', B', Q'' : q'_{30} = Q''|\mathsf{msg}(D', B')) \quad [263]$$

$$a:\ q'_{30} = \varepsilon \quad [265]$$

$\hookrightarrow$ S. 210

$$a:\ \exists D', B', Q'' : q'_{30} = Q''|\mathsf{msg}(D', B') \quad [266]$$

$$a:\ q'_{30} = q''_{34}|\mathsf{msg}(d'_{34}, b'_{34}) \quad [273]$$

wie [245] mit

$$\begin{array}{l}
a:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30} \quad [240] \\
a:\ q'_{30} = q''_{34}|\mathsf{msg}(d'_{34}, b'_{34}) \quad [273] \\
\hline
a:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q''_{34}|\mathsf{msg}(d'_{34}, b'_{34}) \\
a:\ \mathsf{RQ} = q_{33}|\mathsf{msg}(\mathsf{SFile}(n_{33}), b_{33}) \quad [259] \\
b:\ \mathsf{RQ} = q_{33} \quad [256] \\
\hline
b:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q''_{34}
\end{array}$$

$$\vdots$$

von [248] (S. 209):

$a:\ \neg((b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$ [22]

$b:\ \mathsf{SBit} = b_2$ [24]

$a:\ \mathsf{SBit} = b_2$ [27]

$a:\ \mathsf{SNo} = n_{22}$ [167]

$a:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30}$ [240]

$b:\ \mathsf{SNo} = n_{33}$ [257]

$b:\ \mathsf{SBit} = b_{33}$ [258]

$a:\ \mathsf{RQ} = q_{33}|\mathsf{msg}(\mathsf{SFile}(n_{33}), b_{33})$ [259]

$a:\ q'_{30} = \varepsilon$ [265]

aus [22]:

Linker Zweig:

$a:\ \neg(b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [267]

$a:\ b_1 = \mathsf{SBit}$ [269]

$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [270]

$\square$: $a:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30}$ [240]
$a:\ q'_{30} = \varepsilon$ [265]
$a:\ \mathsf{RQ} = q_{33}|\mathsf{msg}(\mathsf{SFile}(n_{33}), b_{33})$ [259]

$\rightarrow\ a:\ d_1 = \mathsf{SFile}(n_{33})$

$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [270]
$a:\ \mathsf{SNo} = n_{22}$ [167]
$b:\ \mathsf{SNo} = n_{22}$ [164]
$b:\ \mathsf{SNo} = n_{33}$ [257]

$\rightarrow\ a:\ \neg(d_1 = \mathsf{SFile}(n_{33}))$

Rechter Zweig:

$a:\ \neg(b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [268]

$a:\ b_1 = \mathsf{flip}(\mathsf{SBit})$ [271]

$a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo})))$ [272]

$\square$: $a:\ \mathsf{RQ} = q_{30}|\mathsf{msg}(d_1, b_1)|q'_{30}$ [240]
$a:\ q'_{30} = \varepsilon$ [265]
$a:\ \mathsf{RQ} = q_{33}|\mathsf{msg}(\mathsf{SFile}(n_{33}), b_{33})$ [259]

$\rightarrow\ b_1 = b_{33}$

$b:\ \mathsf{SBit} = b_{33}$ [258]
$b:\ \mathsf{SBit} = b_2$ [24]

$\rightarrow\ b_{33} = b_2$

$a:\ \mathsf{SBit} = b_2$ [27]
$a:\ b_1 = \mathsf{flip}(\mathsf{SBit})$ [271]

$\rightarrow\ b_2 = \mathsf{flip}(b_1)$

$$\vdots$$

von [245] (S. 209):

$$a:\ \neg((b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge (b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})))) \quad [22]$$

$$b:\ \mathsf{SBit} = b_2 \quad [24]$$

$$a:\ \mathsf{SBit} = b_2 \quad [27]$$

$$b:\ \mathsf{SNo} = n_{22} \quad [164]$$

$$a:\ \mathsf{SNo} = n_{22} \quad [167]$$

$$b:\ \mathsf{RQ} = q|\mathsf{msg}(d_1, b_1)|q' \quad [(**)]$$

$$|$$

aus [12]:

$$b:\ (\mathsf{RIM} = \mathsf{msg}(D_{35}, B_{35}) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{35}, B_{35})|Q') \to \quad [274]$$
$$((B_{35} = \mathsf{SBit} \to D_{35} = \mathsf{SFile}(\mathsf{SNo})) \wedge (B_{35} = \mathsf{flip}(\mathsf{SBit}) \to D_{35} = \mathsf{SFile}(p(\mathsf{SNo}))))$$

Left branch:

$$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{35}, B_{35}) \vee \quad [275]$$
$$\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{35}, B_{35})|Q')$$

$$|$$

$$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{35}, B_{35})) \quad [277]$$

$$b:\ \neg(\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{35}, B_{35})|Q') \quad [278]$$

$$b:\ \mathsf{RQ} = Q_{35}|\mathsf{msg}(D_{35}, B_{35})|Q')_{35} \quad [279]$$

$$\square\ \{Q_{35} \leftarrow q,\ D_{35} \leftarrow d_1,$$
$$B_{35} \leftarrow b_1,\ Q'_{35} \leftarrow q'\}((**), 278)$$

Right branch:

$$b:\ (b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \wedge \quad [276]$$
$$(b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))))$$

$$|$$

$$b:\ b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo}) \quad [279]$$

$$b:\ b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo})) \quad [280]$$

$$|$$

aus [22]:

$$a:\ \neg(b_1 = \mathsf{SBit} \to d_1 = \mathsf{SFile}(\mathsf{SNo})) \quad [281]$$

$$a:\ b_1 = \mathsf{SBit} \quad [283]$$

$$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo})) \quad [284]$$

$\hookrightarrow$ S. 213

$$a:\ \neg(b_1 = \mathsf{flip}(\mathsf{SBit}) \to d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [282]$$

$$a:\ b_1 = \mathsf{flip}(\mathsf{SBit}) \quad [285]$$

$$a:\ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [286]$$

$\hookrightarrow$ S. 214

$\vdots$

von [284] (S. 212):

$b:\ \mathsf{SBit} = b_2$ [24]

$a:\ \mathsf{SBit} = b_2$ [27]

$b:\ \mathsf{SNo} = n_{22}$ [164]

$a:\ \mathsf{SNo} = n_{22}$ [167]

$b:\ b_1 = \mathsf{SBit} \rightarrow d_1 = \mathsf{SFile}(\mathsf{SNo})$ [279]

$a:\ b_1 = \mathsf{SBit}$ [283]

$a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [284]

aus [279]:

$b:\ \neg(b_1 = \mathsf{SBit})$ [287]

$\Box:$ $a:\ \mathsf{SBit} = b_2$ [27]
$a:\ b_1 = \mathsf{SBit}$ [283]
$\rightarrow\ b_2 = b_1$
$b:\ \mathsf{SBit} = b_2$ [24]
$b:\ \neg(b_1 = \mathsf{SBit})$ [287]
$\rightarrow\ \neg b_2 = b_1$

$b:\ d_1 = \mathsf{SFile}(\mathsf{SNo})$ [288]

aus SData:

$b:\ \forall D, N : \mathsf{SFile}(N) = D \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N) = D)$ [289]

$b:\ \mathsf{SFile}(N_{36}) = D_{36} \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N_{36}) = D_{36})$ [290]

$b:\ \neg(\mathsf{SFile}(N_{36}) = D_{36})$ [291]

$\Box:$ $b:\ d_1 = \mathsf{SFile}(\mathsf{SNo})$ [288]
$b:\ \mathsf{SNo} = n_{22}$ [164]
$\{N_{36} \leftarrow n_{22},\ D_{36} \leftarrow d_1\}$

$b:\ \mathsf{A}\Box(\mathsf{SFile}(n_{22}) = d_1)$ [292]

$a:\ \mathsf{SFile}(n_{22}) = d_1$ [293]

$a:\ \mathsf{A}\Box(\mathsf{SFile}(n_{22}) = d_1)$ [294]

$\Box:$ $a:\ \neg(d_1 = \mathsf{SFile}(\mathsf{SNo}))$ [284]
$a:\ \mathsf{SFile}(n_{22}) = d_1$ [293]
$a:\ \mathsf{SNo} = n_{22}$ [167]

$\vdots$

von [286] (S. 212):

$b: \ \mathsf{SBit} = b_2 \quad [24]$

$a: \ \mathsf{SBit} = b_2 \quad [27]$

$b: \ \mathsf{SNo} = n_{22} \quad [164]$

$a: \ \mathsf{SNo} = n_{22} \quad [167]$

$b: \ b_1 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_1 = \mathsf{SFile}(p(\mathsf{SNo})) \quad [280]$

$a: \ b_1 = \mathsf{flip}(\mathsf{SBit}) \quad [285]$

$a: \ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [286]$

aus [280]:

$b: \ \neg(b_1 = \mathsf{flip}(\mathsf{SBit})) \quad [295]$

$\square: \ a: \ \mathsf{SBit} = b_2 \quad [27]$

$a: \ b_1 = \mathsf{flip}(\mathsf{SBit}) \quad [285]$

$\rightarrow \ \mathsf{flip}(b_2) = b_1$

$b: \ \mathsf{SBit} = b_2 \quad [24]$

$b: \ \neg(b_1 = \mathsf{flip}(\mathsf{SBit})) \quad [295]$

$\rightarrow \ \neg\mathsf{flip}(b_2) = b_1$

$b: \ d_1 = \mathsf{SFile}(p(\mathsf{SNo})) \quad [296]$

aus SData:

$b: \ \forall D, N: \mathsf{SFile}(N) = D \rightarrow \mathsf{A}\square(\mathsf{SFile}(N) = D) \quad [297]$

$b: \ \mathsf{SFile}(N_{37}) = D_{37} \rightarrow \mathsf{A}\square(\mathsf{SFile}(N_{37}) = D_{37}) \quad [298]$

$b: \ \neg(\mathsf{SFile}(N_{37}) = D_{37}) \quad [299]$

$\square: \ b: \ d_1 = \mathsf{SFile}(p(\mathsf{SNo})) \quad [296]$

$b: \ \mathsf{SNo} = n_{22} \quad [164]$

$\{N_{37} \leftarrow p(n_{22}),\ D_{37} \leftarrow d_1\}$

$b: \ \mathsf{A}\square(\mathsf{SFile}(p(n_{22})) = d_1) \quad [300]$

$a: \ \mathsf{SFile}(p(n_{22})) = d_1 \quad [301]$

$a: \ \mathsf{A}\square(\mathsf{SFile}(p(n_{22})) = d_1) \quad [302]$

$\square: \ a: \ \mathsf{SFile}(p(n_{22})) = d_1 \quad [301]$

$a: \ \neg(d_1 = \mathsf{SFile}(p(\mathsf{SNo}))) \quad [286]$

$a: \ \mathsf{SNo} = n_{22} \quad [167]$

10 Korollar 1: Am Dateiende ist Schluß

$$\mathsf{A}\Box(\mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot)$$

Beweis: Induktion.

$0: \ \mathsf{SNo} = 0 \quad [2]$

$0: \ \neg(\mathsf{A}\Box(\mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot)) \quad [3]$

$p : [\,0, \emptyset, \infty] \quad [4]$

$0: \ p\ \neg(\mathsf{A}\Box(\mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot)) \quad [5]$

$0: \ \neg(\mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot) \quad [6]$

$0: \ \neg(\mathsf{SNo} = 0) \quad [9]$

$0: \ \neg(\mathsf{SFile}(\mathsf{SNo}) \neq \bot) \quad [10]$

$\Box\ (2, 9)$

$0: \ \mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot \quad [7]$

$0: \ (p)\neg(\Box(\mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot)) \quad [8]$

$p : [\,0, \{\mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot\}, a, \emptyset, \infty] \quad [11]$

$a: \ \neg(\mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot) \quad [12]$

$a: \ \neg(\mathsf{SNo} = 0) \quad [13]$

$a: \ \neg(\mathsf{SFile}(\mathsf{SNo}) \neq \bot) \quad [14]$

Vorgängerknoten von a betrachten:

$p : [\,0, \circ, a, \emptyset, \infty] \quad [15]$

wie [16] mit 0 anstelle b und $0: \ \mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot \quad [7]$

$p : [\,0, \{\mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot\}, b, \circ, a, \emptyset, \infty] \quad [16]$

$b: \ \mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot \quad [17]$

$b: \ \mathsf{SNo} = 0 \quad [18]$

$\hookrightarrow$ S. 217

$b: \ \mathsf{SFile}(\mathsf{SNo}) \neq \bot \quad [19]$

$\hookrightarrow$ S. 218

$$\vdots$$

von [18] (S. 216):

$p : [\,0, \{\mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot\}, b, \circ, a, \emptyset, \infty]$ [16]

$a :\ \neg(\mathsf{SNo} = 0)$ [13]

$a :\ \neg(\mathsf{SFile}(\mathsf{SNo}) \neq \bot)$ [14]

$b :\ \mathsf{SNo} = 0$ [18]

aus SNo:

$b :\ \forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}(\mathsf{SNo} = N \ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})$ [20]

$b :\ \mathsf{SNo} = N_4 \rightarrow \mathsf{A}(\mathsf{SNo} = N_4 \ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})$ [21]

Linker Zweig:

$b :\ \neg(\mathsf{SNo} = N_4)$ [22]

$\Box\ \{N_4 \leftarrow 0\}(18, 22)$

Rechter Zweig:

$b :\ \mathsf{A}(\mathsf{SNo} = 0 \ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})$ [23]

$b :\ (\mathsf{A})(\mathsf{SNo} = 0 \ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})$ [24]

auf p:

$a :\ \mathsf{A}(\mathsf{SNo} = 0 \ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})$ [25]

$a :\ \mathsf{ProcAck} = \mathsf{true}$ [26]

aus PA1,2:

$b :\ \mathsf{SIM} = \mathsf{msg}(d_5, b_5)$ [30]

$b :\ \mathsf{SBit} = b_5$ [31]

$b :\ \mathsf{RQ} = q_5$ [32]

$b :\ \mathsf{SNo} = 0$ [33] (aus [18])

$a :\ \mathsf{SFile}(s(0)) \neq \bot$ [34]

$a :\ \mathsf{RQ} = q_5 | \mathsf{msg}(\mathsf{SFile}(s(0)), \mathsf{flip}(b_5))$ [35]

$a :\ \mathsf{SNo} = s(0)$ [36]

$a :\ \mathsf{SBit} = \mathsf{flip}(b_5)$ [37]

$a :\ \mathsf{ready} = \mathsf{false}$ [38]

$\Box :$	$a :\ \neg(\mathsf{SFile}(\mathsf{SNo}) \neq \bot)$ [14]
	$a :\ \mathsf{SNo} = s(0)$ [36]
	$a :\ \mathsf{SFile}(s(0)) \neq \bot$ [34]

$a :\ \mathsf{SFile}(s(0)) = \bot$ [39]

$a :\ \mathsf{RQ} = q_5$ [40]

$a :\ \mathsf{SNo} = 0$ [41]

$a :\ \mathsf{SBit} = b_5$ [42]

$a :\ \mathsf{ready} = \mathsf{true}$ [43]

$\Box\ (13, 41)$

$a :\ \mathsf{SNo} = 0$ [27]

$a :\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [28]

$a :\ (\mathsf{A})(\mathsf{SNo} = 0 \ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})$ [29]

$\Box\ (13, 27)$

$$\vdots$$

von [19] (S. 216):

$$p : [\,0, \{\mathsf{SNo} = 0 \lor \mathsf{SFile}(\mathsf{SNo}) \neq \bot\}, b, \circ, a, \emptyset, \infty] \quad [16]$$

$$a :\ \neg(\mathsf{SNo} = 0) \quad [13]$$

$$a :\ \neg(\mathsf{SFile}(\mathsf{SNo}) \neq \bot) \quad [14]$$

$$b :\ \mathsf{SFile}(\mathsf{SNo}) \neq \bot \quad [19]$$

$$|$$

aus EA:

$$b :\ \exists n : \mathsf{SNo} = N \quad [44]$$

$$b :\ \mathsf{SNo} = n_6 \quad [45]$$

$$b :\ \mathsf{SFile}(\mathsf{SNo}) = d_6 \quad [46]$$

$$|$$

aus SData:

$$b :\ \forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\Box(\mathsf{SFile}(N) = D) \quad [47]$$

$$b :\ \mathsf{SFile}(N_7) = D_7 \to \mathsf{A}\Box(\mathsf{SFile}(N_7) = D_7) \quad [48]$$

$$b :\ \neg(\mathsf{SFile}(N_7) = D_7) \quad [49]$$

$$\boxed{\begin{array}{ll} \Box : & b :\ \mathsf{SNo} = n_6 \quad [45] \\ & b :\ \mathsf{SFile}(\mathsf{SNo}) = d_6 \quad [46] \\ & \{N_7 \leftarrow n_6,\ D_7 \leftarrow d_6\} \end{array}}$$

$$b :\ \mathsf{A}\Box(\mathsf{SFile}(n_6) = d_6) \quad [50]$$

$$b :\ \mathsf{SFile}(n_6) = d_6 \quad [51]$$

$$b :\ (\mathsf{A})\Box(\mathsf{SFile}(n_6) = d_6) \quad [52]$$

auf p:

$$a :\ \mathsf{A}\Box(\mathsf{SFile}(n_6) = d_6) \quad [53]$$

$$|$$

$$a :\ \mathsf{SFile}(n_6) = d_6 \quad [54]$$

$$a :\ (\mathsf{A})\Box(\mathsf{SFile}(n_6) = d_6) \quad [55]$$

$$|$$

aus SNo:

$$b :\ \forall N : \mathsf{SNo} = N \to \mathsf{A}(\mathsf{SNo} = N \ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true}) \quad [56]$$

$$b :\ \mathsf{SNo} = N_8 \to \mathsf{A}(\mathsf{SNo} = N_8 \ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true}) \quad [57]$$

$$b :\ \neg(\mathsf{SNo} = N_8) \quad [58]$$

$$\Box\ \{N_8 \leftarrow n_6\}(45, 59)$$

$$b :\ \mathsf{A}(\mathsf{SNo} = n_6 \ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true}) \quad [60]$$

$$b :\ (\mathsf{A})(\mathsf{SNo} = n_6 \ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true}) \quad [61]$$

↪ S. 219

$\vdots$

von [61] (S. 218):

$p : [\,0, \{\mathsf{SNo} = 0 \vee \mathsf{SFile(SNo)} \neq \bot\}, b, \circ, a, \emptyset, \infty]$ [16]

$a:\ \neg(\mathsf{SFile(SNo)} \neq \bot)$ [14]

$b:\ \mathsf{SNo} = n_6$ [45]

$b:\ \mathsf{SFile(SNo)} = d_6$ [46]

$a:\ \mathsf{SFile}(n_6) = d_6$ [54]

$b:\ (\mathsf{A})(\mathsf{SNo} = n_6 \text{ unless } \mathsf{ProcAck} = \mathsf{true})$ [61]

auf p:

$a:\ \mathsf{A}(\mathsf{SNo} = n_6 \text{ unless } \mathsf{ProcAck} = \mathsf{true})$ [62]

Left branch:

$a:\ \mathsf{ProcAck} = \mathsf{true}$ [63]

aus PA1,2:

$b:\ \mathsf{SIM} = \mathsf{msg}(d_9, b_9)$ [67]

$b:\ \mathsf{SBit} = b_9$ [68]

$b:\ \mathsf{RQ} = q_9$ [69]

$b:\ \mathsf{SNo} = n_6$ [70] (aus [45])

Right branch:

$a:\ \mathsf{SNo} = n_6$ [64]

$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [65]

$a:\ (\mathsf{A})(\mathsf{SNo} = n_6 \text{ unless } \mathsf{ProcAck} = \mathsf{true})$ [66]

$\Box:$
$b:\ \mathsf{SFile(SNo)} \neq \bot$ [19]
$b:\ \mathsf{SNo} = n_6$ [45]
$b:\ \mathsf{SFile(SNo)} = d_6$ [46]
$b:\ \mathsf{SFile(SNo)} \neq \bot$ [19]
$\rightarrow\ d_6 \neq \bot$
$a:\ \mathsf{SNo} = n_6$ [64]
$a:\ \mathsf{SFile}(n_6) = d_6$ [54]
$a:\ \neg(\mathsf{SFile(SNo)} \neq \bot)$ [14]
$\rightarrow\ d_6 = \bot$

Branch from [70]:

$a:\ \mathsf{SFile}(s(n_6)) \neq \bot$ [71]

$a:\ \mathsf{RQ} = q_8 | \mathsf{msg}(\mathsf{SFile}(s(n_6)), \mathsf{flip}(b_9))$ [72]

$a:\ \mathsf{SNo} = s(n_6)$ [73]

$a:\ \mathsf{SBit} = \mathsf{flip}(b_9)$ [74]

$a:\ \mathsf{ready} = \mathsf{false}$ [75]

$\Box:$
$a:\ \mathsf{SFile}(s(n_6)) \neq \bot$ [71]
$a:\ \neg(\mathsf{SFile(SNo)} \neq \bot)$ [14]
$a:\ \mathsf{SNo} = s(n_6)$ [73]

$a:\ \mathsf{SFile}(s(n_6)) = \bot$ [76]

$a:\ \mathsf{RQ} = q_9$ [77]

$a:\ \mathsf{SNo} = n_6$ [78]

$a:\ \mathsf{SBit} = b_9$ [79]

$a:\ \mathsf{ready} = \mathsf{true}$ [80]

$\Box:$
$b:\ \mathsf{SNo} = n_6$ [45]
$b:\ \mathsf{SFile(SNo)} = d_6$ [46]
$b:\ \mathsf{SFile(SNo)} \neq \bot$ [19]
$\rightarrow\ d_6 \neq \bot$
$a:\ \mathsf{SNo} = n_6$ [78]
$a:\ \neg(\mathsf{SFile(SNo)} \neq \bot)$ [14]
$a:\ \mathsf{SFile}(n_6) = d_6$ [54]
$\rightarrow\ d_6 = \bot$

11 Korollar 2: Datenübertragung beendet

In Korollar 2 wird der Zustand der Evolving Algebra wenn $\mathsf{ready} = \mathsf{true}$ gilt, beschrieben:
Das zu übertragende File ist zu Ende, der Empfänger erwartet die nächste Nachricht (die es nicht gibt) und es sind nur noch Quittungen unterwegs, die den Sender nicht mehr interessieren.

$$\begin{aligned}\mathsf{A}\Box(\mathsf{ready} = \mathsf{true} \rightarrow (&\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \\ &(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge \\ &(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit})))\end{aligned}$$

Beweis: Induktion.

$$0: \ \mathsf{ready} = \mathsf{false} \quad [2]$$

$$\begin{aligned}0: \ \neg(\mathsf{A}\Box(\mathsf{ready} = \mathsf{true} \rightarrow (&\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \qquad [3] \\ &(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge \\ &(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))))\end{aligned}$$

$$p : [\,0, \emptyset, \infty] \quad [4]$$

$$\begin{aligned}0: \ p\,\neg(\Box(\mathsf{ready} = \mathsf{true} \rightarrow (&\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \qquad [5] \\ &(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge \\ &(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))))\end{aligned}$$

$$0: \ \neg(\mathsf{ready} = \mathsf{true} \rightarrow (\ldots)) \quad [6] \qquad\qquad 0: \ \mathsf{ready} = \mathsf{true} \rightarrow (\ldots) \quad [7]$$

$$0: \ \mathsf{ready} = \mathsf{true} \quad [9] \qquad\qquad 0: \ (p)\neg(\Box(\mathsf{ready} = \mathsf{true} \rightarrow (\ldots))) \quad [8]$$

$$\Box \ (2, 9)$$

$$\begin{aligned}p : [\,0, \{\mathsf{ready} = \mathsf{true} \rightarrow (&\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \qquad [11] \\ &(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge \\ &(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))\}, a, \emptyset, \infty]\end{aligned}$$

$$\begin{aligned}a: \ \neg(\mathsf{ready} = \mathsf{true} \rightarrow (&\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \qquad [12] \\ &(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge \\ &(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit})))\end{aligned}$$

$$a: \ \mathsf{ready} = \mathsf{true} \quad [13]$$

$$\begin{aligned}a: \ &\neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge \quad [14] \\ &(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))\end{aligned}$$

Vorgängerknoten von a betrachten:

$p : [\,0, \circ, a, \emptyset, \infty]$ [15] $\hookrightarrow$ S. 221

$\boxed{\text{wie [16] mit 0 anstelle } b.}$

$\vdots$

von [16] (S. 220):, (rechter Zweig)

$p : [\,0, \{\mathsf{ready} = \mathsf{true} \rightarrow (\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge (\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))\}, a, \emptyset, \infty]$ [11]

$a :$ $\mathsf{ready} = \mathsf{true}$ [13]

$a :$ $\neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge (\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$ [14]

(Vorgängerknoten)

$p : [\,0, \{\mathsf{ready} = \mathsf{true} \rightarrow (\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge (\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))\}, b, \circ, a, \emptyset, \infty]$ [16]

$b :$ $\mathsf{ready} = \mathsf{true} \rightarrow (\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge (\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$ [17]

Linker Zweig:

$b :$ $\neg(\mathsf{ready} = \mathsf{true})$ [18]

mit Bool:

$b :$ $\mathsf{ready} = \mathsf{false}$ [23]

aus ready:

$b :$ $\forall T : \mathsf{ready} = T \rightarrow \mathsf{A}(\mathsf{ready} = T\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [24]

$b :$ $\mathsf{ready} = T_1 \rightarrow \mathsf{A}(\mathsf{ready} = T_1\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [25]

$b :$ $\neg(\mathsf{ready} = T_1)$ [26]

$\square$ $\{T_1 \leftarrow \mathsf{false}\}(23, 26)$

$b :$ $\mathsf{A}(\mathsf{ready} = \mathsf{false}\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})$ [27]

$b :$ $(\mathsf{A})(\mathsf{ready} = \mathsf{false}\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})$ [28]

auf p:

$a :$ $\mathsf{A}(\mathsf{ready} = \mathsf{false}\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})$ [29]

$a :$ $\mathsf{ProcAck} = \mathsf{true}$ [30]

$\hookrightarrow$ S. 222

$a :$ $\mathsf{ready} = \mathsf{false}$ [31]

$a :$ $\neg(\mathsf{ProcAck} = \mathsf{true})$ [32]

$a :$ $\mathsf{A}(\mathsf{ready} = \mathsf{false}\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})$ [33]

$\square$ $(13, 31)$

Rechter Zweig von [17]:

$b :$ $\mathsf{SFile}(s(\mathsf{SNo})) = \bot$ [19]

$b :$ $\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})$ [20]

$b :$ $\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}$ [21]

$b :$ $\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}$ [22]

$\hookrightarrow$ S. 235

$\vdots$

von [30] (S. 221):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a :$ $\mathsf{ready} = \mathsf{true}$ [13]

$a :$ $\neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \to B = \mathsf{SBit}) \wedge$ [14]
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \to B' = \mathsf{SBit}))$

$a :$ $\mathsf{ProcAck} = \mathsf{true}$ [30]

aus PA2 in b:

$b :$ $\mathsf{SIM} = \mathsf{msg}(d_2, b_2)$ [34]

$b :$ $\mathsf{SBit} = b_2$ [35]

$b :$ $\mathsf{RQ} = q_2$ [36]

$b :$ $\mathsf{SNo} = n_2$ [37]

$a :$ $\mathsf{SFile}(s(n_2)) \neq \bot$ [38]

$a :$ $\mathsf{RQ} = q_2|\mathsf{msg}(\mathsf{SFile}(s(n_2)), \mathsf{flip}(b_2))$ [39]

$a :$ $\mathsf{SNo} = s(n_2)$ [40]

$a :$ $\mathsf{SBit} = \mathsf{flip}(b_2)$ [41]

$a :$ $\mathsf{ready} = \mathsf{false}$ [42]

$\Box$ $(13, 42)$

$a :$ $\mathsf{SFile}(s(n_2)) = \bot$ [43]

$a :$ $\mathsf{RQ} = q_2$ [44]

$a :$ $\mathsf{SNo} = n_2$ [45]

$a :$ $\mathsf{SBit} = b_2$ [46]

$a :$ $\mathsf{ready} = \mathsf{true}$ [47]

mit Lemma 2:

$b :$ $\forall B : ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B)|Q')) \to$ [48]
$(\mathsf{SBit} = B \to \mathsf{RBit} = \mathsf{flip}(B))$

$b :$ $((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_3)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_3)|Q')) \to$ [49]
$(\mathsf{SBit} = B_3 \to \mathsf{RBit} = \mathsf{flip}(B_3))$

$b :$ $\neg((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_3)) \vee$ [50]
$(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_3)|Q'))$

$b :$ $\neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_3))$ [52]

$b :$ $\neg(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_3)|Q')$ [53]

$b :$ $\neg(\mathsf{SIM} = \mathsf{msg}(D_3, B_3))$ [54]

$\Box\{D_3 \leftarrow d_2,\ B_3 \leftarrow b_2\}(34, 54)$

$b :$ $\mathsf{SBit} = b_2 \to \mathsf{RBit} = \mathsf{flip}(b_2)$ [51]

$b :$ $\neg(\mathsf{SBit} = b_2)$ [55]

$\Box$ $(35, 55)$

$b :$ $\mathsf{RBit} = \mathsf{flip}(b_2)$ [56]

$\hookrightarrow$ S. 223

$$\vdots$$

von [56] (S. 222):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a:$ $\mathsf{ready} = \mathsf{true}$ [13]

$a:$ $\neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D,B) \rightarrow B = \mathsf{SBit}) \wedge$ [14]
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$

$b:$ $\mathsf{SIM} = \mathsf{msg}(d_2, b_2)$ [34]
$b:$ $\mathsf{SBit} = b_2$ [35]
$b:$ $\mathsf{SNo} = n_2$ [37]
$a:$ $\mathsf{SFile}(s(n_2)) = \bot$ [43]
$a:$ $\mathsf{SNo} = n_2$ [45]
$a:$ $\mathsf{SBit} = b_2$ [46]
$b:$ $\mathsf{RBit} = \mathsf{flip}(b_2)$ [56]

mit Lemma 1, Teil 1:

$b:$ $\forall B : (\exists D : \mathsf{SIM} = \mathsf{msg}(D,B)) \rightarrow (B = \mathsf{SBit} \rightarrow ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B)|Q^1)) \wedge$ [57]
$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B)|Q^3))))$

$b:$ $(\exists D : \mathsf{SIM} = \mathsf{msg}(D,B_4)) \rightarrow (B_4 = \mathsf{SBit} \rightarrow ((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, B_4)|Q^1)) \wedge$ [58]
$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, B_4)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, B_4)|Q^3))))$

$b:$ $\neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_4))$ [59]
$b:$ $\neg(\mathsf{SIM} = \mathsf{msg}(D_4, B_4))$ [61]
$\square\ \{D_4 \leftarrow d_2,\ B_4 \leftarrow b_2\}(34, 61)$

$b:$ $(b_2 = \mathsf{SBit} \rightarrow$ [60]
$((\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_2)|Q^1)) \wedge$
$(\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_2)) \wedge$
$(\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_2)|Q^3))))$

$b:$ $\neg(b_2 = \mathsf{SBit})$ [62]
$\square\ (35, 62)$

$b:$ $\mathsf{SQ} = \varepsilon \vee (\exists D^1, Q^1 : \mathsf{SQ} = \mathsf{msg}(D^1, b_2)|Q^1)$ [63]
$b:$ $\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_2)$ [64]
$b:$ $\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_2)|Q^3)$ [65]

aus [14]:

$a:$ $\neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot)$ [66]

$\square:$	$a:$ $\mathsf{SFile}(s(n_2)) = \bot$ [43]
	$a:$ $\mathsf{SNo} = n_2$ [45]

$a:$ $\neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge$ [67]
$(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D,B) \rightarrow B = \mathsf{SBit}) \wedge$
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$

$\hookrightarrow$ S. 224

$\vdots$

von [67] (S. 223):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

a : $\mathsf{ready} = \mathsf{true}$ [13]

b : $\mathsf{SBit} = b_2$ [35]

b : $\mathsf{SNo} = n_2$ [37]

a : $\mathsf{SBit} = b_2$ [46]

b : $\mathsf{RBit} = \mathsf{flip}(b_2)$ [56]

b : $\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_2)$ [64]

b : $\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_2)|Q^3)$ [65]

a : $\neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge$ [67]
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$

aus RBit:

b : $\forall B : \mathsf{RBit} = B \rightarrow \mathsf{A}(\mathsf{RBit} = B \text{ unless}^+ \mathsf{AccDat} = \mathsf{true})$ [68]

b : $\mathsf{RBit} = B_5 \rightarrow \mathsf{A}(\mathsf{RBit} = B_5 \text{ unless}^+ \mathsf{AccDat} = \mathsf{true})$ [69]

b : $\neg(\mathsf{RBit} = B_5)$ [70]
$\Box\ \{B_5 \leftarrow \mathsf{flip}(b_2)\}(56, 70)$

b : $\mathsf{A}(\mathsf{RBit} = \mathsf{flip}(b_2) \text{ unless}^+ \mathsf{AccDat} = \mathsf{true})$ [71]
b : $(\mathsf{A})(\mathsf{RBit} = \mathsf{flip}(b_2) \text{ unless } \mathsf{AccDat} = \mathsf{true})$ [72]

auf p:

a : $\mathsf{A}(\mathsf{RBit} = \mathsf{flip}(b_2) \text{ unless } \mathsf{AccDat} = \mathsf{true})$ [73]

a : $\mathsf{AccDat} = \mathsf{true}$ [74]
aus AD1:
b : $\mathsf{RIM} = \mathsf{msg}(d_6, b_6)$ [78]
b : $\mathsf{RBit} = b_6$ [79]

a : $\mathsf{RBit} = \mathsf{flip}(b_2)$ [75]
a : $\neg(\mathsf{AccDat} = \mathsf{true})$ [76]
a : $\mathsf{A}(\mathsf{ready} = \mathsf{false} \text{ unless } \mathsf{AccDat} = \mathsf{true})$ [77]
$\hookrightarrow$ S. 225

aus [64]:

b : $\mathsf{RIM} = \bot$ [80]
$\Box$ (E3, 78, 80)

b : $\exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_2)$ [81]
b : $\mathsf{RIM} = \mathsf{msg}(d_6^2, b_2)$ [82]

$$\boxed{\begin{array}{ll} \Box : & b : \mathsf{RIM} = \mathsf{msg}(d_6^2, b_2) \quad [82] \\ & b : \mathsf{RIM} = \mathsf{msg}(d_6, b_6) \quad [78] \\ \hline & \rightarrow\ b_2 = b_6 \\ & b : \mathsf{RBit} = \mathsf{flip}(b_2) \quad [56] \\ & b : \mathsf{RBit} = b_6 \quad [79] \\ \hline & \rightarrow\ \mathsf{flip}(b_2) = b_6 \end{array}}$$

$\vdots$

von [77] (S. 224):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a :$ $\mathsf{ready} = \mathsf{true}$ [13]

$b :$ $\mathsf{SBit} = b_2$ [35]

$b :$ $\mathsf{SNo} = n_2$ [37]

$a :$ $\mathsf{SBit} = b_2$ [46]

$b :$ $\mathsf{RBit} = \mathsf{flip}(b_2)$ [56]

$b :$ $\mathsf{RIM} = \bot \vee \exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_2)$ [64]

$b :$ $\mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_2)|Q^3)$ [65]

$a :$ $\neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge$ [67]
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$

$a :$ $\mathsf{RBit} = \mathsf{flip}(b_2)$ [75]

aus [67]:

$a :$ $\neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}))$ [83]

$\square :$ $a :$ $\mathsf{SBit} = b_2$ [46]
$a :$ $\mathsf{RBit} = \mathsf{flip}(b_2)$ [75]

$a :$ $\neg((\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge$ [84]
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$

$a :$ $\neg(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit})$ [85]

$a :$ $\neg(\mathsf{RIM} = \mathsf{msg}(d_8, b_8) \rightarrow b_8 = \mathsf{SBit})$ [87]

$a :$ $\mathsf{RIM} = \mathsf{msg}(d_8, b_8)$ [88]

$a :$ $\neg(b_8 = \mathsf{SBit})$ [89]

$a :$ $\neg(\forall D', B', Q, Q' :$ [86]
$\mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit})$

$a :$ $\neg(\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8 \rightarrow b'_8 = \mathsf{SBit})$ [129]

$a :$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a :$ $\neg(b'_8 = \mathsf{SBit})$ [131]

$\hookrightarrow$ S. 228

aus [64]:

$b :$ $\mathsf{RIM} = \bot$ [90]

aus RIM:

$b :$ $\forall M : \mathsf{RIM} = M \rightarrow \mathsf{A}(\mathsf{RIM} = M \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [92]

$b :$ $\mathsf{RIM} = M_8 \rightarrow \mathsf{A}(\mathsf{RIM} = M_8 \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [93]

$b :$ $\neg(\mathsf{RIM} = M_8)$ [94]

$\square$ $\{M_8 \leftarrow \bot\}(90, 94)$

$b :$ $\mathsf{A}(\mathsf{RIM} = \bot \ \mathsf{unless}^+$ [95]
$\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$

$\hookrightarrow$ S. 226

$b :$ $\exists D^2 : \mathsf{RIM} = \mathsf{msg}(D^2, b_2)$ [91]

$b :$ $\mathsf{RIM} = \mathsf{msg}(d^2_{11}, b_2)$ [112]

$\hookrightarrow$ S. 227

$\vdots$

von [95] (S. 225):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a :\ \mathsf{SBit} = b_2$ [46]

$b :\ \mathsf{RQ} = \varepsilon \vee (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_2)|Q^3)$ [65]

$a :\ \mathsf{RIM} = \mathsf{msg}(d_8, b_8)$ [88]

$a :\ \neg(b_8 = \mathsf{SBit})$ [89]

$b :\ \mathsf{RIM} = \bot$ [90]

$b :\ \mathsf{A}(\mathsf{RIM} = \bot\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [95]

$b :\ (\mathsf{A})(\mathsf{RIM} = \bot\ \mathsf{unless}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [96]

auf p:

$a :\ \mathsf{A}(\mathsf{RIM} = \bot\ \mathsf{unless}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [97]

$a :\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [98]

$a :\ \mathsf{RIM} = \bot$ [99]

$a :\ \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [100]

$a :\ \mathsf{A}(\mathsf{RIM} = \bot\ \mathsf{unless}$ [101]

$\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$

$\square\ (99, 88)$

$a :\ \mathsf{RecCom} = \mathsf{true}$ [102]

aus RC2 in b:

$b :\ \mathsf{RQ} = \mathsf{msg}(d_1, b_1)|q_1$ [104]

$a :\ \mathsf{RQ} = q_1$ [105]

$a :\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [106]

$a :\ \mathsf{AckMsg} = \mathsf{true}$ [103]

aus AM1 in b:

$b :\ \mathsf{RIM} = \mathsf{msg}(d_{10}, b_{10})$ [110]

$b :\ \mathsf{RBit} = \mathsf{flip}(b_{10})$ [111]

$\square\ (\mathrm{E3}, 90, 110)$

aus [65]:

$b :\ \mathsf{RQ} = \varepsilon$ [107]

$\square\ (\mathrm{E2}, 104, 107)$

$b :\ \exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_2)|Q^3$ [108]

$b :\ \mathsf{RQ} = \mathsf{msg}(d_9^3, b_2)|q_9^3$ [104]

$\square :$

$b :\ \mathsf{RQ} = \mathsf{msg}(d_1, b_1)|q_1$ [109]

$b :\ \mathsf{RQ} = \mathsf{msg}(d_9^3, b_2)|q_9^3$ [109]

$\rightarrow\ b_1 = b_2$

$a :\ \mathsf{RIM} = \mathsf{msg}(d_1, b_1)$ [106]

$a :\ \mathsf{RIM} = \mathsf{msg}(d_8, b_8)$ [88]

$\rightarrow\ b_1 = b_8$

$a :\ \mathsf{SBit} = b_2$ [46]

$a :\ \neg(b_8 = \mathsf{SBit})$ [89]

$\rightarrow\ b_2 \neq b_8$

$\vdots$

von [112] (S. 225):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a:$ $\mathsf{SBit} = b_2$ [46]

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_8, b_8)$ [88]

$a:$ $\neg(b_8 = \mathsf{SBit})$ [89]

$b:$ $\mathsf{RIM} = \mathsf{msg}(d_{11}^2, b_2)$ [112]

aus RIM:

$b:$ $\forall M : \mathsf{RIM} = M \rightarrow \mathsf{A}(\mathsf{RIM} = M \ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [113]

$b:$ $\mathsf{RIM} = M_8 \rightarrow \mathsf{A}(\mathsf{RIM} = M_8 \ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [114]

$b:$ $\neg(\mathsf{RIM} = M_8)$ [115]

$\Box$ $\{M_8 \leftarrow \mathsf{msg}(d_{11}^2, b_2)\}(112, 115)$

$b:$ $\mathsf{A}(\mathsf{RIM} = \mathsf{msg}(d_{11}^2, b_2)\ \mathsf{unless}^+$ [116]
$\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$

$b:$ $(\mathsf{A})(\mathsf{RIM} = \mathsf{msg}(d_{11}^2, b_2)\ \mathsf{unless}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [117]

auf p:

$a:$ $\mathsf{A}(\mathsf{RIM} = \mathsf{msg}(d_{11}^2, b_2)\ \mathsf{unless}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [118]

$a:$ $\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [119]

$a:$ $\mathsf{RecCom} = \mathsf{true}$ [123]

aus RC1 in b:

$b:$ $\mathsf{RIM} = \bot$ [125]

$b:$ $\mathsf{RQ} = \mathsf{msg}(d_1, b_1)|q_1$ [126]

$\Box$ $(\mathrm{E3}, 112, 125)$

$a:$ $\mathsf{AckMsg} = \mathsf{true}$ [124]

aus AM1,AM2 in b:

$a:$ $\mathsf{RIM} = \bot$ [127]

$\Box$ $(\mathrm{E3}, 88, 127)$

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_{11}^2, b_2)$ [120]

$a:$ $\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [121]

$a:$ $\mathsf{A}(\mathsf{RIM} = \mathsf{msg}(d_{11}^2, b_2)\ \mathsf{unless}$ [122]
$\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$

$\Box$:

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_8, b_8)$ [88]

$a:$ $\mathsf{RIM} = \mathsf{msg}(d_{11}^2, b_2)$ [120]

$\rightarrow$ $b_8 = b_2$

$a:$ $\mathsf{SBit} = b_2$ [46]

$a:$ $\neg(b_8 = \mathsf{SBit})$ [89]

$\rightarrow$ $b_2 \neq b_8$

$\vdots$

von [131] (S. 225):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a :$ $\mathsf{ready} = \mathsf{true}$ [13]

$b :$ $\mathsf{SBit} = b_2$ [35]

$b :$ $\mathsf{SNo} = n_2$ [37]

$a :$ $\mathsf{SBit} = b_2$ [46]

$b :$ $\mathsf{RQ} = \varepsilon \lor (\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_2)|Q^3)$ [65]

$a :$ $\mathsf{RQ} = q_8|\mathsf{msg}(d_8', b_8')|q_8'$ [130]

$a :$ $\neg(b_8' = \mathsf{SBit})$ [131]

Die Kombination [36] und [44], die zu einem sofortigen Abschluß des Astes führen würde, wird hier absichtlich nicht verwendet, da sie implizit die Parallelität stärker als notwendig einschränkt und außerdem einer Wiederverwendung des Beweises im Wege steht. Aus dem letzgenannten Grund wird [30] ebenfalls nicht verwendet.

aus [65]:

$b :$ $\mathsf{RQ} = \varepsilon$ [132]

$b :$ $\exists D^3, Q^3 : \mathsf{RQ} = \mathsf{msg}(D^3, b_2)|Q^3$ [133]

$b :$ $\mathsf{RQ} = \mathsf{msg}(d_{14}^3, b_2)|q_{14}^3$ [169]

$\hookrightarrow$ S. 230

aus RQ:

$b :$ $\forall Q : \mathsf{RQ} = Q \to \mathsf{A}(\mathsf{RQ} = Q\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [134]

$b :$ $\mathsf{RQ} = Q_{12} \to \mathsf{A}(\mathsf{RQ} = Q_{12}\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [135]

$b :$ $\neg(\mathsf{RQ} = Q_{12})$ [136]

$\square$ $\{\mathsf{RQ} \leftarrow \varepsilon\}(132, 136)$

$b :$ $\mathsf{A}(\mathsf{RQ} = \varepsilon\ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [137]

$b :$ $(\mathsf{A})(\mathsf{RQ} = \varepsilon\ \mathsf{unless}\ \mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [138]

auf p:

$a :$ $\mathsf{A}(\mathsf{RQ} = \varepsilon\ \mathsf{unless}\ \mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [139]

$a :$ $\mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true}$ [140]

$\hookrightarrow$ S. 229

$a :$ $\mathsf{RQ} = \varepsilon$ [141]

$a :$ $\neg(\mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [142]

$a :$ $(\mathsf{A})(\mathsf{RQ} = \varepsilon\ \mathsf{unless}\ (\ldots))$ [143]

$\square$ $(\mathrm{E2}, 130, 141)$

$\vdots$

von [140] (S. 228):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a:$ $\mathsf{ready} = \mathsf{true}$ [13]

$b:$ $\mathsf{SBit} = b_2$ [35]

$b:$ $\mathsf{SNo} = n_2$ [37]

$a:$ $\mathsf{SBit} = b_2$ [46]

$a:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a:$ $\neg(b'_8 = \mathsf{SBit})$ [131]

$b:$ $\mathsf{RQ} = \varepsilon$ [132]

$a:$ $\mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}$ [140]

$a:$ $\mathsf{RecCom} = \mathsf{true}$ [144]

aus RC1 in b:

$b:$ $\mathsf{RIM} = \bot$ [147]

$b:$ $\mathsf{RQ} = \mathsf{msg}(d_{13}, b_{13})|q_{13}$ [148]

$\Box$ (E2, 132, 148)

$a:$ $\mathsf{RLose} = \mathsf{true}$ [145]

aus RL1 in b:

$b:$ $\mathsf{RQ} \neq \varepsilon$ [149]

$\Box$ (E2, 132, 149)

$a:$ $\mathsf{ReTrans} = \mathsf{true} \vee$ [146]
$\mathsf{ProcAck} = \mathsf{true}$

$a:$ $\mathsf{ReTrans} = \mathsf{true}$ [150]

aus RT2 in b:

$b:$ $\mathsf{RQ} = \varepsilon$ [152] (aus [132])

$b:$ $\mathsf{SNo} = n_2$ [153] (aus [37])

$b:$ $\mathsf{SBit} = b_2$ [154] (aus [35])

$a:$ $\mathsf{RQ} = \mathsf{msg}(\mathsf{SFile}(n_2), b_2)$ [155]

$\Box$:	$a:$ $\mathsf{RQ} = q_8\|\mathsf{msg}(d'_8, b'_8)\|q'_8$ [130]
	$a:$ $\mathsf{RQ} = \mathsf{msg}(\mathsf{SFile}(n_2), b_2)$ [155]
	$\rightarrow b_2 = b'_8$
	$a:$ $\mathsf{SBit} = b_2$ [46]
	$a:$ $\neg(b'_8 = \mathsf{SBit})$ [131]
	$\rightarrow b_2 \neq b'_8$

$a:$ $\mathsf{ProcAck} = \mathsf{true}$ [151]

aus PA2 in b:

$b:$ $\mathsf{RQ} = \varepsilon$ [156] (aus [132])

$b:$ $\mathsf{SNo} = n_2$ [157] (aus [37])

$b:$ $\mathsf{SBit} = b_2$ [158] (aus [35])

$a:$ $\mathsf{SFile}(s(n_2)) = \bot$ [164]

$a:$ $\mathsf{RQ} = \varepsilon$ [165]

$a:$ $\mathsf{SNo} = n_2$ [166]

$a:$ $\mathsf{SBit} = b_2$ [167]

$a:$ $\mathsf{ready} = \mathsf{true}$ [168]

$\Box$ (E2, 130, 168)

$a:$ $\mathsf{SFile}(s(n_2)) \neq \bot$ [159]

$a:$ $\mathsf{RQ} = \mathsf{msg}(\mathsf{SFile}(s(n_2)), \mathsf{flip}(b_2))$ [160]

$a:$ $\mathsf{SNo} = s(n_2)$ [161]

$a:$ $\mathsf{SBit} = \mathsf{flip}(b_2)$ [162]

$a:$ $\mathsf{ready} = \mathsf{false}$ [163]

$\Box$ (13, 163)

$\vdots$

von [169] (S. 228):

$p : [0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a :$ $\mathsf{ready} = \mathsf{true}$ [13]

$b :$ $\mathsf{SBit} = b_2$ [35]

$b :$ $\mathsf{SNo} = n_2$ [37]

$a :$ $\mathsf{SBit} = b_2$ [46]

$a :$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a :$ $\neg(b'_8 = \mathsf{SBit})$ [131]

$b :$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [169]

aus Lemma 1, A10:

$b :$ $\forall B : (\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \rightarrow$ [170]
$(B = \mathsf{SBit} \rightarrow (\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit}))$

$b :$ $(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{15})|Q) \rightarrow$ [171]
$(B_{15} = \mathsf{SBit} \rightarrow (\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit}))$

$b :$ $\neg(\exists D, Q : \mathsf{SQ} = \mathsf{msg}(D, B_{15})|Q)$ [172]

$b :$ $\neg(\mathsf{SQ} = \mathsf{msg}(D_{15}, B_{15})|Q_{15})$ [174]

$\Box$ $\{D_15 \leftarrow d^3_{14},\ B_{15} \leftarrow b_2,\ Q_{15} \leftarrow q^3_{14}\}(169, 174)$

$b :$ $B_{15} = \mathsf{SBit} \rightarrow (\ldots)$ [173]

$b :$ $\neg(b_2 = \mathsf{SBit})$ [175]

$\Box$ $(35, 175)$

$b :$ $\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \rightarrow B' = \mathsf{SBit}$ [176]

aus RQ:

$b :$ $\forall Q : \mathsf{RQ} = Q \rightarrow \mathsf{A}(\mathsf{RQ} = Q\ \mathsf{unless}^{+}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee$ [177]
$\mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$

$b :$ $\mathsf{RQ} = Q_{16} \rightarrow \mathsf{A}(\mathsf{RQ} = Q_{16}\ \mathsf{unless}^{+}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee$ [178]
$\mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$

$b :$ $\neg(\mathsf{RQ} = Q_{16})$ [179]

$\Box$ $\{Q_{16} \leftarrow \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}\}(169, 179)$

$b :$ $\mathsf{A}(\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}\ \mathsf{unless}^{+}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee$ [180]
$\mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$

$\hookrightarrow$ S. 231

$\vdots$

von [180] (S. 230):

$p : [0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a :$ $\mathsf{ready} = \mathsf{true}$ [13]

$b :$ $\mathsf{SBit} = b_2$ [35]

$b :$ $\mathsf{SNo} = n_2$ [37]

$a :$ $\mathsf{SBit} = b_2$ [46]

$a :$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a :$ $\neg(b'_8 = \mathsf{SBit})$ [131]

$b :$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [169]

$b :$ $\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \to B' = \mathsf{SBit}$ [176]

$|$

$b :$ $\mathsf{A}(\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ unless^+ $\mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor$ $\mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [180]

$|$

$b :$ $(\mathsf{A})(\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ unless $\mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor$ $\mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [181]

auf p:

$a :$ $\mathsf{A}(\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ unless $\mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor$ $\mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [182]

$a :$ $\mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor$ $\mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true}$ [183]

$\hookrightarrow$ S. 232

$a :$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [184]

$a :$ $\neg(\mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor$ $\mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true})$ [185]

$a :$ $(\mathsf{A})(\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ unless $(\ldots))$ [186]

$|$

aus [176]:

$b :$ $\mathsf{SQ} = Q'_{19}|\mathsf{msg}(D'_{19}, B'_{19})|Q''_{19} \to B'_{19} = \mathsf{SBit}$ [221]

$b :$ $\neg(\mathsf{SQ} = Q'_{19}|\mathsf{msg}(D'_{19}, B'_{19})|Q''_{19})$ [222]

$\Box :$ $a :$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [184]
$a :$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]
$b :$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [169]

$b :$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$
$\{Q'_{19} \leftarrow q_8,\ D'_{19} \leftarrow d'_8,$
$B'_{19} \leftarrow b_8,\ Q''_{19} \leftarrow q'_8\}$

$b :$ $b'_8 = \mathsf{SBit}$ [223]

$\Box :$ $b :$ $\mathsf{SBit} = b_2$ [35]
$b :$ $b'_8 = \mathsf{SBit}$ [223]

$\to$ $b_2 = b'_8$

$a :$ $\mathsf{SBit} = b_2$ [46]
$a :$ $\neg(b'_8 = \mathsf{SBit})$ [131]

$\to$ $b_2 \neq b'_8$

$\vdots$

von [183] (S. 231):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a:$ $\mathsf{ready} = \mathsf{true}$ [13]

$b:$ $\mathsf{SBit} = b_2$ [35]

$b:$ $\mathsf{SNo} = n_2$ [37]

$a:$ $\mathsf{SBit} = b_2$ [46]

$a:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a:$ $\neg(b'_8 = \mathsf{SBit})$ [131]

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [169]

$b:$ $\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \to B' = \mathsf{SBit}$ [176]

$a:$ $\mathsf{RecCom} = \mathsf{true} \lor \mathsf{RLose} = \mathsf{true} \lor \mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true}$ [183]

$a:$ $\mathsf{RecCom} = \mathsf{true}$ [187]

aus RC2 in b:

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [190]

(aus [169])

$a:$ $\mathsf{RQ} = q^3_{14}$ [191]

$a:$ $\mathsf{RIM} = \mathsf{msg}(d^3_{14}, b_2)$ [192]

wie [184]: die betreffende Nachricht war in b schon in RQ enthalten:

$a:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a:$ $\mathsf{RQ} = q^3_{14}$ [191]

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [190]

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q_8|$
$|\mathsf{msg}(d'_8, b'_8)|q'_8$

$a:$ $\mathsf{RLose} = \mathsf{true}$ [188]

aus RL2 in b:

$a:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [193]

(aus [130])

$b:$ $\mathsf{RQ} = r_8|\mathsf{msg}(d'_8, b'_8)|r'_8$ [194]

wie [184]: die betreffende Nachricht war in b schon in RQ enthalten:

$b:$ $\mathsf{RQ} = r_8|\mathsf{msg}(d'_8, b'_8)|r'_8$ [194]

$a:$ $\mathsf{ReTrans} = \mathsf{true} \lor \mathsf{ProcAck} = \mathsf{true}$ [189]

$a:$ $\mathsf{ReTrans} = \mathsf{true}$ [195]

$\hookrightarrow$ S. 233

$a:$ $\mathsf{ProcAck} = \mathsf{true}$ [196]

$\hookrightarrow$ S. 234

$\vdots$

von [195] (S. 232):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$b:$ $\mathsf{SBit} = b_2$ [35]

$b:$ $\mathsf{SNo} = n_2$ [37]

$a:$ $\mathsf{SBit} = b_2$ [46]

$a:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a:$ $\neg(b'_8 = \mathsf{SBit})$ [131]

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [169]

$b:$ $\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \to B' = \mathsf{SBit}$ [176]

$a:$ $\mathsf{ReTrans} = \mathsf{true}$ [195]

aus RT2 in b:

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [197] (aus [169])

$b:$ $\mathsf{SNo} = n_2$ [198] (aus [37])

$b:$ $\mathsf{SBit} = b_2$ [199] (aus [35])

$a:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}|\mathsf{msg}(\mathsf{SFile}(n_2), b_2)$ [200]

mit Q2:

$a:$ $\forall Q, Q' : (\exists D, B : Q = \mathsf{msg}(D, B)|Q') \to Q' = \varepsilon \vee (\exists D', B', Q'' : Q' = Q''|\mathsf{msg}(D', B'))$ [201]

$a:$ $(\exists D, B : Q_{17} = \mathsf{msg}(D, B))|Q'_{17} \to Q'_{17} = \varepsilon \vee (\exists D', B', Q'' : Q'_{17} = Q''|\mathsf{msg}(D', B'))$ [202]

$a:$ $\neg(\exists D, B : Q_{17} = \mathsf{msg}(D, B)|Q'_{17}$ [203]

$\square$ $\{Q_{17} \leftarrow \mathsf{msg}(d'_8, b'_8)|q'_8,\ Q'_{17} \leftarrow q'_8\}(130, 203)$

$a:$ $q'_8 = \varepsilon \vee (\exists D', B', Q'' : q'_8 = Q''|\mathsf{msg}(D', B'))$ [204]

$a:$ $q'_8 = \varepsilon$ [205]

$\square:$ $a:$ $q'_8 = \varepsilon$ [205]

$a:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|$ [200]

$|q^3_{14}|\mathsf{msg}(\mathsf{SFile}(n_2), b_2)$

$\to$ $b'_8 = b_2$

$a:$ $\mathsf{SBit} = b_2$ [46]

$a:$ $\neg(b'_8 = \mathsf{SBit})$ [131]

$\to$ $b_2 \neq b'_8$

$a:$ $\exists D', B', Q'' : q'_8 = Q''|\mathsf{msg}(D', B')$ [206]

$a:$ $q'_8 = q''_{18}|\mathsf{msg}(d'_{18}, b'_{18})$ [207]

wie [184]: die betreffende Nachricht war in b schon in RQ enthalten:

$a:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a:$ $q'_8 = q''_{18}|\mathsf{msg}(d'_{18}, b'_{18})$ [207]

$a:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}|$ [200]

$|\mathsf{msg}(\mathsf{SFile}(n_2), b_2)$

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [197]

$\to b:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q''_{18}$

$\vdots$

von [196] (S. 232):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a:$ $\mathsf{ready} = \mathsf{true}$ [13]

$b:$ $\mathsf{SBit} = b_2$ [35]

$b:$ $\mathsf{SNo} = n_2$ [37]

$a:$ $\mathsf{SBit} = b_2$ [46]

$a:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a:$ $\neg(b'_8 = \mathsf{SBit})$ [131]

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [169]

$b:$ $\forall Q', Q'', D', B' : \mathsf{SQ} = Q'|\mathsf{msg}(D', B')|Q'' \to B' = \mathsf{SBit}$ [176]

$a:$ $\mathsf{ProcAck} = \mathsf{true}$ [196]

|

aus PA2 in b:

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [208] (aus [169])

$b:$ $\mathsf{SNo} = n_2$ [209] (aus [37])

$b:$ $\mathsf{SBit} = b_2$ [210] (aus [35])

$a:$ $\mathsf{SFile}(s(n_2)) \neq \bot$ [211]

$a:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}|$ [212]
$|\mathsf{msg}(\mathsf{SFile}(s(n_2)), \mathsf{flip}(b_2))$

$a:$ $\mathsf{SNo} = s(n_2)$ [213]

$a:$ $\mathsf{SBit} = \mathsf{flip}(b_2)$ [214]

$a:$ $\mathsf{ready} = \mathsf{false}$ [215]

$\Box$ (13, 215)

$a:$ $\mathsf{SFile}(s(n_2)) = \bot$ [216]

$a:$ $\mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [217]

$a:$ $\mathsf{SNo} = n_2$ [218]

$a:$ $\mathsf{SBit} = b_2$ [219]

$a:$ $\mathsf{ready} = \mathsf{true}$ [220]

wie [184]: die betreffende Nachricht war in b schon in RQ enthalten:

$a:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$ [130]

$a:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [217]

$b:$ $\mathsf{RQ} = \mathsf{msg}(d^3_{14}, b_2)|q^3_{14}$ [208]

$b:$ $\mathsf{RQ} = q_8|\mathsf{msg}(d'_8, b'_8)|q'_8$

$$\vdots$$

von [22] (S. 221):

$$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]\quad[16]$$

$$a:\ \mathsf{ready} = \mathsf{true}\quad[13]$$

$$|$$

$$a:\ \neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D,B) \rightarrow B = \mathsf{SBit}) \wedge \quad [14]$$
$$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D',B')|Q' \rightarrow B' = \mathsf{SBit}))$$

$$|$$

$$b:\ \mathsf{SFile}(s(\mathsf{SNo})) = \bot\quad[19]$$
$$b:\ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})\quad[20]$$
$$b:\ \forall D, B : \mathsf{RIM} = \mathsf{msg}(D,B) \rightarrow B = \mathsf{SBit}\quad[21]$$
$$b:\ \forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D',B')|Q' \rightarrow B' = \mathsf{SBit}\quad[22]$$

$$|$$

aus EA:

$$b:\ \exists n : \mathsf{SNo} = N\quad[224]$$
$$b:\ \mathsf{SNo} = n_{20}\quad[225]$$
$$b:\ \exists n : \mathsf{SBit} = B\quad[226]$$
$$b:\ \mathsf{SBit} = b_{20}\quad[227]$$

$$|$$

aus SData: $b:\ \forall D, N : \mathsf{SFile}(N) = D \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N) = D)$ [228]

$$b:\ \mathsf{SFile}(N_{21}) = D_{21} \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N_{21}) = D_{21})\quad[229]$$

Linker Zweig:

$$b:\ \neg(\mathsf{SFile}(N_{21}) = D_{21})\quad[230]$$

$$\boxed{\begin{array}{ll} \Box : & b:\ \mathsf{SFile}(s(\mathsf{SNo})) = \bot\quad[19] \\ & b:\ \mathsf{SNo} = n_{20}\quad[225] \\ & \{N_{21} \leftarrow s(n_{20}),\ D_{21} \leftarrow \bot\} \end{array}}$$

Rechter Zweig:

$$b:\ \mathsf{A}\Box(\mathsf{SFile}(s(n_{20})) = \bot)\quad[231]$$
$$b:\ \mathsf{SFile}(s(n_{20})) = \bot)\quad[232]$$
$$b:\ (\mathsf{A})\Box(\mathsf{SFile}(s(n_{20})) = \bot)\quad[233]$$

auf p:

$$a:\ \mathsf{A}\Box(\mathsf{SFile}(s(n_{20})) = \bot)\quad[234]$$

$$|$$

$$a:\ \mathsf{SFile}(s(n_{20})) = \bot\quad[235]$$
$$a:\ (\mathsf{A})\Box(\mathsf{SFile}(s(n_{20})) = \bot)\quad[236]$$

$$|$$

aus SNo:

$$b:\ \forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}(\mathsf{SNo} = N\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})\quad[237]$$
$$b:\ \mathsf{SNo} = N_{22} \rightarrow \mathsf{A}(\mathsf{SNo} = N_{22}\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})\quad[238]$$

Linker Zweig:

$$b:\ \neg(\mathsf{SNo} = N_{22})\quad[239]$$
$$\Box\ \{N_{22} \leftarrow n_{20}\}(225, 239)$$

Rechter Zweig:

$$b:\ \mathsf{A}(\mathsf{SNo} = n_{20}\ \mathsf{unless}^+\ \mathsf{ProcAck} = \mathsf{true})\quad[240]$$
$$b:\ (\mathsf{A})(\mathsf{SNo} = n_{20}\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})\quad[241]$$

$\hookrightarrow$ S. 236

$\vdots$

von [241] (S. 235):

$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]

$a:$ $\mathsf{ready} = \mathsf{true}$ [13]

|

$a:$ $\neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \to B = \mathsf{SBit}) \wedge$ [14]
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \to B' = \mathsf{SBit}))$

|

$b:$ $\mathsf{SFile}(s(\mathsf{SNo})) = \bot$ [19]

$b:$ $\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})$ [20]

$b:$ $\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \to B = \mathsf{SBit}$ [21]

$b:$ $\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \to B' = \mathsf{SBit}$ [22]

$b:$ $\mathsf{SNo} = n_{20}$ [225]

$b:$ $\mathsf{SBit} = b_{20}$ [227]

$a:$ $\mathsf{SFile}(s(n_{20})) = \bot$ [235]

$b:$ $(\mathsf{A})(\mathsf{SNo} = n_{20}$ unless $\mathsf{ProcAck} = \mathsf{true})$ [241]

|

auf p: $a:$ $\mathsf{A}(\mathsf{SNo} = n_{20}$ unless $\mathsf{ProcAck} = \mathsf{true})$ [242]

$a:$ $\mathsf{ProcAck} = \mathsf{true}$ [243]

|

aus PA1,2:

$b:$ $\mathsf{SIM} = \mathsf{msg}(d_{22}, b_{20})$ [247]

$b:$ $\mathsf{SBit} = b_{20}$ [248] (aus [227])

$b:$ $\mathsf{RQ} = q_{22}$ [249]

$b:$ $\mathsf{SNo} = n_{20}$ [250] (aus [225])

$a:$ $\mathsf{SFile}(s(n_{20})) \neq \bot$ [251]

$a:$ $\mathsf{RQ} = q_{22}|\mathsf{msg}(\mathsf{SFile}(s(n_{20})), \mathsf{flip}(b_{20}))$ [252]

$a:$ $\mathsf{SNo} = s(n_{20})$ [253]

$a:$ $\mathsf{SBit} = \mathsf{flip}(b_{20})$ [254]

$a:$ $\mathsf{ready} = \mathsf{false}$ [255]

$\Box$ $(13, 255)$

$a:$ $\mathsf{SFile}(s(n_{20})) = \bot$ [256]

$a:$ $\mathsf{RQ} = q_{22}$ [257]

$a:$ $\mathsf{SNo} = n_{20}$ [258]

$a:$ $\mathsf{SBit} = b_{20}$ [259]

$a:$ $\mathsf{ready} = \mathsf{true}$ [260]

aus [14]:

$a:$ $\neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot)$ [261]

$\Box$: $a:$ $\mathsf{SFile}(s(n_{20})) = \bot$ [235]
$a:$ $\mathsf{SNo} = n_{20}$ [258]

$a:$ $\neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge$ [262]
$(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \to B = \mathsf{SBit}) \wedge$
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \to B' = \mathsf{SBit})))$

$\hookrightarrow$ (siehe Seite 238)

$a:$ $\mathsf{SNo} = n_{20}$ [244]

$a:$ $\neg(\mathsf{ProcAck} = \mathsf{true})$ [245]

$a:$ $(\mathsf{A})(\mathsf{SNo} = n_{20}$ unless $\mathsf{ProcAck} = \mathsf{true})$ [246]

$\hookrightarrow$ S. 237

$$\vdots$$

von [246] (S. 236):

$$p : [\,0, \{\ldots\}, b, \circ, a, \emptyset, \infty]\quad [16]$$

$$a:\ \mathsf{ready} = \mathsf{true}\quad [13]$$

$$a:\ \neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge (\forall D, B : \mathsf{RIM} = \mathsf{msg}(D,B) \rightarrow B = \mathsf{SBit}) \wedge \quad [14]$$
$$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D',B')|Q' \rightarrow B' = \mathsf{SBit}))$$

$$b:\ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})\quad [20]$$

$$b:\ \forall D, B : \mathsf{RIM} = \mathsf{msg}(D,B) \rightarrow B = \mathsf{SBit}\quad [21]$$

$$b:\ \forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D',B')|Q' \rightarrow B' = \mathsf{SBit}\quad [22]$$

$$b:\ \mathsf{SNo} = n_{20}\quad [225]$$

$$b:\ \mathsf{SBit} = b_{20}\quad [227]$$

$$a:\ \mathsf{SFile}(s(n_{20})) = \bot\quad [235]$$

$$b:\ (\mathsf{A})(\mathsf{SNo} = n_{20}\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})\quad [241]$$

$$a:\ \mathsf{SNo} = n_{20}\quad [244]$$

$$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})\quad [245]$$

aus [14]:

$$a:\ \neg(\mathsf{SFile}(s(\mathsf{SNo})) = \bot)\quad [263]$$

$$\boxed{\begin{array}{ll} \Box: & a:\ \mathsf{SFile}(s(n_{20})) = \bot\quad [235] \\ & a:\ \mathsf{SNo} = n_{20}\quad [244] \end{array}}$$

$$a:\ \neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \quad [264]$$
$$(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D,B) \rightarrow B = \mathsf{SBit}) \wedge$$
$$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D',B')|Q' \rightarrow B' = \mathsf{SBit})))$$

aus SBit:

$$b:\ \forall B : \mathsf{SBit} = B \rightarrow \mathsf{A}(\mathsf{SBit} = B\ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})\quad [265]$$

$$b:\ \mathsf{SBit} = B_{23} \rightarrow \mathsf{A}(\mathsf{SBit} = B_{23}\ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})\quad [266]$$

$$b:\ \neg(\mathsf{SBit} = B_{23})\quad [267]$$
$$\Box\ \{B_{23} \leftarrow b_{20}\}(227, 267)$$

$$b:\ \mathsf{A}(\mathsf{SBit} = b_{20}\ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})\quad [268]$$
$$b:\ (\mathsf{A})(\mathsf{SBit} = b_{20}\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})\quad [269]$$

auf p:

$$a:\ \mathsf{A}(\mathsf{SBit} = b_{20}\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})\quad [270]$$

$$a:\ \mathsf{ProcAck} = \mathsf{true}\quad [271]$$
$$\Box\ (245, 271)$$

$$a:\ \mathsf{SBit} = b_{20}\quad [272]$$
$$a:\ \neg(\mathsf{ProcAck} = \mathsf{true})\quad [273]$$
$$a:\ (\mathsf{A})(\mathsf{SBit} = b_{20}\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true})\quad [274]$$

$\hookrightarrow$ (siehe Seite 238)

Der Rest des Beweises erfolgt wie in [68] ff. (Seite 224) mit den folgenden Knoten:

$p : [0, \{\ldots\}, b, \circ, a, \emptyset, \infty]$ [16]
$a :$ $\mathsf{ready} = \mathsf{true}$ [13]
$b :$ $\mathsf{SNo} = n_{20}$ [225]
$b :$ $\mathsf{SBit} = b_{20}$ [227]
$a :$ $\mathsf{SBit} = b_{20}$ [259] bzw. $a :$ $\mathsf{SBit} = b_{20}$ [272]
$b :$ $\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})$ [20]

[64] und [65] werden durch
$b :$ $\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}$ [21]
$b :$ $\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}$ [22]
ersetzt,

$a :$ $\neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge$ [262] bzw. [264]
$(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge$
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$

12 Theorem 1: Korrektheit der Übertragung

$$\mathsf{A}\Box(\forall N : \mathsf{RFile}(N) = \bot \lor \mathsf{RFile}(N) = \mathsf{SFile}(N))$$

Beweis:

Der Beweis basiert auf dem Schema zur Durchführung eines Induktionsbeweises. Wieder ist der Induktionsanfang trivial, es wird nur der Induktionsschritt ausgeführt:

$$\vdots$$

$$p : [\,0, \{\neg(\neg A)\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$

$$a :\ \neg A \quad [9]$$

$$b :\ \neg(\neg A) \quad [12]$$

$$|$$

$$a :\ \neg(\forall N : \mathsf{RFile}(N) = \bot \lor \mathsf{RFile}(N) = \mathsf{SFile}(N)) \quad [9]$$

$$b :\ \forall N : \mathsf{RFile}(N) = \bot \lor \mathsf{RFile}(N) = \mathsf{SFile}(N) \quad [12]$$

$$|$$

$b :$ Lemma 3 [15]

$b :$ Lemma 4 [16]

$b :$ Lemma 5 [17]

$$|$$

aus [9]:

$$a :\ \neg(\mathsf{RFile}(n_1) = \bot \lor \mathsf{RFile}(n_1) = \mathsf{SFile}(n_1)) \quad [20]$$

$$a :\ \neg(\mathsf{RFile}(n_1) = \bot) \quad [21]$$

$$a :\ \neg(\mathsf{RFile}(n_1) = \mathsf{SFile}(n_1)) \quad [22]$$

$$|$$

aus [12]:

$$b :\ \mathsf{RFile}(N_2) = \bot \lor \mathsf{RFile}(N_2) = \mathsf{SFile}(N_2) \quad [23]$$

$$b :\ \mathsf{RFile}(N_2) = \bot \quad [24] \qquad\qquad b :\ \mathsf{RFile}(N_2) = \mathsf{SFile}(N_2) \quad [25]$$

$\hookrightarrow$ S. 244

$$|$$

aus RData:

$$b :\ \forall D, N : \mathsf{RFile}(N) = D \to \mathsf{A}(\mathsf{RFile}(N) = D \ \mathsf{unless}^+\ (\mathsf{AccDat} = \mathsf{true} \land \mathsf{RNo} = s(N))) \quad [26]$$

mit Tab. 0.11, $\{D \leftarrow \bot, N \leftarrow N_2\}$:

N_2 einsetzen (aus [28]):

$$a :\ \mathsf{AccDat} = \mathsf{true} \land \mathsf{RNo} = s(n_1) \quad [27]$$

$$a :\ \mathsf{AccDat} = \mathsf{true} \quad [29]$$

$$a :\ \mathsf{RNo} = s(n_1) \quad [30]$$

$\hookrightarrow$ S. 241

$$a :\ \mathsf{RFile}(N_2) = \bot \quad [28]$$

$$\Box\ \{N_2 \leftarrow n_1\}(21, 28)$$

$$\vdots$$

von [30] (S. 240):

$$a:\ \neg(\mathsf{RFile}(n_1) = \mathsf{SFile}(n_1))\quad [22]$$

$$a:\ \mathsf{AccDat} = \mathsf{true}\quad [29]$$

$$a:\ \mathsf{RNo} = s(n_1)\quad [30]$$

$$|$$

aus Tab. 0.9:

$$b:\ \mathsf{RIM} = \mathsf{msg}(d_3, b_3)\quad [31]$$

$$b:\ \mathsf{RBit} = b_3\quad [32]$$

$$b:\ \mathsf{RNo} = n_4\quad [33]$$

$$a:\ \mathsf{RFile}(n_4) = d_3\quad [34]$$

$$a:\ \mathsf{RNo} = s(n_4)\quad [35]$$

$$a:\ \mathsf{RBit} = \mathsf{flip}(b_3)\quad [36]$$

$$|$$

Lemma 4:

$$b:\ (\mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}) \wedge (\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo}))\quad [37]$$

$$b:\ \mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}\quad [38]$$

$$b:\ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo})\quad [39]$$

$$|$$

aus BR: $b:\ \forall B : \mathsf{RBit} = B \rightarrow (\mathsf{SBit} = B \vee \mathsf{SBit} = \mathsf{flip}(B))\quad [40]$

$$b:\ \mathsf{RBit} = B_5 \rightarrow (\mathsf{SBit} = B_5 \vee \mathsf{SBit} = \mathsf{flip}(B_5))\quad [41]$$

$$b:\ \neg(\mathsf{RBit} = B_5)\quad [42]$$

$$\Box\ \{B_5 \leftarrow b_3\}(32, 42)$$

$$b:\ \mathsf{SBit} = b_3 \vee \mathsf{SBit} = \mathsf{flip}(b_3)\quad [43]$$

$$b:\ \mathsf{SBit} = b_3\quad [44]$$

$\hookrightarrow$ S. 242

$$b:\ \mathsf{SBit} = \mathsf{flip}(b_3)\quad [45]$$

$$|$$

aus Lemma 3:

$$b:\ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_8)) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_8)|Q')) \rightarrow \quad [67]$$
$$(\mathsf{SBit} = \mathsf{flip}(B_8) \rightarrow \mathsf{RBit} = \mathsf{flip}(B_8))$$

$$b:\ \neg((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_8)) \vee \quad [68]$$
$$(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_8)|Q'))$$

$$|$$

$$b:\ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_8))\quad [70]$$

$$b:\ \neg(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_8)|Q')\quad [71]$$

$$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_8, B_8))\quad [72]$$

$$\Box\ \{D_8 \leftarrow d_3,\ B_8 \leftarrow b_3\}(31, 72)$$

$$b:\ \mathsf{SBit} = \mathsf{flip}(b_3) \rightarrow \mathsf{RBit} = \mathsf{flip}(b_3)\quad [69]$$

$$b:\ \neg(\mathsf{SBit} = \mathsf{flip}(b_3))\quad [73]$$

$$\Box\ (45, 73)$$

$$b:\ \mathsf{RBit} = \mathsf{flip}(b_3)\quad [74]$$

$$\Box\ (32, 74)$$

$\vdots$

von [44] (S. 241):

$a:\ \neg(\mathsf{RFile}(n_1) = \mathsf{SFile}(n_1))$ [22]

$a:\ \mathsf{RNo} = s(n_1)$ [30]

$b:\ \mathsf{RIM} = \mathsf{msg}(d_3, b_3)$ [31]

$b:\ \mathsf{RNo} = n_4$ [33]

$a:\ \mathsf{RFile}(n_4) = d_3$ [34]

$a:\ \mathsf{RNo} = s(n_4)$ [35]

$b:\ \mathsf{SBit} = b_3$ [44]

aus [38]:

$b:\ \neg(\mathsf{SBit} = \mathsf{RBit})$ [46]

$\boxed{\square :\ b:\ \mathsf{SBit} = b_3\ [44] \quad b:\ \mathsf{RBit} = b_3\ [32]}$

$b:\ \mathsf{RNo} = \mathsf{SNo}$ [47]

Lemma 5:

$b:\ \forall D, B : (\mathsf{RIM} = \mathsf{msg}(D,B) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D,B)|Q') \rightarrow$ [48]
$((B = \mathsf{SBit} \rightarrow D = \mathsf{SFile}(\mathsf{SNo})) \wedge (B = \mathsf{flip}(\mathsf{SBit}) \rightarrow D = \mathsf{SFile}(p(\mathsf{SNo}))))$

$b:\ (\mathsf{RIM} = \mathsf{msg}(D_6,B_6) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_6,B_6)|Q') \rightarrow$ [49]
$((B_6 = \mathsf{SBit} \rightarrow D_6 = \mathsf{SFile}(\mathsf{SNo})) \wedge (B_6 = \mathsf{flip}(\mathsf{SBit}) \rightarrow D_6 = \mathsf{SFile}(p(\mathsf{SNo}))))$

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_6,B_6) \vee$ [50]
$\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_6,B_6)|Q')$

$b:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_6,B_6))$ [52]

$b:\ \neg(\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_6,B_6)|Q')$ [53]

$\square\{D_6 \leftarrow d_3,\ B_6 \leftarrow b_3\}(31, 52)$

$b:\ (b_3 = \mathsf{SBit} \rightarrow d_3 = \mathsf{SFile}(\mathsf{SNo})) \wedge$ [51]
$(b_3 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_3 = \mathsf{SFile}(p(\mathsf{SNo})))$

$b:\ b_3 = \mathsf{SBit} \rightarrow d_3 = \mathsf{SFile}(\mathsf{SNo})$ [54]

$b:\ b_3 = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_3 = \mathsf{SFile}(p(\mathsf{SNo}))$ [55]

$b:\ \neg(b_3 = \mathsf{SBit})$ [56]

$\square\ (44, 56)$

$b:\ d_3 = \mathsf{SFile}(\mathsf{SNo})$ [57]

$\hookrightarrow$ S. 243

$$\vdots$$

von [57] (S. 242):

$a:\ \neg(\mathsf{RFile}(n_1) = \mathsf{SFile}(n_1))\quad [22]$

$a:\ \mathsf{RNo} = s(n_1)\quad [30]$

$b:\ \mathsf{RNo} = n_4\quad [33]$

$a:\ \mathsf{RFile}(n_4) = d_3\quad [34]$

$a:\ \mathsf{RNo} = s(n_4)\quad [35]$

$b:\ \mathsf{SBit} = b_3\quad [44]$

$b:\ \mathsf{RNo} = \mathsf{SNo}\quad [47]$

$b:\ d_3 = \mathsf{SFile}(\mathsf{SNo})\quad [57]$

|

aus SData:

$b:\ \forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\Box(\mathsf{SFile}(N) = D)\quad [58]$

$b:\ \mathsf{SFile}(N_7) = D_7 \to \mathsf{A}\Box(\mathsf{SFile}(N_7) = D_7)\quad [59]$

Linker Zweig:

$b:\ \neg(\mathsf{SFile}(N_7) = D_7)\quad [60]$

$\Box:\ b:\ d_3 = \mathsf{SFile}(\mathsf{SNo})\quad [57]$

$b:\ \mathsf{RNo} = \mathsf{SNo}\quad [47]$

$b:\ \mathsf{RNo} = n_4\quad [33]$

$\{N_7 \leftarrow n_4,\ D_7 \leftarrow d_3\}$

Rechter Zweig:

$b:\ \mathsf{A}\Box(\mathsf{SFile}(n_4) = d_3)\quad [61]$

$b:\ \mathsf{SFile}(n_4) = d_3\quad [62]$

$b:\ (\mathsf{A})\Box(\mathsf{SFile}(n_4) = d_3)\quad [63]$

auf p:

$a:\ \mathsf{A}\Box(\mathsf{SFile}(n_4) = d_3)\quad [64]$

$a:\ \mathsf{SFile}(n_4) = d_3\quad [65]$

$a:\ (\mathsf{A})\Box(\mathsf{SFile}(n_4) = d_3)\quad [66]$

$\Box:$

$$\frac{\begin{array}{l} a:\ \mathsf{RNo} = s(n_4)\quad [35] \\ a:\ \mathsf{RNo} = s(n_1)\quad [30]\end{array}}{\to\ n_4 = n_1}
\qquad
\frac{\frac{\begin{array}{l} a:\ \mathsf{SFile}(n_4) = d_3\quad [65] \\ a:\ \mathsf{RFile}(n_4) = d_3\quad [34]\end{array}}{\to\ \mathsf{SFile}(n_4) = \mathsf{RFile}(n_4)} \quad a:\ \neg(\mathsf{RFile}(n_1) = \mathsf{SFile}(n_1))\quad [22]}{\to\ n_4 \neq n_1}$$

$\vdots$

von [25] (S. 240):

$a: \neg(\mathsf{RFile}(n_1) = \mathsf{SFile}(n_1)) \quad [22]$

$b: \mathsf{RFile}(N_2) = \mathsf{SFile}(N_2) \quad [25]$

N_2 einsetzen (aus [28]):

$b: \mathsf{RFile}(n_1) = \mathsf{SFile}(n_1) \quad [75]$

EA:

$b: \mathsf{RFile}(n_1) = d_9 \quad [76]$

aus RData:

$b: \forall D, N: \mathsf{RFile}(N) = D \rightarrow \mathsf{A}(\mathsf{RFile}(N) = D \ \mathsf{unless}^+ \ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(N))) \quad [77]$

mit Tab. 0.11, $\{D \leftarrow d_9, N \leftarrow n_1\}$:

$a: \mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1) \quad [78]$

$\Box$: wie [27]:
Neue Zuweisung von $\mathsf{SFile}(n_1)$
durch AccDat.

$a: \mathsf{RFile}(n_1) = d_9 \quad [79]$

aus SData:

$b: \forall D, N: \mathsf{SFile}(N) = D \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N) = D) \quad [80]$

$b: \mathsf{SFile}(N_{10}) = D_{10} \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N_{10}) = D_{10}) \quad [81]$

$b: \neg(\mathsf{SFile}(N_{10}) = D_{10}) \quad [82]$

$\Box$: $b: \mathsf{RFile}(n_1) = \mathsf{SFile}(n_1) \quad [75]$
$b: \mathsf{RFile}(n_1) = d_9 \quad [76]$
$\{N_{10} \leftarrow n_1, \ D_{10} \leftarrow d_9\}$

$b: \mathsf{A}\Box(\mathsf{SFile}(n_1) = d_9) \quad [83]$

$b: \mathsf{SFile}(n_1) = d_9 \quad [84]$

$b: (\mathsf{A})\Box(\mathsf{SFile}(n_1) = d_9) \quad [85]$

auf p:

$a: \mathsf{A}\Box(\mathsf{SFile}(n_1) = d_9) \quad [86]$

$a: \mathsf{SFile}(n_1) = d_9 \quad [87]$

$a: (\mathsf{A})\Box(\mathsf{SFile}(n_1) = d_9) \quad [88]$

$\Box$: $a: \mathsf{SFile}(n_1) = d_9 \quad [87]$
$a: \mathsf{RFile}(n_1) = d_9 \quad [79]$
$a: \neg(\mathsf{RFile}(n_1) = \mathsf{SFile}(n_1)) \quad [22]$

In Knoten [76] äußert sich die Forderung, daß zur Anwendung einer Invarianzspezifikation die rechte Seite der Ausgangsgleichung zustandsunabhängig ausgewertet werden muß. Im vorliegenden Fall wird für den Wert $\mathsf{RFile}_b(n_1)$ der Skolembezeichner d_9 eingeführt.

13 Lemma 6: Keine Lücken in der Übertragung

$$\mathsf{A}\Box(\forall N : \mathsf{RNo} = s(N) \to \mathsf{RFile}(N) \neq \bot)$$

Beweis:

Der Beweis basiert auf dem Schema zur Durchführung eines Induktionsbeweises. Wieder ist der Induktionsanfang trivial, es wird nur der Induktionsschritt ausgeführt:

$$\vdots$$

$$p : [\,0, \{\neg(\neg A)\}, b, \circ, a, \emptyset, \infty\,] \quad [11]$$
$$a : \neg A \quad [9]$$
$$b : \neg(\neg A) \quad [12]$$

$$a : \neg(\forall N : \mathsf{RNo} = s(N) \to \mathsf{RFile}(N) \neq \bot) \quad [9]$$
$$b : \forall N : \mathsf{RNo} = s(N) \to \mathsf{RFile}(N) \neq \bot \quad [12]$$

aus [9]:

$$a : \neg(\mathsf{RNo} = s(n_1) \to \mathsf{RFile}(n_1) \neq \bot) \quad [20]$$
$$a : \mathsf{RNo} = s(n_1) \quad [21]$$
$$a : \neg(\mathsf{RFile}(n_1) \neq \bot) \quad [22]$$

aus EA:

$$b : \exists N : \mathsf{RNo} = N \quad [23]$$
$$b : \mathsf{RNo} = n_2 \quad [24]$$

aus RNo: $b : \forall N : \mathsf{RNo} = N \to \mathsf{A}(\mathsf{RNo} = N \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \quad [25]$

mit Tab. 0.11, $\{N \leftarrow n_2\}$:

Linker Zweig:

$$a : \mathsf{AccDat} = \mathsf{true} \quad [26]$$

mit Tab. 0.9:

$$b : \mathsf{RIM} = \mathsf{msg}(d_3, b_3) \quad [29]$$
$$b : \mathsf{RBit} = b_3 \quad [30]$$
$$b : \mathsf{RNo} = n_4 \quad [31]$$
$$a : \mathsf{RFile}(n_4) = d_3 \quad [32]$$
$$a : \mathsf{RNo} = s(n_4) \quad [33]$$
$$a : \mathsf{RBit} = \mathsf{flip}(b_3) \quad [34]$$

$\Box$:		
	$a : \mathsf{RNo} = s(n_1)$ [21]	$a : \neg(\mathsf{RFile}(n_1) \neq \bot)$ [22]
	$a : \mathsf{RNo} = s(n_4)$ [33]	$a : \mathsf{RFile}(n_4) = d_3$ [32]
	$\to n_1 = n_4$	$\to n_1 \neq n_4$

Rechter Zweig:

$$a : \mathsf{RNo} = n_2 \quad [27]$$
$$a : \neg(\mathsf{AccDat} = \mathsf{true}) \quad [28]$$

↪ S. 247

$\vdots$

von [28] (S. 246):

$p : [\,0, \{\neg(\neg A)\}, b, \circ, a, \emptyset, \infty\,]$ [11]

$b:\ \forall N : \mathsf{RNo} = s(N) \rightarrow \mathsf{RFile}(N) \neq \bot$ [12]

$a:\ \mathsf{RNo} = s(n_1)$ [21]

$a:\ \neg(\mathsf{RFile}(n_1) \neq \bot)$ [22]

$b:\ \mathsf{RNo} = n_2$ [24]

$a:\ \mathsf{RNo} = n_2$ [27]

$a:\ \neg(\mathsf{AccDat} = \mathsf{true})$ [28]

aus [12]:

$b:\ \mathsf{RNo} = s(N_5) \rightarrow \mathsf{RFile}(N_5) \neq \bot$ [35]

$b:\ \neg(\mathsf{RNo} = s(N_5))$ [36]

$\Box:$	$a:\ \mathsf{RNo} = n_2$ [27]
	$b:\ \mathsf{RNo} = n_2$ [24]
	$a:\ \mathsf{RNo} = s(n_1)$ [21]
	$\Box\ \{N_5 \leftarrow n_1\}$

$b:\ \mathsf{RFile}(n_1) \neq \bot$ [37]

aus F3R:

$b:\ \forall N : \mathsf{RFile}(N) = \bot \vee \exists D : \mathsf{RFile}(N) = D$ [38]

$b:\ \mathsf{RFile}(N_6) = \bot \vee \exists D : \mathsf{RFile}(N_6) = D$ [39]

$b:\ \mathsf{RFile}(N_6) = \bot$ [40]

$\Box\ \{N_6 \leftarrow n_1\}(37, 40)$

$b:\ \exists D : \mathsf{RFile}(n_1) = D$ [41]

$b:\ \mathsf{RFile}(n_1) = d_6$ [42]

aus RData:

$b:\ \forall D, N : \mathsf{RFile}(N) = D \rightarrow \mathsf{A}(\mathsf{RFile}(N) = D\ \mathsf{unless}^+\ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(N))$ [43]

mit Tab. 0.11, $\{D \leftarrow d_6,\ N \leftarrow n_1\}$:

$a:\ \mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)$ [44]

$a:\ \mathsf{AccDat} = \mathsf{true}$ [45]

$a:\ \mathsf{RNo} = s(n_1)$ [46]

$\Box\ (28, 46)$

$a:\ \mathsf{RFile}(n_1) = d_6$ [47]

$\Box:$	$b:\ \mathsf{RFile}(n_1) \neq \bot$ [37]
	$b:\ \mathsf{RFile}(n_1) = d_6$ [42]
	$\rightarrow\ d_6 \neq \bot$
	$a:\ \neg(\mathsf{RFile}(n_1) \neq \bot)$ [22]
	$a:\ \mathsf{RFile}(n_1) = d_6$ [47]
	$\rightarrow\ d_6 = \bot$

14 Korollar 3: Korrektheit der Quittung

Nach diesen Erkenntnissen kann man ein (rein prädikatenlogisches) Korollar formulieren, das in den folgenden Beweisen verwendet wird: Wenn eine erwartete Quittung eintrifft, ist der Empfänger bereit, das nächste Datum zu empfangen und hat das quittierte Datum korrekt abgelegt.

$$\forall D, B, N : ((\mathsf{SIM} = \mathsf{msg}(D, B) \wedge \mathsf{SBit} = B \wedge \mathsf{SNo} = N) \rightarrow$$
$$(\mathsf{RBit} = \mathsf{flip}(B) \wedge \mathsf{RNo} = s(N) \wedge \mathsf{RFile}(N) = \mathsf{SFile}(N)))$$

Beweis:

$$\neg(\forall D, B, N : ((\mathsf{SIM} = \mathsf{msg}(D, B) \wedge \mathsf{SBit} = B \wedge \mathsf{SNo} = N) \rightarrow \quad [1]$$
$$(\mathsf{RBit} = \mathsf{flip}(B) \wedge \mathsf{RNo} = s(N) \wedge \mathsf{RFile}(N) = \mathsf{SFile}(N)))$$

$$\neg((\mathsf{SIM} = \mathsf{msg}(d_1, b_1) \wedge \mathsf{SBit} = b_1 \wedge \mathsf{SNo} = n_1) \rightarrow \quad [2]$$
$$(\mathsf{RBit} = \mathsf{flip}(B) \wedge \mathsf{RNo} = s(\mathsf{SNo}) \wedge \mathsf{RFile}(N) = \mathsf{SFile}(N)))$$

$$\mathsf{SIM} = \mathsf{msg}(d_1, b_1) \wedge \mathsf{SBit} = b_1 \wedge \mathsf{SNo} = n_1 \quad [3]$$
$$\neg(\mathsf{RBit} = \mathsf{flip}(b_1) \wedge \mathsf{RNo} = s(n_1) \wedge \mathsf{RFile}(n_1) = \mathsf{SFile}(n_1)) \quad [4]$$

$$\mathsf{SIM} = \mathsf{msg}(d_1, b_1) \quad [5]$$
$$\mathsf{SBit} = b_1 \quad [6]$$
$$\mathsf{SNo} = n_1 \quad [7]$$

mit Lemma 2:

$$\forall B : \quad ((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B)|Q')) \rightarrow \quad [8]$$
$$(\mathsf{SBit} = B \rightarrow \mathsf{RBit} = \mathsf{flip}(B))$$

$$((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_2)) \vee (\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_2)|Q')) \rightarrow \quad [9]$$
$$(\mathsf{SBit} = B_2 \rightarrow \mathsf{RBit} = \mathsf{flip}(B_2))$$

$$\neg((\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_2)) \vee \quad [10]$$
$$(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_2)|Q'))$$

$$\neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, B_2)) \quad [12]$$
$$\neg(\exists Q, Q', D' : \mathsf{SQ} = Q|\mathsf{msg}(D', B_2)|Q') \quad [13]$$
$$\neg(\mathsf{SIM} = \mathsf{msg}(D_2, B_2)) \quad [14]$$
$$\Box\{D_2 \leftarrow d_1,\ B_2 \leftarrow b_1\}(5, 14)$$

$$\mathsf{SBit} = b_1 \rightarrow \mathsf{RBit} = \mathsf{flip}(b_1) \quad [11]$$

$$\neg(\mathsf{SBit} = b_1) \quad [15]$$
$$\Box\ (6, 15)$$

$$\mathsf{RBit} = \mathsf{flip}(b_1) \quad [16]$$

↪ S. 249

$\vdots$

von [16] (S. 248):

$\neg(\mathsf{RBit} = \mathsf{flip}(b_1) \wedge \mathsf{RNo} = s(n_1) \wedge \mathsf{RFile}(n_1) = \mathsf{SFile}(n_1) \quad [4]$

$\mathsf{SNo} = n_1 \quad [7]$

$\mathsf{RBit} = \mathsf{flip}(b_1) \quad [16]$

mit Lemma 4:

$(\mathsf{SBit} = \mathsf{RBit} \to \mathsf{RNo} = \mathsf{SNo}) \wedge (\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \to \mathsf{RNo} = s(\mathsf{SNo})) \quad [17]$

$\mathsf{SBit} = \mathsf{RBit} \to \mathsf{RNo} = \mathsf{SNo} \quad [18]$

$\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \to \mathsf{RNo} = s(\mathsf{SNo}) \quad [19]$

$\neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit})) \quad [20]$

$\square$:	$\mathsf{SBit} = b_1 \quad [6]$
	$\mathsf{RBit} = \mathsf{flip}(b_1) \quad [16]$

$\mathsf{RNo} = s(\mathsf{SNo}) \quad [21]$

Lemma 6:

$\forall N : \mathsf{RNo} = s(N) \to \mathsf{RFile}(N) \neq \bot \quad [22]$

$\mathsf{RNo} = s(N_3) \to \mathsf{RFile}(N_3) \neq \bot \quad [23]$

$\neg(\mathsf{RNo} = s(N_3)) \quad [24]$

$\square$:	$\mathsf{RNo} = s(\mathsf{SNo}) \quad [21]$
	$\mathsf{SNo} = n_1 \quad [7]$
	$\{N_3 \leftarrow n_1\}$

$b : \ \mathsf{RFile}(n_1) \neq \bot \quad [25]$

Theorem 1:

$\forall N : \mathsf{RFile}(N) = \bot \vee \mathsf{RFile}(N) = \mathsf{SFile}(N) \quad [26]$

$\mathsf{RFile}(N_4) = \bot \vee \mathsf{RFile}(N_4) = \mathsf{SFile}(N_4) \quad [27]$

$\mathsf{RFile}(N_4) = \bot \quad [28]$

$\square \ \{N_4 \leftarrow n_1\}(25, 28)$

$\mathsf{RFile}(n_1) = \mathsf{SFile}(n_1) \quad [29]$

aus [4]: $\neg(\mathsf{RBit} = \mathsf{flip}(b_1) \wedge \mathsf{RNo} = s(n_1) \wedge \mathsf{RFile}(n_1) = \mathsf{SFile}(n_1) \quad [4]$

$\neg(\mathsf{RBit} = \mathsf{flip}(b_1) \quad [30]$

$\square \ (16, 30)$

$\neg(\mathsf{RNo} = s(n_1) \quad [31]$

$\square$:	$\mathsf{RNo} = s(\mathsf{SNo}) \quad [21]$
	$\mathsf{SNo} = n_1 \quad [7]$

$\neg(\mathsf{RFile}(n_1) = \mathsf{SFile}(n_1) \quad [32]$

$\square \ (29, 32)$

15 Korollar 4: Persistenz übertragener Daten

Ein weiteres Korollar betrifft die Persistenz der in RFile gespeicherten Daten:

$$\mathsf{A}\Box(\forall D, N : \mathsf{RFile}(N) = D \wedge D \neq \perp \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N) = D))$$

Beweis:

$$0: \ \neg(\mathsf{A}\Box(\forall D, N : \mathsf{RFile}(N) = D \wedge D \neq \perp \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N) = D))) \quad [1]$$
$$p : [\,0, \emptyset, \infty] \quad [2]$$
$$0: \ p\ \neg(\Box(\forall D, N : \mathsf{RFile}(N) = D \wedge D \neq \perp \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N) = D))) \quad [3]$$

$$0: \ p\ \neg(\forall D, N : (\ldots)) \quad [4]$$

wie [6] mit 0 anstelle a

$$0: \ (p)\Diamond\neg(\forall D, N : \mathsf{RFile}(N) = D \wedge D \neq \perp \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N) = D)) \quad [5]$$

$$p : [\,0, \{\forall D, N : \mathsf{RFile}(N) = D \wedge D \neq \perp \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N) = D)\}, a, \emptyset, \infty] \quad [6]$$
$$a: \ \neg(\forall D, N : \mathsf{RFile}(N) = D \wedge D \neq \perp \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N) = D)) \quad [7]$$
$$a: \ \neg(\mathsf{RFile}(n_1) = d_1 \wedge d_1 \neq \perp \rightarrow \mathsf{A}\Box(\mathsf{RFile}(n_1) = d_1)) \quad [8]$$

$$a: \ \mathsf{RFile}(n_1) = d_1 \wedge d_1 \neq \perp \quad [9]$$
$$a: \ \neg(\mathsf{A}\Box(\mathsf{RFile}(n_1) = d_1)) \quad [10]$$

$$a: \ \mathsf{RFile}(n_1) = d_1 \quad [11]$$
$$a: \ d_1 \neq \perp \quad [12]$$

mit Theorem 1:

$$a: \ \forall N : \mathsf{RFile}(N) = \perp \vee \mathsf{RFile}(N) = \mathsf{SFile}(N) \quad [13]$$
$$a: \ \mathsf{RFile}(N_2) = \perp \vee \mathsf{RFile}(N_2) = \mathsf{SFile}(N_2) \quad [14]$$

$$a: \ \mathsf{RFile}(N_2) = \perp \quad [15]$$

$\Box$: $a: \ \mathsf{RFile}(n_1) = d_1$ [11]
$a: \ d_1 \neq \perp$ [12]
$\{N_2 \leftarrow n_1\}$

$$a: \ \mathsf{RFile}(n_1) = \mathsf{SFile}(n_1) \quad [16]$$

aus SData:

$$a: \ \forall D, N : \mathsf{SFile}(N) = D \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N) = D) \quad [17]$$
$$a: \ \mathsf{SFile}(N_3) = D_3 \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N_3) = D_3) \quad [18]$$

$$a: \ \neg(\mathsf{SFile}(N_3) = D_3) \quad [19]$$

$\Box$: $a: \ \mathsf{RFile}(n_1) = \mathsf{SFile}(n_1)$ [16]
$a: \ \mathsf{RFile}(n_1) = d_1$ [11]
$\{N_3 \leftarrow n_1, D_3 \leftarrow d_1\}$

$$a: \ \mathsf{A}\Box(\mathsf{SFile}(n_1) = d_1) \quad [20]$$
$$a: \ \mathsf{SFile}(n_1) = d_1 \quad [21]$$
$$a: \ (\mathsf{A})\Box(\mathsf{SFile}(n_1) = d_1) \quad [22]$$

↪ S. 251

$\vdots$

von [22] (S. 250):

$a:\ \neg(\mathsf{A}\Box(\mathsf{RFile}(n_1) = d_1))$ [10]

$a:\ \mathsf{RFile}(n_1) = d_1$ [11]

$a:\ d_1 \neq \bot$ [12]

$a:\ \mathsf{SFile}(n_1) = d_1$ [21]

$a:\ (\mathsf{A})\Box(\mathsf{SFile}(n_1) = d_1)$ [22]

aus [10]:

$q : [\,a, \emptyset, \infty]$ [23]

$a:\ q\ \neg(\Box(\mathsf{RFile}(n_1) = d_1))$ [24]

[22] auf q:

$q : [\,a, \{\mathsf{SFile}(n_1) = d_1\}, \infty]$ [25]

aus [24]:

$a:\ \neg(\mathsf{RFile}(n_1) = d_1)$ [26]
$\Box\ (11, 26)$

$a:\ (q)\Diamond(\neg(\mathsf{RFile}(n_1) = d_1))$ [27]

$q : [\,a, \{\mathsf{SFile}(n_1) = d_1, \mathsf{RFile}(n_1) = d_1\}, b, \{\mathsf{SFile}(n_1) = d_1\}, \infty]$ [28]

$b:\ \mathsf{SFile}(n_1) = d_1$ [29]

$b:\ \neg(\mathsf{RFile}(n_1) = d_1)$ [30]

Vorgängerknoten von b betrachten:

$q : [\,a, \circ, b, \{\mathsf{SFile}(n_1) = d_1\}, \infty]$ [31]

wie [32] mit a anstelle c und
$a:\ \mathsf{RFile}(n_1) = d_1$ [11]
$a:\ \mathsf{SFile}(n_1) = d_1$ [21]

$q : [\,a, \{\mathsf{RFile}(n_1) = d_1, \mathsf{SFile}(n_1) = d_1\},$ [32]
$c, \circ, b, \{\mathsf{SFile}(n_1) = d_1\}, \infty]$

$c:\ \mathsf{SFile}(n_1) = d_1$ [33]

$c:\ \mathsf{RFile}(n_1) = d_1$ [34]

aus RData:

$c:\ \forall D, N : \mathsf{RFile}(N) = D \rightarrow \mathsf{A}(\mathsf{RFile}(N) = D\ \mathsf{unless}^{+}\ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(N)))$ [35]

$c:\ \mathsf{RFile}(N_4) = D_4 \rightarrow \mathsf{A}(\mathsf{RFile}(N_4) = D_4\ \mathsf{unless}^{+}\ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(N_4)))$ [36]

$c:\ \neg(\mathsf{RFile}(N_4) = D_4)$ [37]
$\Box\ \{N_4 \leftarrow n_1,\ D_4 \leftarrow d_1\}(34, 37)$

$c:\ \mathsf{A}(\mathsf{RFile}(n_1) = d_1\ \mathsf{unless}^{+}\ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)))$ [38]

$c:\ (\mathsf{A})(\mathsf{RFile}(n_1) = d_1\ \mathsf{unless}\ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)))$ [39]

$\hookrightarrow$ S. 252

$\vdots$

von [39] (S. 251):

$q : [\,a, \{\mathsf{RFile}(n_1) = d_1, \mathsf{SFile}(n_1) = d_1\}, c, \circ, b, \{\mathsf{SFile}(n_1) = d_1\}, \infty]$ [32]

$b :\ \mathsf{SFile}(n_1) = d_1$ [29]

$b :\ \neg(\mathsf{RFile}(n_1) = d_1)$ [30]

$c :\ (\mathsf{A})(\mathsf{RFile}(n_1) = d_1\ \mathsf{unless}\ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)))$ [39]

|

auf q:

$b :\ \mathsf{A}(\mathsf{RFile}(n_1) = d_1\ \mathsf{unless}\ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)))$ [40]

Linker Zweig:

$b :\ \mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)$ [41]

$b :\ \mathsf{AccDat} = \mathsf{true}$ [45]

$b :\ \mathsf{RNo} = s(n_1)$ [46]

|

aus AD1:

$c :\ (\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \rightarrow (\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = B)$ [47]

Linker Zweig:

$c :\ \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}))$ [48]

$c :\ (\mathsf{A})\circ\neg(\mathsf{AccDat} = \mathsf{true})$ [50]

auf q:

$b :\ \neg(\mathsf{AccDat} = \mathsf{true})$ [51]

$\Box$ (45, 51)

Rechter Zweig:

$c :\ \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = B$ [49]

$c :\ \mathsf{RIM} = \mathsf{msg}(d_5, b_5) \wedge \mathsf{RBit} = b_5$ [52]

$c :\ \mathsf{RIM} = \mathsf{msg}(d_5, b_5)$ [53]

$c :\ \mathsf{RBit} = b_5$ [54]

|

aus EA:

$c :\ \exists N : \mathsf{RNo} = N$ [55]

$c :\ \mathsf{RNo} = n_6$ [56]

|

mit F5:

$c :\ \forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow D \neq \bot$ [57]

$c :\ \mathsf{RIM} = \mathsf{msg}(D_7, B_7) \rightarrow D_7 \neq \bot$ [58]

Linker Zweig:

$c :\ \neg(\mathsf{RIM} = \mathsf{msg}(D_7, B_7))$ [59]

$\Box\ \{D_7 \leftarrow d_5,\ B_7 \leftarrow b_5\}(53, 59)$

Rechter Zweig:

$c :\ d_5 \neq \bot$ [60]

$\hookrightarrow$ S. 253

Rechter Zweig (von [40]):

$b :\ \mathsf{RFile}(n_1) = d_1$ [42]

$b :\ \neg(\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1))$ [43]

$b :\ (\mathsf{A})(\mathsf{RFile}(n_1) = d_1\ \mathsf{unless}\ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)))$ [44]

$\Box$ (30, 42)

$$\vdots$$

von [60] (S. 252):

$$q : [\, a, \{\mathsf{RFile}(n_1) = d_1, \mathsf{SFile}(n_1) = d_1\}, c, \circ, b, \{\mathsf{SFile}(n_1) = d_1\}, \infty] \quad [32]$$

$$b:\ \mathsf{SFile}(n_1) = d_1 \quad [29]$$
$$b:\ \neg(\mathsf{RFile}(n_1) = d_1) \quad [30]$$
$$b:\ \mathsf{AccDat} = \mathsf{true} \quad [45]$$
$$b:\ \mathsf{RNo} = s(n_1) \quad [46]$$
$$c:\ \mathsf{RIM} = \mathsf{msg}(d_5, b_5) \quad [53]$$
$$c:\ \mathsf{RBit} = b_5 \quad [54]$$
$$c:\ \mathsf{RNo} = n_6 \quad [56]$$
$$c:\ d_5 \neq \bot \quad [60]$$

aus AD2: $c:\ \forall D, B, N :\ (\mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RNo} = N \wedge \mathsf{RBit} = B) \rightarrow$ [61]

$$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(N) = D \wedge \mathsf{RNo} = s(N) \wedge \mathsf{RBit} = \mathsf{flip}(B))$$

$$c:\ (\mathsf{RIM} = \mathsf{msg}(D_8, B_8) \wedge \mathsf{RNo} = N_8 \wedge \mathsf{RBit} = B_8) \rightarrow \quad [62]$$
$$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(N_8) = D_8 \wedge \mathsf{RNo} = s(N_8) \wedge \mathsf{RBit} = \mathsf{flip}(B_8))$$

$$c:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_8, B_8) \wedge \mathsf{RNo} = N_8 \wedge \mathsf{RBit} = B_8) \quad [63]$$
$$\Box^*\ \{D_8 \leftarrow d_5,\ B_8 \leftarrow b_5,\ N_8 \leftarrow n_6\}(53, 54, 56, 63)$$

$$c:\ \mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \quad [64]$$
$$\mathsf{RFile}(n_6) = d_5 \wedge$$
$$\mathsf{RNo} = s(n_6) \wedge \mathsf{RBit} = \mathsf{flip}(b_5))$$

$$c:\ (\mathsf{A})\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(n_6) = d_5 \wedge \mathsf{RNo} = s(n_6) \wedge \mathsf{RBit} = \mathsf{flip}(b_5)) \quad [65]$$

auf q:

$$b:\ \mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(n_6) = d_5 \wedge \mathsf{RNo} = s(n_6) \wedge \mathsf{RBit} = \mathsf{flip}(b_5) \quad [66]$$

$$b:\ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [67]$$
$$\Box\ (45, 67)$$

$$b:\ \mathsf{RFile}(n_6) = d_5 \quad [68]$$
$$b:\ \mathsf{RNo} = s(n_6) \quad [69]$$
$$b:\ \mathsf{RBit} = \mathsf{flip}(b_5) \quad [70]$$

mit Theorem 1: $b:\ \forall N : \mathsf{RFile}(N) = \bot \vee \mathsf{RFile}(N) = \mathsf{SFile}(N)$ [71]

$$b:\ \mathsf{RFile}(N_9) = \bot \vee \mathsf{RFile}(N_9) = \mathsf{SFile}(N_9) \quad [72]$$

$$b:\ \mathsf{RFile}(N_9) = \bot \quad [73]$$

$$\boxed{\begin{array}{ll} \Box: & b:\ \mathsf{RFile}(n_6) = d_5 \quad [68] \\ & b:\ d_5 \neq \bot \quad [60] \\ & \{N_9 \leftarrow n_6\} \end{array}}$$

$$b:\ \mathsf{RFile}(n_6) = \mathsf{SFile}(n_6) \quad [74]$$

$$\boxed{\begin{array}{lll} \Box: & b:\ \mathsf{RNo} = s(n_1) \quad [46] & b:\ \mathsf{SFile}(n_1) = d_1 \quad [29] \\ & \underline{b:\ \mathsf{RNo} = s(n_6) \quad [69]} & b:\ \neg(\mathsf{RFile}(n_1) = d_1) \quad [30] \\ & \rightarrow\ n_1 = n_6 & \end{array}}$$

16 Korollar 5: ready=true

In Korollar 5 werden mehrere Aussagen über das weitere Verhalten der EA wenn $\mathsf{ready} = \mathsf{true}$ gilt, zusammengefaßt:
1:

$$\mathsf{A}\Box(\mathsf{ready} = \mathsf{true} \rightarrow \mathsf{A}\Box(\mathsf{ready} = \mathsf{true}))$$

2:

$$\mathsf{A}\Box(\mathsf{ready} = \mathsf{true} \rightarrow (\forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}\Box(\mathsf{SNo} = N)))$$

3:

$$\mathsf{A}\Box(\mathsf{ready} = \mathsf{true} \rightarrow (\forall D, N : \mathsf{RFile}(N) = D \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N) = D)))$$

Beweis von 1:

$0 : \ \mathsf{ready} = \mathsf{false} \quad [2]$

$0 : \ \neg(\mathsf{A}\Box(\mathsf{ready} = \mathsf{true} \rightarrow \mathsf{A}\Box(\mathsf{ready} = \mathsf{true}))) \quad [3]$

$p : [\,0, \emptyset, \infty] \quad [4]$

$0 : \ p\ \neg(\Box(\mathsf{ready} = \mathsf{true} \rightarrow \mathsf{A}\Box(\mathsf{ready} = \mathsf{true}))) \quad [5]$

$0 : \ \neg(\mathsf{ready} = \mathsf{true} \rightarrow (\ldots)) \quad [6]$

$0 : \ \mathsf{ready} = \mathsf{true} \quad [9]$

$0 : \ \neg(\ldots) \quad [10]$

$\Box \ (2, 9)$

$0 : \ \mathsf{ready} = \mathsf{true} \rightarrow \mathsf{A}\Box(\mathsf{ready} = \mathsf{true}) \quad [7]$

$0 : \ (p)\neg(\Box(\mathsf{ready} = \mathsf{true} \rightarrow \mathsf{A}\Box(\mathsf{ready} = \mathsf{true}))) \quad [8]$

$p : [\,0, \{\mathsf{ready} = \mathsf{true} \rightarrow \mathsf{A}\Box(\mathsf{ready} = \mathsf{true})\}, a, \emptyset, \infty] \quad [11]$

$a : \ \neg(\mathsf{ready} = \mathsf{true} \rightarrow \mathsf{A}\Box(\mathsf{ready} = \mathsf{true})) \quad [12]$

$a : \ \mathsf{ready} = \mathsf{true} \quad [13]$

$a : \ \neg(\mathsf{A}\Box(\mathsf{ready} = \mathsf{true})) \quad [14]$

$q : [\,a, \emptyset, \infty] \quad [15]$

$a : \ q\ \neg(\Box(\mathsf{ready} = \mathsf{true})) \quad [16]$

$a : \ \neg(\mathsf{ready} = \mathsf{true}) \quad [17]$

$\Box \ (13, 17)$

$a : \ (q)\neg(\Box(\mathsf{ready} = \mathsf{true})) \quad [18]$

$q : [\,a, \{\mathsf{ready} = \mathsf{true}\}, b, \emptyset, \infty] \quad [19]$

$b : \ \neg(\mathsf{ready} = \mathsf{true}) \quad [20]$

Vorgängerknoten von b betrachten:

$q : [\,a, \circ, b, \emptyset, \infty] \quad [21]$

wie [22] mit 0 anstelle b und
$a : \ \mathsf{ready} = \mathsf{true} \quad [13]$

$q : [\,a, \{\mathsf{ready} = \mathsf{true}\}, c, \circ, b, \emptyset, \infty] \quad [22]$

$c : \ \mathsf{ready} = \mathsf{true} \quad [23]$

$\hookrightarrow$ S. 256

$\vdots$

von [23] (S. 255):

$q : [\,a, \{\mathsf{ready} = \mathsf{true}\}, c, \circ, b, \emptyset, \infty]$ [22]

$b :\ \neg(\mathsf{ready} = \mathsf{true})$ [20]

$c :\ \mathsf{ready} = \mathsf{true}$ [23]

|

aus Korollar 2:

$c :\ \mathsf{ready} = \mathsf{true} \rightarrow (\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge$ [24]
$(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}) \wedge$
$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}))$

Left branch:

$c :\ \neg(\mathsf{ready} = \mathsf{true})$ [25]
$\Box\ (23, 25)$

Right branch:

$c :\ \mathsf{SFile}(s(\mathsf{SNo})) = \bot$ [26]
$c :\ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})$ [27]
$c :\ \forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \rightarrow B = \mathsf{SBit}$ [28]
$c :\ \forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \rightarrow B' = \mathsf{SBit}$ [29]

|

aus EA:

$c :\ \exists N : \mathsf{SNo} = N$ [30]
$c :\ \mathsf{SNo} = n_1$ [31]

|

aus SData:

$c :\ \forall D, N : \mathsf{SFile}(N) = D \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N) = D)$ [32]
$c :\ \mathsf{SFile}(N_2) = D_2 \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N_2) = D_2)$ [33]

Left branch:

$c :\ \neg(\mathsf{SFile}(N_2) = D_2)$ [34]

$\Box :\ c :\ \mathsf{SFile}(s(\mathsf{SNo})) = \bot$ [26]
$c :\ \mathsf{SNo} = n_1$ [31]
$\{N_2 \leftarrow s(n_1),\ D_2 \leftarrow \bot\}$

Right branch:

$c :\ \mathsf{A}\Box(\mathsf{SFile}(s(n_1)) = \bot)$ [35]
$c :\ \mathsf{SFile}(s(n_1)) = \bot$ [36]
$c :\ (\mathsf{A})\Box(\mathsf{SFile}(s(n_1)) = \bot)$ [37]
auf q:
$b :\ \mathsf{A}\Box(\mathsf{SFile}(s(n_1)) = \bot)$ [38]

|

$b :\ \mathsf{SFile}(s(n_1)) = \bot$ [39]
$b :\ (\mathsf{A})\Box(\mathsf{SFile}(s(n_1)) = \bot)$ [40]

|

aus ready:

$c :\ \forall T : \mathsf{ready} = T \rightarrow \mathsf{A}(\mathsf{ready} = T\ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})$ [41]
$c :\ \mathsf{ready} = T_3 \rightarrow \mathsf{A}(\mathsf{ready} = T_3\ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})$ [42]

Left branch:

$c :\ \neg(\mathsf{ready} = T_3)$ [43]
$\Box\ \{T_3 \leftarrow \mathsf{true}\}(23, 43)$

Right branch:

$c :\ \mathsf{A}(\mathsf{ready} = \mathsf{true}\ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true})$ [44]
$\hookrightarrow$ S. 257

$$\vdots$$

von [44] (S. 256):

$q : [\,a, \{\mathsf{ready} = \mathsf{true}\}, c, \circ, b, \emptyset, \infty]$ [22]

$b :$ $\neg(\mathsf{ready} = \mathsf{true})$ [20]

$c :$ $\mathsf{SNo} = n_1$ [31]

$b :$ $\mathsf{SFile}(s(n_1)) = \perp$ [39]

$c :$ $\mathsf{A}(\mathsf{ready} = \mathsf{true\ unless}^+ \ \mathsf{ProcAck} = \mathsf{true})$ [44]

$c :$ $(\mathsf{A})(\mathsf{ready} = \mathsf{true\ unless\ ProcAck} = \mathsf{true})$ [45]

auf q:

$b :$ $\mathsf{A}(\mathsf{ready} = \mathsf{true\ unless\ ProcAck} = \mathsf{true})$ [46]

Linker Zweig:

$b :$ $\mathsf{ProcAck} = \mathsf{true}$ [47]

aus PA1:

$c :$ $\mathsf{SIM} = \mathsf{msg}(d_4, b_4)$ [51]

$c :$ $\mathsf{SBit} = b_4$ [52]

$c :$ $\mathsf{RQ} = q_4$ [53]

$c :$ $\mathsf{SNo} = n_4$ [54]

Rechter Zweig:

$b :$ $\mathsf{ready} = \mathsf{true}$ [48]

$b :$ $\neg(\mathsf{ProcAck} = \mathsf{true})$ [49]

$b :$ $\mathsf{A}(\mathsf{ready} = \mathsf{true\ unless\ ProcAck} = \mathsf{true})$ [50]

$\square$ $(20, 48)$

aus PA2 (mit $c :$ $\mathsf{SNo} = n_1$ [31]):

$b :$ $\mathsf{SFile}(s(n_1)) \neq \perp$ [55]

$b :$ $\mathsf{RQ} = q_4|\mathsf{msg}(\mathsf{SFile}(s(n_1)), \mathsf{flip}(b_4))$ [56]

$b :$ $\mathsf{SNo} = s(n_1)$ [57]

$b :$ $\mathsf{SBit} = \mathsf{flip}(b_4)$ [58]

$b :$ $\mathsf{ready} = \mathsf{false}$ [59]

$\square$ $(55, 39)$

$b :$ $\mathsf{SFile}(s(n_1)) = \perp$ [60]

$b :$ $\mathsf{RQ} = q_4$ [61]

$b :$ $\mathsf{SNo} = n_1$ [62]

$b :$ $\mathsf{SBit} = b_4$ [63]

$b :$ $\mathsf{ready} = \mathsf{true}$ [64]

$\square$ $(20, 64)$

Beweis von 2:

$0: \ \mathsf{ready} = \mathsf{false} \quad [2]$

$0: \ \neg(\mathsf{A}\Box(\mathsf{ready} = \mathsf{true} \rightarrow (\forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}\Box(\mathsf{SNo} = N)))) \quad [3]$

$p : [\,0, \emptyset, \infty] \quad [4]$

$0: \ p\ \neg(\Box(\mathsf{ready} = \mathsf{true} \rightarrow (\forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}\Box(\mathsf{SNo} = N)))) \quad [5]$

$0: \ \neg(\mathsf{ready} = \mathsf{true} \rightarrow (\ldots)) \quad [6]$

$0: \ \mathsf{ready} = \mathsf{true} \quad [9]$

$0: \ \neg(\ldots) \quad [10]$

$\Box \ (2,9)$

$0: \ \mathsf{ready} = \mathsf{true} \rightarrow (\forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}\Box(\mathsf{SNo} = N)) \quad [7]$

$0: \ (p)\neg(\Box(\mathsf{ready} = \mathsf{true} \rightarrow (\forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}\Box(\mathsf{SNo} = N)))) \quad [8]$

$p : [\,0, \{\mathsf{ready} = \mathsf{true} \rightarrow (\forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}\Box(\mathsf{SNo} = N)\}, a, \emptyset, \infty] \quad [11]$

$a: \ \neg(\mathsf{ready} = \mathsf{true} \rightarrow (\forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}\Box(\mathsf{SNo} = N))) \quad [12]$

$a: \ \mathsf{ready} = \mathsf{true} \quad [13]$

$a: \ \neg(\forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}\Box(\mathsf{SNo} = N)) \quad [14]$

$a: \ \neg(\mathsf{SNo} = n_1 \rightarrow \mathsf{A}\Box(\mathsf{SNo} = n_1)) \quad [15]$

$a: \ \mathsf{SNo} = n_1 \quad [16]$

$a: \ \neg(\mathsf{A}\Box(\mathsf{SNo} = n_1)) \quad [17]$

$q : [\,a, \emptyset, \infty] \quad [18]$

$a: \ q\ \neg\Box(\mathsf{SNo} = n_1) \quad [19]$

$a: \ \neg(\mathsf{SNo} = n_1) \quad [20]$

$\Box \ (16,20)$

$a: \ (q)\neg\Box(\mathsf{SNo} = n_1) \quad [21]$

mit Korollar 5, Teil 1:

$a: \ \mathsf{ready} = \mathsf{true} \rightarrow \mathsf{A}\Box(\mathsf{ready} = \mathsf{true}) \quad [22]$

$a: \ \neg(\mathsf{ready} = \mathsf{true}) \quad [23]$

$a: \ \mathsf{A}\Box(\mathsf{ready} = \mathsf{true}) \quad [24]$

$a: \ \mathsf{ready} = \mathsf{true} \quad [25]$

$a: \ (\mathsf{A})\Box(\mathsf{ready} = \mathsf{true}) \quad [26]$

auf q:

$q : [\,a, \{\mathsf{ready} = \mathsf{true}\}, \infty] \quad [27]$

$\hookrightarrow$ S. 259

$\vdots$

von [27] (S. 258):

$q : [a, \{\mathsf{ready} = \mathsf{true}\}, \infty]$ [27]

$a :$ $\mathsf{ready} = \mathsf{true}$ [13]

$a :$ $\mathsf{SNo} = n_1$ [16]

$a :$ $(q)\neg\Box(\mathsf{SNo} = n_1)$ [21]

[21] auf q:

$q : [a, \{\mathsf{ready} = \mathsf{true}, \mathsf{SNo} = n_1\}, b, \{\mathsf{ready} = \mathsf{true}\}, \infty]$ [28]

$b :$ $\mathsf{ready} = \mathsf{true}$ [29]

$b :$ $\neg(\mathsf{SNo} = n_1)$ [30]

Vorgängerknoten von b betrachten:

$q : [a, \circ, b, \{\mathsf{ready} = \mathsf{true}\}, \infty]$ [31]

wie [32] mit 0 anstelle b und
$a :$ $\mathsf{ready} = \mathsf{true}$ [13]
$a :$ $\mathsf{SNo} = n_1$ [16]

$q : [a, \{\mathsf{ready} = \mathsf{true}, \mathsf{SNo} = n_1\}, c, \circ, b, \{\mathsf{ready} = \mathsf{true}\}, \infty]$ [32]

$c :$ $\mathsf{ready} = \mathsf{true}$ [33]

$c :$ $\mathsf{SNo} = n_1$ [34]

aus SNo:

$c :$ $\forall N : \mathsf{SNo} = N \rightarrow \mathsf{A}(\mathsf{SNo} = N \text{ unless}^+ \text{ ProcAck} = \mathsf{true})$ [35]

$c :$ $\mathsf{SNo} = N_2 \rightarrow \mathsf{A}(\mathsf{SNo} = N_2 \text{ unless}^+ \text{ ProcAck} = \mathsf{true})$ [36]

$c :$ $\neg(\mathsf{SNo} = N_2)$ [37]

$\Box$ $\{N_2 \leftarrow n_1\}(34, 37)$

$c :$ $\mathsf{A}(\mathsf{SNo} = n_1 \text{ unless}^+ \text{ ProcAck} = \mathsf{true})$ [38]

$c :$ $(\mathsf{A})(\mathsf{SNo} = n_1 \text{ unless ProcAck} = \mathsf{true})$ [39]

auf q:

$b :$ $\mathsf{A}(\mathsf{SNo} = n_1 \text{ unless ProcAck} = \mathsf{true})$ [40]

$a :$ $\mathsf{ProcAck} = \mathsf{true}$ [41]

aus PA1:

$c :$ $\mathsf{SIM} = \mathsf{msg}(d_3, b_3)$ [45]

$c :$ $\mathsf{SBit} = b_3$ [46]

$c :$ $\mathsf{RQ} = q_3$ [47]

$c :$ $\mathsf{SNo} = n_3$ [48]

aus PA2 (mit $c :$ $\mathsf{SNo} = n_1$ [34]):

$b :$ $\mathsf{SFile}(s(n_1)) \neq \bot$ [49]

$b :$ $\mathsf{RQ} = q_3 | \mathsf{msg}(\mathsf{SFile}(s(n_1)), \mathsf{flip}(b_3))$ [50]

$b :$ $\mathsf{SNo} = s(n_1)$ [51]

$b :$ $\mathsf{SBit} = \mathsf{flip}(b_3)$ [52]

$b :$ $\mathsf{ready} = \mathsf{false}$ [53]

$\Box$ $(29, 53)$

$b :$ $\mathsf{SFile}(s(n_1)) = \bot$ [54]

$b :$ $\mathsf{RQ} = q_3$ [55]

$b :$ $\mathsf{SNo} = n_1$ [56]

$b :$ $\mathsf{SBit} = b_3$ [57]

$b :$ $\mathsf{ready} = \mathsf{true}$ [58]

$\Box$ $(30, 56)$

$b :$ $\mathsf{SNo} = n_1$ [42]

$b :$ $\neg(\mathsf{ProcAck} = \mathsf{true})$ [43]

$b :$ $(\mathsf{A})(\mathsf{SNo} = n_1 \text{ unless ProcAck} = \mathsf{true})$ [44]

$\Box$ $(30, 42)$

Beweis von 3:

$$0: \ \mathsf{ready} = \mathsf{false} \quad [2]$$
$$0: \ \neg(\mathsf{A}\Box(\mathsf{ready} = \mathsf{true} \to (\forall D, N : \mathsf{RFile}(N) = D \to \mathsf{A}\Box(\mathsf{RFile}(N) = D)))) \quad [3]$$
$$p : [\,0, \emptyset, \infty] \quad [4]$$
$$0: \ p\ \neg(\Box(\mathsf{ready} = \mathsf{true} \to (\forall D, N : \mathsf{RFile}(N) = D \to \mathsf{A}\Box(\mathsf{RFile}(N) = D)))) \quad [5]$$

$$0: \ \neg(\mathsf{ready} = \mathsf{true} \to (\ldots)) \quad [6]$$
$$0: \ \mathsf{ready} = \mathsf{true} \quad [9]$$
$$0: \ \neg(\ldots) \quad [10]$$
$$\Box\ (2, 9)$$

$$0: \ \mathsf{ready} = \mathsf{true} \to (\forall D, N : \mathsf{RFile}(N) = D \to \mathsf{A}\Box(\mathsf{RFile}(N) = D)) \quad [7]$$
$$0: \ (p)\neg(\Box(\mathsf{ready} = \mathsf{true} \to (\forall D, N : \mathsf{RFile}(N) = D \to \mathsf{A}\Box(\mathsf{RFile}(N) = D)))) \quad [8]$$

$$p : [\,0, \{\mathsf{ready} = \mathsf{true} \to (\ldots)\}, a, \emptyset, \infty] \quad [11]$$
$$a: \ \neg(\mathsf{ready} = \mathsf{true} \to (\forall D, N : \mathsf{RFile}(N) = D \to \mathsf{A}\Box(\mathsf{RFile}(N) = D))) \quad [12]$$
$$a: \ \mathsf{ready} = \mathsf{true} \quad [13]$$
$$a: \ \neg(\forall D, N : \mathsf{RFile}(N) = D \to \mathsf{A}\Box(\mathsf{RFile}(N) = D)) \quad [14]$$
$$a: \ \neg(\mathsf{RFile}(n_1) = d_1 \to \mathsf{A}\Box(\mathsf{RFile}(n_1) = d_1)) \quad [15]$$
$$a: \ \mathsf{RFile}(n_1) = d_1 \quad [16]$$
$$a: \ \neg\mathsf{A}\Box(\mathsf{RFile}(n_1) = d_1) \quad [17]$$
$$q : [\,a, \emptyset, \infty] \quad [18]$$
$$a: \ q\ \neg\Box(\mathsf{RFile}(n_1) = d_1) \quad [19]$$

$$a: \ \neg(\mathsf{RFile}(n_1) = d_1) \quad [20]$$
$$\Box\ (16, 20)$$

$$a: \ (q)\neg(\Box\mathsf{RFile}(n_1) = d_1) \quad [21]$$

mit Korollar 5, Teil 1:

$$a: \ \mathsf{ready} = \mathsf{true} \to \mathsf{A}\Box(\mathsf{ready} = \mathsf{true}) \quad [22]$$

$$a: \ \neg(\mathsf{ready} = \mathsf{true}) \quad [23]$$
$$\Box\ (13, 23)$$

$$a: \ \mathsf{A}\Box(\mathsf{ready} = \mathsf{true}) \quad [24]$$
$$a: \ \mathsf{ready} = \mathsf{true} \quad [25]$$
$$a: \ (\mathsf{A})\Box(\mathsf{ready} = \mathsf{true}) \quad [26]$$

auf q:

$$q : [\,a, \{\mathsf{ready} = \mathsf{true}\}, \infty] \quad [27]$$

$\hookrightarrow$ S. 261

$\vdots$

von [27] (S. 260):

$q : [\,a, \{\mathsf{ready} = \mathsf{true}\}, \infty]$ [27]

$a :$ $\mathsf{ready} = \mathsf{true}$ [13]

$a :$ $\mathsf{RFile}(n_1) = d_1$ [16]

$a :$ $(q)\neg\Box(\mathsf{RFile}(n_1) = d_1)$ [21]

[21] auf q:

$q : [\,a, \{\mathsf{ready} = \mathsf{true}, \mathsf{RFile}(n_1) = d_1\}, b, \{\mathsf{ready} = \mathsf{true}\}, \infty]$ [28]

$b :$ $\mathsf{ready} = \mathsf{true}$ [29]

$b :$ $\neg(\mathsf{RFile}(n_1) = d_1)$ [30]

Vorgängerknoten von b betrachten:

$q : [\,a, \circ, b, \{\mathsf{ready} = \mathsf{true}\}, \infty]$ [31]

wie [32] mit 0 anstelle b und
$a :$ $\mathsf{ready} = \mathsf{true}$ [13]
$a :$ $\mathsf{RFile}(n_1) = d_1$ [16]

$q : [\,a, \{\mathsf{ready} = \mathsf{true}, \mathsf{SNo} = n_1\},$ [32]
$c, \circ, b, \{\mathsf{ready} = \mathsf{true}\}, \infty]$

$c :$ $\mathsf{ready} = \mathsf{true}$ [33]

$c :$ $\mathsf{RFile}(n_1) = d_1$ [34]

aus RData:

$c :$ $\forall D, N : \mathsf{RFile}(N) = D \rightarrow \mathsf{A}(\mathsf{RFile}(N) = D \ \mathsf{unless}^+ \ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(N)))$ [35]

$c :$ $\mathsf{RFile}(N_2) = D_2 \rightarrow \mathsf{A}(\mathsf{RFile}(N_2) = D_2 \ \mathsf{unless}^+ \ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(N_2)))$ [36]

$c :$ $\neg(\mathsf{RFile}(N_2) = D_2)$ [37]

$\Box\ \{N_2 \leftarrow n_1,\ D_2 \leftarrow d_1\}(34, 37)$

$c :$ $\mathsf{A}(\mathsf{RFile}(n_1) = d_1 \ \mathsf{unless}^+$ [38]
$(\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)))$

$c :$ $(\mathsf{A})(\mathsf{RFile}(n_1) = d_1 \ \mathsf{unless} \ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)))$ [39]

auf p:

$b :$ $\mathsf{A}(\mathsf{RFile}(n_1) = d_1 \ \mathsf{unless} \ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)))$ [40]

$b :$ $\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1)$ [41]

$b :$ $\mathsf{AccDat} = \mathsf{true}$ [45]

$b :$ $\mathsf{RNo} = s(n_1)$ [46]

$\hookrightarrow$ S. 262

$b :$ $\mathsf{RFile}(n_1) = d_1$ [42]

$b :$ $\neg(\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1))$ [43]

$b :$ $(\mathsf{A})(\mathsf{RFile}(n_1) = d_1 \ \mathsf{unless}$ [44]
$(\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(n_1))$

$\Box\ (30, 42)$

$$\vdots$$

von [46] (S. 261):

$$q : [a, \{\mathsf{ready} = \mathsf{true}, \mathsf{SNo} = n_1\}, c, \circ, b, \{\mathsf{ready} = \mathsf{true}\}, \infty] \quad [32]$$
$$b : \ \mathsf{ready} = \mathsf{true} \quad [29]$$
$$b : \ \neg(\mathsf{RFile}(n_1) = d_1) \quad [30]$$
$$c : \ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \quad [38]$$
$$c : \ \forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \to B = \mathsf{SBit} \quad [39]$$
$$b : \ \mathsf{AccDat} = \mathsf{true} \quad [45]$$

aus Korollar 2:

$$b : \ \mathsf{ready} = \mathsf{true} \to (\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \quad [47]$$
$$(\forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \to B = \mathsf{SBit}) \wedge$$
$$(\forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \to B' = \mathsf{SBit}))$$

$$b : \ \neg(\mathsf{ready} = \mathsf{true}) \quad [48]$$
$$\square \ (29, 48)$$

$$b : \ \mathsf{SFile}(s(\mathsf{SNo})) = \bot \quad [49]$$
$$b : \ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \quad [50]$$
$$b : \ \forall D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \to B = \mathsf{SBit} \quad [51]$$
$$b : \ \forall D', B', Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D', B')|Q' \to B' = \mathsf{SBit} \quad [52]$$

aus AD1:

$$c : \ (\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \to (\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = B) \quad [53]$$

$$c : \ \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [54]$$
$$c : \ (\mathsf{A})\circ\neg(\mathsf{AccDat} = \mathsf{true}) \quad [55]$$

auf p:

$$b : \ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [56]$$
$$\square \ (45, 56)$$

$$b : \ \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = B \quad [57]$$
$$b : \ \mathsf{RIM} = \mathsf{msg}(d_3, b_3) \wedge \mathsf{RBit} = b_3 \quad [58]$$
$$b : \ \mathsf{RIM} = \mathsf{msg}(d_3, b_3) \quad [59]$$
$$b : \ \mathsf{RBit} = b_3 \quad [60]$$

aus [51]:

$$b : \ \mathsf{RIM} = \mathsf{msg}(D_4, B_4) \to B_4 = \mathsf{SBit} \quad [61]$$

$$b : \ \neg(\mathsf{RIM} = \mathsf{msg}(D_4, B_4)) \quad [62]$$
$$\square \ \{D_4 \leftarrow d_3, \ B_4 \leftarrow b_3\}(59, 62)$$

$$b : \ b_3 = \mathsf{SBit} \quad [63]$$

$$\boxed{\begin{array}{ll} \square : & b : \ \mathsf{RBit} = b_3 \quad [60] \\ & b : \ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \quad [50] \end{array}}$$

17 Lemma 7: Verhalten von RQ

Nachdem bisher über Induktion einige Aussagen bewiesen wurden, die sich mehr mit den statischen Eigenschaften beschäftigen, ist es nun an der Zeit, das Aussagen über das dynamische Verhalten des Protokolls zu machen.

An dieser Stelle gewinnt auch der Einsatz von Temporallogik und insbesondere Fairness an Bedeutung. Damit erfolgt ab hier auch der Einsatz der in [May95], Abschnitt 9 genannten Gleichungsbehandlung und Optimierungen. In den verwendeten Axiomen und schon bewiesenen Lemmata wird an geeigneten Stellen der ∇-Quantor anstelle des $\forall$-Quantors eingesetzt.

Für Fairness wird das Schema aus [May95], S. 135 verwendet:

$$\text{Fairness von } \lambda \text{ bzgl. } R\text{:}$$
$$0: \ \mathsf{R}(\Diamond\Box\mathsf{A}\circ\neg R \vee \Diamond\circ R) \quad [*1*]$$

$$\alpha: \ \lambda\Diamond^{+}\lambda\Box\mathsf{A}\circ\neg R \quad [*2*]$$
$$\text{bzw.}$$
$$\alpha: \ (\lambda)\Diamond\lambda\Box\mathsf{A}\circ\neg R \quad [*2*]$$
$$\text{bzw.}$$
$$\alpha: \ (\lambda)\Diamond(\neg\lambda\Diamond\mathsf{E}\circ R) \quad [*2*]$$
$$\vdots$$

$$\alpha: \ (\lambda)\Diamond R \quad [*3*]$$
$$\vdots$$

Als erstes muß man sich mit dem Problem beschäftigen, Aussagen über das Verhalten der Schlangen RQ und SQ zu erhalten.

Diese dienen der Nachrichten- bzw. Informationsübermittlung. Dabei ist es notwendig, diese Begriffe zu unterscheiden: Eine Information ist „ein Stück Wissen“, sie ist nicht physikalisch vorhanden, sondern „einfach da“. Im Gegensatz dazu ist eine Nachricht physikalisch vorhanden, sie enthält aber wiederum nicht unmittelbar Information. Diese gewinnt erst der Empfänger, wenn er die Nachricht erhält und sie – nach einem mit dem Sender vereinbarten Verfahren – entschlüsselt oder zur weiteren Verwendung ablegt.

Im vorliegenden Fall enthalten $\mathsf{SFile}(0)$, $\mathsf{SFile}(1)$, … Information (sowohl durch ihren Inhalt, als auch durch ihre Reihenfolge) – die aber als solche für das Protokoll irrelevant ist, wichtig ist nur, daß sie komplett und in der richtigen Reihenfolge übertragen wird. Um dies zu ermöglichen müssen Sender und Empfänger weitere Informationen über ihren aktuellen Zustand in Form der Kontrollbits austauschen. Aus Sicht des Senders ergibt sich damit in jedem Zustand die folgende Situation: Er will die Information „Es soll d übertragen werden und mein Kontrollbit ist b“ an dem Empfänger weitergeben. Dies geschieht über eine bzw. viele Nachrichten der Form $\mathsf{msg}(d, b)$. Erhält der Empfänger diese, so weiß er, daß dabei d eine Informationseinheit ist, die nicht ver-, sondern nur bearbeitet, d.h. aus SFile nach RFile übertragen werden muß, und b als Kontrollbit eine direkte Information für ihn darstellt.

Damit ist klar, daß die Aufgabe von RQ nicht die Übertragung einer Nachricht $\mathsf{msg}(d, b)$, sondern die Übertragung der o.g. Information ist.

Entsprechend wird die nächste größere Aussage nicht lauten „Wenn eine Nachricht msg(d, b) vom Sender abgeschickt wird, kommt sie irgendwann beim Empfänger an“ (diese Aussage wäre falsch, denn eine Nachricht kann auf dem Weg durch SLose verloren gehen), sondern „Wenn der d übertragen werden soll und das Kontrollbit des Senders b ist, kommt diese Information irgendwann beim Empfänger an“.

Für den Beweis stellt sich das Problem, daß eine Aussage für unendlich viele verschiedene Situationen bewiesen werden muß: Man weiß (fast) keine Details über RQ im Moment des Sendens, insbesondere nicht, wieviele Nachrichten RQ enthält.

Es ist also erforderlich, eine Aussage für alle RQ zu machen. Da RQ beliebig lang ist, kommt nur Induktion in Frage. Der Versuch, dabei über die Länge von RQ zu induzieren, ist fruchtlos, also muß man unter Betrachtung der Situation anders vorgehen:

Der Sender will die Information „Ich will d übertragen und mein Kontrollbit ist b“ an den Empfänger übertragen. Bevor er nicht sicher ist, daß dies geschehen ist, macht er nichts anderes, insbesondere bleibt SBit $= b$ unverändert. Mit ReTrans werden geduldig entsprechende Nachrichten msg(d, b) gesendet.

Aufgrund der Fairness nimmt der Empfänger mit RecCom Nachrichten vom Kopf von RQ weg. Da nun RQ nur endlich viele „alte“ Nachrichten mit SBit $=$ flip(b) enthält und diese nach Lemma 1 alle vorne in RQ liegen, sind diese irgendwann alle aus RQ entfernt. Mit ReTrans werden immer weiter Nachrichten msg(d, b) an RQ angehängt, sodaß der Empfänger mit RecCom irgendwann eine solche entgegennimmt - womit er die beabsichtigte Information enthält.

Entsprechend induziert man über die Anzahl der „alten“ Nachrichten, deren Kontrollbit flip(b) ist, wobei man diese nur grob nach oben abschätzt.

Der Induktionsschritt hat folgenden Inhalt:

Sei n gegeben. Nach Induktionsvoraussetzung ist in allen Zuständen jedes RQ, das höchstens $n-1$ „alte“ Nachrichten enthält, in obigem Sinne abbaubar. Dann ist in allen Zuständen auch jedes RQ, das n „alte“ Nachrichten enthält abbaubar: Eine Nachricht aus RQ, nämlich die erste, wird in absehbarer Zeit sicher durch RecCom entfernt. Hat sie noch Kontrollbit flip(SBit), so kann man sich auf die Induktionsvoraussetzung abstützen, hat sie schon Kontrollbit b, so ist das Ziel direkt erreicht.

Dazu werden die folgenden Konstanten in die Extended Evolving Algebra aufgenommen:

$$\begin{array}{ll} \mathsf{ARSB}, & \mathsf{ASSB} \\ \mathsf{ARfSB}, & \mathsf{ASfSB} \end{array}$$

Im Startzustand sind sie mit dem Wert Null initialisiert.

A R/S (f) SB $= n$ bedeutet dabei, daß RQ bzw. SQ maximal n Nachrichten mit Kontrollbit SBit bzw. flip(SBit) enthält. Die Abschätzung nach oben wird gemacht, um SLose von der Veränderung dieser Konstanten auszunehmen, da solche Veränderungen im gemeinsamen Wissen der kontrollierbaren Instanzen nicht enthalten sind.

Entsprechend kommen die folgenden Übergangsregeln hinzu. Dabei ist zu berücksichtigen, daß verschiedene Regeln gleichzeitig schreibend auf die neuen Konstanten zugreifen können. Dies betrifft insbesondere

$\mathsf{ProcAck}$ bei dem die Werte für $\mathsf{flip(SBit)}$ und SBit vertauscht werden. Da in den Beweisen nur Fälle betrachtet werden, in denen $\mathsf{ProcAck}$ nicht angewendet wird werden die Regeln nur für diese Fälle formuliert. Die vollständige Formulierung ist Routine. Der gegenseitige Ausschluß bezüglich des Zugriffs auf RQ verhindert im übrigen eine parallele Ausführung von RecCom und $\mathsf{ProcAck}$.

$$\begin{array}{ll}
\text{RC3:} & \forall D,B : \nabla ARSB, ARfSB : \mathsf{A}\circ(\ (\mathsf{RecCom} = \mathsf{true} \wedge \neg(\mathsf{ProcAck} = \mathsf{true}) \wedge \mathsf{RIM} = \mathsf{msg}(D,B)) \rightarrow \\
& \qquad ((B = \mathsf{SBit} \rightarrow (\mathsf{ARSB} = p(ARSB) \wedge \mathsf{ARfSB} = ARfSB)) \wedge \\
& \qquad\ (B = \mathsf{flip(SBit)} \rightarrow (\mathsf{ARSB} = ARSB \wedge \mathsf{ARfSB} = p(ARfSB)))))
\end{array}$$

$$\begin{array}{ll}
\text{SC3:} & \forall D,B : \nabla ASSB, ASfSB : \mathsf{A}\circ(\ (\mathsf{SendCom} = \mathsf{true} \wedge \neg(\mathsf{ProcAck} = \mathsf{true}) \wedge \mathsf{SIM} = \mathsf{msg}(D,B)) \rightarrow \\
& \qquad ((B = \mathsf{SBit} \rightarrow (\mathsf{ASSB} = p(ASSB) \wedge \mathsf{ASfSB} = ASfSB)) \wedge \\
& \qquad\ (B = \mathsf{flip(SBit)} \rightarrow (\mathsf{ASSB} = ASSB \wedge \mathsf{ASfSB} = p(ASfSB)))))
\end{array}$$

$$\begin{array}{ll}
\text{PA3:} & \nabla ARSB, ARfSB : \mathsf{A}\circ(\ (\mathsf{ProcAck} = \mathsf{true} \wedge \neg(\mathsf{SendCom} = \mathsf{true})) \rightarrow \\
& \qquad ((\neg ready \rightarrow (\mathsf{ARSB} = s(ARfSB) \wedge \mathsf{ARfSB} = ARSB)) \wedge \\
& \qquad\ (\mathsf{ready} \rightarrow (\mathsf{ARSB} = ARSB \wedge \mathsf{ARfSB} = ARfSB))))
\end{array}$$

$$\text{RT3:} \quad \nabla ARSB, ARfSB : \mathsf{A}\circ(\mathsf{ReTrans} = \mathsf{true} \rightarrow (\mathsf{ARSB} = s(ARSB) \wedge \mathsf{ARfSB} = ARfSB))$$

$$\begin{array}{ll}
\text{AM3:} & \forall D,B : \nabla ASSB, ASfSB : \\
& \quad \mathsf{RIM} = \mathsf{msg}(D,B) \rightarrow \mathsf{A}\circ(\ (\mathsf{AckMsg} = \mathsf{true} \wedge \neg(\mathsf{ProcAck} = \mathsf{true})) \rightarrow \\
& \qquad ((B = \mathsf{SBit} \rightarrow (\mathsf{ASSB} = s(ASSB) \wedge \mathsf{ASfSB} = ASfSB)) \wedge \\
& \qquad\ (B = \mathsf{flip(SBit)} \rightarrow (\mathsf{ASSB} = ASSB \wedge \mathsf{ASfSB} = s(ASfSB)))))
\end{array}$$

Daß man bei $\mathsf{ProcAck}$ nicht das Wissen aus Lemma 1 anwendet, daß nach Anwendung von $\mathsf{ProcAck}$ die neue Nachricht die einzige mit $\mathsf{Bit}(m) = \mathsf{SBit}$ und damit $\mathsf{ASSB} = 0$ und $\mathsf{ARSB} = 1$ ist, hat den Grund, daß man das beim Design der EEA noch nicht weiß – es beeinträchtigt den Beweis auch in keiner Weise.

Schließlich benötigt man noch die Invarianzaussagen

$$\begin{array}{ll}
\text{RQS:} & \nabla ARSB : \mathsf{A}(\mathsf{ARSB} = ARSB \ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true}) \\
\text{SQS:} & \nabla ASSB : \mathsf{A}(\mathsf{ASSB} = ASSB \ \mathsf{unless}^+ \\
& \qquad ((\mathsf{AckMsg} = \mathsf{true} \wedge \mathsf{RBit} = \mathsf{SBit}) \vee \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})) \\
\text{RQF:} & \nabla ARfSB : \mathsf{A}(\mathsf{ARfSB} = ARfSB \ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}) \\
\text{SQF:} & \nabla ARfSB : \mathsf{A}(\mathsf{ASfSB} = N \ \mathsf{unless}^+ \\
& \qquad ((\mathsf{AckMsg} = \mathsf{true} \wedge \mathsf{RBit} = \mathsf{SBit}) \vee \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}))
\end{array}$$

Des weiteren gelten die folgenden Formeln:

$$\begin{array}{ll}
\text{RQ0:} & \mathsf{ARSB} = 0 \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D,Q : \mathsf{RQ} = \mathsf{msg}(D, \mathsf{flip(SBit)})|Q) \\
\text{RQ0F:} & \mathsf{ARfSB} = 0 \rightarrow (\mathsf{RQ} = \varepsilon \vee \exists D,Q : \mathsf{RQ} = \mathsf{msg}(D, \mathsf{SBit})|Q) \\
\text{SQ0:} & \mathsf{ASSB} = 0 \rightarrow (\mathsf{SQ} = \varepsilon \vee \exists Q : \mathsf{SQ} = \mathsf{msg}(\lambda, \mathsf{flip(SBit)})|Q) \\
\text{SQ0F:} & \mathsf{ASfSB} = 0 \rightarrow (\mathsf{SQ} = \varepsilon \vee \exists Q : \mathsf{SQ} = \mathsf{msg}(\lambda, \mathsf{SBit})|Q)
\end{array}$$

Aussage von Lemma 7: Unter Fairnessannahmen gilt

$$\forall N : \mathsf{A}\Box(\forall D : \nabla SBit : (\mathsf{ARfSB} = N \wedge \mathsf{SFile}(\mathsf{SNo}) = D) \rightarrow$$
$$\rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D, SBit)))$$

In dieser Form wird das Lemma bewiesen. Da N dabei ein reiner Hilfsparameter ist, erhält man die Aussagen:

$$\mathsf{A}\Box(\forall D : \nabla SBit : \mathsf{SFile}(\mathsf{SNo}) = D \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D, SBit)))$$

$$\mathsf{A}\Box(\nabla SBit, SFile, SNo : \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(SFile(SNo), SBit)))$$

Beweis:

Der Beweis verwendet Induktion über die natürlichen Zahlen.

Mit $A(n)$ wird die Induktionsaussage der Behauptung für festes n bezeichnet, mit $B(n)$ die darin enthaltene modallogische Aussage für einen festen Zustand.

Induktionsanfang $\mathsf{ARfSB} = 0$: [2]. Es gibt also einen Zustand a, in dem die Aussage für 0 nicht gilt. Aus der Annahme, daß nach a ProcAck nicht mehr angewendet wird ergibt sich ([22]-[38]), daß SFile, SBit und SNo nicht mehr verändert werden.
ARfSB ändert sich nur bei Anwendung von RecCom oder ProcAck. Wird RecCom angewendet [50], so wird dabei wegen $\mathsf{ARfSB} = 0$ eine Nachricht (d_5, SBit) mit Kontrollbit SBit von der Spitze von RQ nach RIM eingelesen. Nach Lemma 5 ist dann auch $d_5 = \mathsf{SFile}(\mathsf{SNo})$.

Die Annahme, daß RecCom nie ausgeführt wird, ist unfair [87]: Es müßte einen Zustand e geben, ab dem RecCom nie mehr ausführbar ist.

Ist $\mathsf{RIM}_e = \perp$ [96], so ist RIM in allen Folgezuständen gleich $\perp$, da AckMsg nicht anwendbar ist, und RecCom nach Annahme nicht anwendbar sein soll ([101] ff.). ReTrans ist immer anwendbar, wird also irgendwann in einem Zustand i auch ausgeführt [130], womit dann $\mathsf{RQ}_i \neq \varepsilon$ ist, also RecCom ausführbar wäre.

Ist $\mathsf{RIM}_e \neq \perp$ [145], so bleibt $\mathsf{RIM} \neq \perp$, bis AckMsg ausgeführt wird [155]. Dies führt zu einem Folgezustand k, in dem $\mathsf{RIM}_k = \perp$ [172] ist, womit man nun genau so weit ist, wie eben mit e [94]. Die Annahme, AckMsg würde nie ausgeführt [153], ist ebenfalls unfair: Es müßte einen Folgezustand m geben, ab dem AckMsg nie mehr ausführbar ist. Da $\mathsf{RIM}_m \neq \perp$ ist, muß also $\mathsf{Bit}(\mathsf{RIM}_m) \neq \mathsf{flip}(\mathsf{RBit}_m)$ sein [187]. Damit ist – und bleibt – AccDat ausführbar [226] und muß aus Fairnessgründen auch irgendwann ausgeführt werden [194], wobei RBit geflippt wird, also danach $\mathsf{Bit}(\mathsf{RIM}) = \mathsf{flip}(\mathsf{RBit})$ ist und AckMsg ausführbar wäre.

Der Induktionsschritt verläuft ganz analog. Wie oben *muß* RecCom irgendwann ausgeführt werden [50+]. Dabei wird eine Nachricht $\mathsf{RIM} = (d, b)$ gelesen. Ist $b = \mathsf{SBit}$ [262], so ist nach Lemma 5 bereits $d = \mathsf{SFile}(\mathsf{SNo})$. Ist $b = \mathsf{flip}(\mathsf{SBit})$, so ist danach $\mathsf{ARfSB} \leq p(s(n_0)) = n_0$[264] und nach Induktionsvoraussetzung für n_0 ein Zustand w' erreichbar, in dem RIM den gewünschten Inhalt hat.

$$0:\ \neg(\forall N : A(N)) \quad [1]$$

$$0:\ \neg(A(0)) \quad [2]$$

$$0:\ \neg(\mathsf{A}\Box(\forall D : \nabla SBit : (\mathsf{ARfSB} = 0 \land \mathsf{SFile(SNo)} = D) \to \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(D, SBit)))) \quad [5]$$

$$p : [\,0, \emptyset, \infty] \quad [6]$$

$$0:\ p\,\neg(\Box(\forall D : \nabla SBit : (\mathsf{ARfSB} = 0 \land \mathsf{SFile(SNo)} = D) \to \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(D, SBit)))) \quad [7]$$

$$0:\ \neg(\forall D : \nabla SBit : (\mathsf{ARfSB} = 0 \land \mathsf{SFile(SNo)} = D) \to \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(D, SBit))) \quad [8]$$

$\boxed{\text{wie [9] ff. mit 0 anstelle } a}$

$$0:\ (p)\neg(\Box(\forall D : \nabla SBit : (\mathsf{ARfSB} = 0 \land \mathsf{SFile(SNo)} = D) \to \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(D, SBit)))) \quad [9]$$

$$p : [\,0, \{B(0)\}, a, \emptyset, \infty] \quad [10]$$

$$a:\ \neg(\forall D : \nabla SBit : (\mathsf{ARfSB} = 0 \land \mathsf{SFile(SNo)} = D) \to \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(D, SBit))) \quad [11]$$

$$a:\ \neg(\nabla SBit : (\mathsf{ARfSB} = 0 \land \mathsf{SFile(SNo)} = d_1) \to \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(d_1, SBit))) \quad [12]$$

$$a:\ \neg((\mathsf{ARfSB} = 0 \land \mathsf{SFile(SNo)} = d_1) \to \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a))) \quad [13]$$

$$a:\ \mathsf{ARfSB} = 0 \land \mathsf{SFile(SNo)} = d_1 \quad [14]$$

$$a:\ \neg\mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)) \quad [15]$$

$$a:\ \mathsf{ARfSB} = 0 \quad [16]$$

$$a:\ \mathsf{SFile(SNo)} = d_1 \quad [17]$$

$$\mathsf{ARfSB}_a = 0 \quad [16']$$

$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [17']$$

$$q : [\,a, \emptyset, \infty] \quad [18]$$

$$a:\ q\neg\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)) \quad [19]$$

$$a:\ (q)\Box\neg(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)) \quad [20]$$

$$q : [\,a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \lor \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a))\}, \infty] \quad [21]$$

↪ S. 269

$$0:\ A(n_0) \quad [3]$$

$$0:\ \neg(A(s(n_0))) \quad [4]$$

↪ S. 282

$$\vdots$$

von [21] (S. 268):

$$q : [\,a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a))\}, \infty] \quad [21]$$
$$\mathsf{ARfSB}_a = 0 \quad [16']$$
$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [17']$$

aus SData:

$$a : \ \forall D, N : \mathsf{SFile}(N) = D \to \mathsf{A}\Box(\mathsf{SFile}(N) = D) \quad [22]$$
$$a : \ \mathsf{SFile}(N_2) = D_2 \to \mathsf{A}\Box(\mathsf{SFile}(N_2) = D_2) \quad [23]$$

$$a : \ \neg(\mathsf{SFile}(N_2) = D_2) \quad [24]$$
$$\mathsf{SFile}_a(N_2) \neq D_2 \quad [24']$$
$$\Box \ \{N_2 \leftarrow \mathsf{SNo}_a, D_2 \leftarrow d_1\}(17', 24')$$

$$a : \ \mathsf{A}\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1) \quad [25]$$
$$a : \ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [26]$$
$$a : \ (\mathsf{A})\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1) \quad [27]$$

$$q : [\,a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, (\mathsf{A})\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1)\}, \infty] \quad [28]$$

aus SBit:

$$a : \ \nabla SBit : \mathsf{A}(\mathsf{SBit} = SBit \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [29]$$
$$a : \ \mathsf{A}(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [30]$$
$$a : \ (\mathsf{A})(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}) \quad [31]$$

aus SNo:

$$a : \ \nabla SNo : \mathsf{A}(\mathsf{SNo} = SNo \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [32]$$
$$a : \ \mathsf{A}(\mathsf{SNo} = \mathsf{SNo}_a \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [33]$$
$$a : \ (\mathsf{A})(\mathsf{SNo} = \mathsf{SNo}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}) \quad [34]$$

[31] und [34] auflösen:

$$q : [\,a, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \ldots\}, \quad [35]$$
$$b, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \ldots\}, \infty]$$

u.a.:

$$b : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [36]$$
$$b : \ \mathsf{ProcAck} = \mathsf{true} \quad [37]$$
$$\Box \ (36, 37)$$

$$q : [\,a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)), \quad [38]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a\}, \infty]$$

aus RQF:

$$a : \ \nabla \mathsf{ARfSB} : \mathsf{A}(\mathsf{ARfSB} = ARfSB \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}) \quad [39]$$
$$a : \ \mathsf{A}(\mathsf{ARfSB} = \mathsf{ARfSB}_a \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}) \quad [40]$$
$$a : \ (\mathsf{A})(\mathsf{ARfSB} = \mathsf{ARfSB}_a \ \mathsf{unless} \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}) \quad [41]$$

$\hookrightarrow$ S. 270

$$\vdots$$

von [41] (S. 269):

$$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a\}, \infty] \quad [38]$$

$$\mathsf{ARfSB}_a = 0 \quad [16']$$

$$a : \ (\mathsf{A})(\mathsf{ARfSB} = 0 \text{ unless } \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}) \quad [41]$$

$$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \quad [49]$$
$$\mathsf{SNo} = \mathsf{SNo}_a, \mathsf{ARfSB} = \mathsf{ARfSB}_a, \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\}, \infty]$$

$\hookrightarrow$ S. 273

$$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \quad [42]$$
$$\mathsf{ARfSB} = \mathsf{ARfSB}_a, \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\},$$
$$c, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \infty]$$

$$c : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [43]$$
$$c : \ \neg(\mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)) \quad [44]$$
$$c : \ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [45]$$
$$c : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [46]$$
$$c : \ \mathsf{SNo} = \mathsf{SNo}_a \quad [47]$$
$$c : \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true} \quad [48]$$

$$\mathsf{RIM}_c \neq \mathsf{msg}(d_1, \mathsf{SBit}_a) \quad [44']$$
$$\mathsf{SFile}_c(\mathsf{SNo}_a) = d_1 \quad [45']$$
$$\mathsf{SBit}_c = \mathsf{SBit}_a \quad [46']$$
$$\mathsf{SNo}_c = \mathsf{SNo}_a \quad [47']$$

$$c : \ \mathsf{RecCom} = \mathsf{true} \quad [50] \qquad\qquad c : \ \mathsf{ProcAck} = \mathsf{true} \quad [51]$$

$$\Box \ (43, 51)$$

Vorgängerzustand von c:

$$q : [\, a, \circ, c, \{\ldots\}, \infty] \quad [52]$$

$\boxed{\text{wie [53] mit } a \text{ anstelle } d.}$

$$q : [\, a, \{\ldots, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{ARfSB} = \mathsf{ARfSB}_a\}, \quad [53]$$
$$d, \circ, c, \{\ldots\}, \infty]$$

$$d : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [54]$$
$$d : \ \mathsf{ARfSB} = \mathsf{ARfSB}_a \quad [55]$$
$$\mathsf{SBit}_d = \mathsf{SBit}_a \quad [54']$$
$$\mathsf{ARfSB}_d = \mathsf{ARfSB}_a \quad [55']$$

$\hookrightarrow$ S. 271

$\vdots$

von [55] (S. 270):

$q : [\,a, \{\ldots, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{ARfSB} = \mathsf{ARfSB}_a\}, d, \circ, c, \{\ldots\}, \infty]$ [53]

$\mathsf{ARfSB}_a = 0$ [16′]

$\mathsf{RIM}_c \neq \mathsf{msg}(d_1, \mathsf{SBit}_a))$ [44′]

$\mathsf{SFile}_c(\mathsf{SNo}_a) = d_1$ [45′]

$\mathsf{SBit}_c = \mathsf{SBit}_a$ [46′]

$\mathsf{SNo}_c = \mathsf{SNo}_a$ [47′]

$c :\ \mathsf{RecCom} = \mathsf{true}$ [50]

$\mathsf{SBit}_d = \mathsf{SBit}_a$ [54′]

$\mathsf{ARfSB}_d = \mathsf{ARfSB}_a$ [55′]

aus RC1:

$d :\ \mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}) \to (\mathsf{RIM} = \bot \wedge \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q)$ [56]

$d :\ \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))$ [57]

$d :\ (\mathsf{A})\neg(\circ(\mathsf{RecCom} = \mathsf{true}))$ [60]

auf q:

$c :\ \neg(\mathsf{RecCom} = \mathsf{true})$ [61]

$\Box$ (50, 61)

$d :\ \mathsf{RIM} = \bot$ [58]

$d :\ \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q$ [59]

$d :\ \mathsf{RQ} = \mathsf{msg}(d_4, b_4)|q_4$ [62]

$\mathsf{RIM}_d = \bot$ [58′]

$\mathsf{RQ}_d = \mathsf{msg}(d_4, b_4)|q_4$ [62′]

aus RQ0F:

$d :\ \mathsf{ARfSB} = 0 \to (\mathsf{RQ} = \varepsilon \vee \exists D, Q : \mathsf{RQ} = \mathsf{msg}(D, \mathsf{SBit})|Q)$ [63]

$d :\ \neg(\mathsf{ARfSB} = 0)$ [64]

$\mathsf{ARfSB}_d \neq 0$ [64′]

$\Box :\ \mathsf{ARfSB}_d = \mathsf{ARfSB}_a$ [55′]

$\mathsf{ARfSB}_a = 0$ [16′]

$\mathsf{ARfSB}_d \neq 0$ [64′]

$d :\ \mathsf{RQ} = \varepsilon \vee \exists D, Q : \mathsf{RQ} = \mathsf{msg}(D, \mathsf{SBit})|Q$ [65]

$d :\ \mathsf{RQ} = \varepsilon$ [66]

$\mathsf{RQ}_d = \varepsilon$ [66′]

$\Box$ (E3, 62′, 66′)

$d :\ \exists D, Q : \mathsf{RQ} = \mathsf{msg}(D, \mathsf{SBit})|Q$ [67]

$d :\ \mathsf{RQ} = \mathsf{msg}(d_5, \mathsf{SBit}_d)|q_5$ [68]

$\mathsf{RQ}_d = \mathsf{msg}(d_5, \mathsf{SBit}_d)|q_5$ [68′]

aus RC2:

$d :\ \forall D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q \to \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \to \mathsf{RQ} = Q \wedge \mathsf{RIM} = \mathsf{msg}(D, B))$ [69]

$d :\ \mathsf{RQ} = \mathsf{msg}(D_6, B_6)|Q_6 \to \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \to \mathsf{RQ} = Q_6 \wedge \mathsf{RIM} = \mathsf{msg}(D_6, B_6))$ [70]

$d :\ \neg(\mathsf{RQ} = \mathsf{msg}(D_6, B_6)|Q_6)$ [71]

$\mathsf{RQ}_d \neq \mathsf{msg}(D_6, B_6)|Q_6)$ [71′]

$\Box\ \{D_6 \leftarrow d_5,\ B_6 \leftarrow \mathsf{SBit}_d,\ Q_6 \leftarrow q_5\}(68', 71')$

$d :\ \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \to$ [72]
$\mathsf{RQ} = q_5 \wedge \mathsf{RIM} = \mathsf{msg}(d_5, \mathsf{SBit}_d))$

$d :\ (\mathsf{A})\circ(\mathsf{RecCom} = \mathsf{true} \to$ [73]
$\mathsf{RQ} = q_5 \wedge \mathsf{RIM} = \mathsf{msg}(d_5, \mathsf{SBit}_d))$

↪ S. 272

$$\vdots$$

von [73] (S. 271):

$$p : [\,0, \{\ldots\}, a, \{\ldots, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{ARfSB} = \mathsf{ARfSB}_a\}, d, \circ, c, \{\ldots\}, \infty] \quad [53]$$
$$\mathsf{RIM}_c \neq \mathsf{msg}(d_1, \mathsf{SBit}_a)) \quad [44']$$
$$\mathsf{SFile}_c(\mathsf{SNo}_a) = d_1 \quad [45']$$
$$\mathsf{SBit}_c = \mathsf{SBit}_a \quad [46']$$
$$\mathsf{SNo}_c = \mathsf{SNo}_a \quad [47']$$
$$c : \ \mathsf{RecCom} = \mathsf{true} \quad [50]$$
$$\mathsf{SBit}_d = \mathsf{SBit}_a \quad [54']$$
$$d : \ (\mathsf{A})\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = q_5 \wedge \mathsf{RIM} = \mathsf{msg}(d_5, \mathsf{SBit}_d)) \quad [73]$$

auf q:

$$c : \ \mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = q_5 \wedge \mathsf{RIM} = \mathsf{msg}(d_5, \mathsf{SBit}_d) \quad [74]$$

Linker Zweig:

$$c : \ \neg(\mathsf{RecCom} = \mathsf{true}) \quad [75]$$
$$\Box \ (50, 75)$$

Rechter Zweig:

$$c : \ \mathsf{RQ} = q_5 \quad [76]$$
$$c : \ \mathsf{RIM} = \mathsf{msg}(d_5, \mathsf{SBit}_d) \quad [77]$$
$$\mathsf{RQ}_c = q_5 \quad [76']$$
$$\mathsf{RIM}_c = \mathsf{msg}(d_5, \mathsf{SBit}_d) \quad [77']$$

aus Lemma 5:

$$c : \ \forall D, B : (\mathsf{RIM} = \mathsf{msg}(D, B) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q') \rightarrow \quad [78]$$
$$((B = \mathsf{SBit} \rightarrow D = \mathsf{SFile}(\mathsf{SNo})) \wedge (B = \mathsf{flip}(\mathsf{SBit}) \rightarrow D = \mathsf{SFile}(p(\mathsf{SNo}))))$$
$$c : \ (\mathsf{RIM} = \mathsf{msg}(D_7, B_7) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_7, B_7)|Q') \rightarrow \quad [79]$$
$$((B_7 = \mathsf{SBit} \rightarrow D_7 = \mathsf{SFile}(\mathsf{SNo})) \wedge (B_7 = \mathsf{flip}(\mathsf{SBit}) \rightarrow D_7 = \mathsf{SFile}(p(\mathsf{SNo}))))$$

Linker Zweig:

$$c : \ \neg(\mathsf{RIM} = \mathsf{msg}(D_7, B_7)) \quad [80]$$
$$c : \ \neg(\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_7, B_7)|Q') \quad [81]$$
$$\mathsf{RIM}_c \neq \mathsf{msg}(D_7, B_7) \quad [80']$$
$$\Box \ \{D_7 \leftarrow d_5, \ B_7 \leftarrow \mathsf{SBit}_d\}(77', 80')$$

Rechter Zweig:

$$c : \ \mathsf{SBit}_d = \mathsf{SBit} \rightarrow d_5 = \mathsf{SFile}(\mathsf{SNo}) \quad [82]$$
$$c : \ \mathsf{SBit}_d = \mathsf{flip}(\mathsf{SBit}) \rightarrow d_5 = \mathsf{SFile}(p(\mathsf{SNo})) \quad [83]$$

Linker Unterzweig:

$$c : \ \neg(\mathsf{SBit}_d = \mathsf{SBit}) \quad [84]$$
$$\mathsf{SBit}_d \neq \mathsf{SBit}_c \quad [84']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{SBit}_c = \mathsf{SBit}_a \quad [46'] \\ & \mathsf{SBit}_d = \mathsf{SBit}_a \quad [54'] \end{array}}$$

Rechter Unterzweig:

$$c : \ d_5 = \mathsf{SFile}(\mathsf{SNo}) \quad [85]$$
$$d_5 = \mathsf{SFile}_c(\mathsf{SNo}_c) \quad [85']$$

$$\boxed{\begin{array}{ll} \Box : & d_5 = \mathsf{SFile}_c(\mathsf{SNo}_c) \quad [85'] \\ & \mathsf{SFile}_c(\mathsf{SNo}_a) = d_1 \quad [45'] \\ & \mathsf{SNo}_c = \mathsf{SNo}_a \quad [47'] \\ \hline & \rightarrow \ d_1 = d_5 \\ & \mathsf{RIM}_c \neq \mathsf{msg}(d_1, \mathsf{SBit}_a)) \quad [44'] \\ & \mathsf{RIM}_c = \mathsf{msg}(d_5, \mathsf{SBit}_d) \quad [77'] \\ & \mathsf{SBit}_d = \mathsf{SBit}_a \quad [54'] \\ \hline & \rightarrow \ d_1 \neq d_5 \end{array}}$$

$\vdots$

von [49] (S. 270):

$q : [\,a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a,$ [49]
$\mathsf{SNo} = \mathsf{SNo}_a, \mathsf{ARfSB} = \mathsf{ARfSB}_a, \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\}, \infty]$

Fairness bzgl. RecCom:
$0 :\ \mathsf{R}((\Box\Diamond\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})) \to (\Diamond(\mathsf{RecCom} = \mathsf{true})))$ [86]
auf q:

$a :\ (q)\Diamond(\neg(q\Diamond\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})))$ [87]

$q : [\,a, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\},$ [89]
$e, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\}, \infty]$

$e :\ \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [90]
$e :\ q\,\neg(\Diamond\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))$ [91]

$e :\ \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))$ [92]
$e :\ (q)\Box(\neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})))$ [93]

$a :\ (q)\Diamond(\mathsf{RecCom} = \mathsf{true})$ [88]

$q : [\,a, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\},$ [240]
$v, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\}, \infty]$

$v :\ \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [241]
$v :\ \mathsf{RecCom} = \mathsf{true}$ [242]
aus [241]:
$v :\ \neg(\mathsf{RecCom} = \mathsf{true})$ [243]
$v :\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [244]
$\Box\ (242, 243)$

$q : [\,a, \{\ldots\}, e, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}), \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))\}, \infty]$ [94]

aus F2R: $e :\ \mathsf{RIM} = \bot \vee \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B)$ [95]

$e :\ \mathsf{RIM} = \bot$ [96]
$\mathsf{RIM}_e = \bot$ [96′]

$e :\ \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B)$ [97]
$e :\ \mathsf{RIM} = \mathsf{msg}(d_{11}, b_{11})$ [145]
$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11})$ [145′]
↪ S. 276

aus RIM:
$e :\ \nabla RIM : \mathsf{A}(\mathsf{RIM} = RIM\ \mathsf{unless}^{+}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [98]
$e :\ \mathsf{A}(\mathsf{RIM} = \mathsf{RIM}_e\ \mathsf{unless}^{+}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [99]
$e :\ (\mathsf{A})(\mathsf{RIM} = \mathsf{RIM}_e\ \mathsf{unless}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [100]
auf q:

$q : [\,a, \{\ldots\},$ [101]
$e, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}),$
$\mathsf{RIM} = \mathsf{RIM}_e\},$
$f, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\}, \infty]$
$f :\ \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [103]
$f :\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [104]
↪ S. 274

$q : [\,a, \{\ldots\},$ [102]
$e, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}),$
$\neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})), \mathsf{RIM} = \mathsf{RIM}_e,$
$\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\}, \infty]$
↪ S. 275

$\vdots$

von [104] (S. 273):

$q : [a, \ldots, e, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}), \mathsf{RIM} = \mathsf{RIM}_e\},$ [101]

$f, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\}, \infty]$

$\mathsf{RIM}_e = \bot$ [96′]

$f : \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [103]

$f : \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [104]

$f : \mathsf{RecCom} = \mathsf{true}$ [105]

aus [103]:

$f : \neg(\mathsf{RecCom} = \mathsf{true})$ [107]

$f : \neg(\mathsf{ProcAck} = \mathsf{true})$ [108]

$\Box$ (105, 107)

$f : \mathsf{AckMsg} = \mathsf{true}$ [106]

Vorgängerzustand von f:

$q : [a, \{\ldots\}, e, \circ, f, \{\ldots\}, \infty]$ [109]

$\boxed{\text{wie [110] mit } e \text{ anstelle } g}$

$q : [a, \ldots, e, \{\mathsf{RIM} = \mathsf{RIM}_e\}, g, \circ, f, \{\ldots\}, \infty]$ [110]

$g : \mathsf{RIM} = \mathsf{RIM}_e$ [111]

$\mathsf{RIM}_g = \mathsf{RIM}_e$ [111′]

aus AM1:

$g : \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}) \rightarrow (\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = \mathsf{flip}(B))$ [112]

$g : \neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))$ [113]

$g : (\mathsf{A})\neg(\circ(\mathsf{AckMsg} = \mathsf{true}))$ [115]

auf q:

$f : \neg(\mathsf{AckMsg} = \mathsf{true})$ [116]

$\Box$ (106, 116)

$g : \exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = \mathsf{flip}(B)$ [114]

$g : \mathsf{RIM} = \mathsf{msg}(d_8, b_8) \wedge \mathsf{RBit} = \mathsf{flip}(b_8)$ [117]

$g : \mathsf{RIM} = \mathsf{msg}(d_8, b_8)$ [118]

$g : \mathsf{RBit} = \mathsf{flip}(b_8)$ [117′]

$\mathsf{RIM}_g = \mathsf{msg}(d_8, b_8)$ [118′]

$\Box :$ $\mathsf{RIM}_g = \mathsf{msg}(d_8, b_8)$ [118′]
$\mathsf{RIM}_g = \mathsf{RIM}_e$ [111′]
$\mathsf{RIM}_e = \bot$ [96′]

$\vdots$

von [102] (S. 273):

$q : [a, \{\ldots\}, e, \{\ldots, \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})), \mathsf{RIM} = \mathsf{RIM}_e, \ldots\}, \infty]$ [102]

Fairness bzgl. ReTrans:

$0 : \mathsf{R}((\Box\Diamond\mathsf{E}\circ(\mathsf{ReTrans} = \mathsf{true})) \to (\Diamond(\mathsf{ReTrans} = \mathsf{true})))$ [119]

auf q:

$e : (q)\Diamond(\neg(q\Diamond\mathsf{E}\circ(\mathsf{ReTrans} = \mathsf{true})))$ [120]

$q : [a, \{\ldots\}, e, \{\ldots\}, h, \{\ldots\}, \infty]$ [122]

$h : q\,\neg(\Diamond\mathsf{E}\circ(\mathsf{ReTrans} = \mathsf{true}))$ [123]

$h : \neg(\mathsf{E}\circ(\mathsf{ReTrans} = \mathsf{true}))$ [124]

$h : (q)\Box\neg(\mathsf{E}\circ(\mathsf{ReTrans} = \mathsf{true}))$ [125]

aus RT1:

$h : \mathsf{E}\circ(\mathsf{ReTrans} = \mathsf{true})$ [126]

$\Box^*$ (124, 126)

$e : (q)\Diamond(\mathsf{ReTrans} = \mathsf{true})$ [121]

$q : [a, \{\ldots\}, e, \{\neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})), \mathsf{RIM} = \bot\},$ [127]
$i, \{\neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})), \mathsf{RIM} = \bot\}, \infty]$

$i : \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))$ [128]

$i : \mathsf{RIM} = \bot$ [129]

$\mathsf{RIM}_i = \bot$ [129′]

$i : \mathsf{ReTrans} = \mathsf{true}$ [130]

Vorgängerzustand von i betrachten:

$q : [a, \{\ldots\}, e, \circ, i, \{\ldots\}, \infty]$ [131]

$\boxed{\text{wie [132] mit } e \text{ anstelle } j}$

$q : [a, \{\ldots\}, e, \{\ldots\}, j, \circ, i, \{\ldots\}, \infty]$ [132]

aus RT2:

$j : \nabla RQ : \mathsf{A}\circ(\mathsf{ReTrans} = \mathsf{true} \to \mathsf{RQ} = RQ|\mathsf{msg}(\mathsf{SFile}(\mathsf{SNo}), \mathsf{SBit}))$ [133]

$j : \mathsf{A}\circ(\mathsf{ReTrans} = \mathsf{true} \to \mathsf{RQ} = \mathsf{RQ}_j|\mathsf{msg}(\mathsf{SFile}(\mathsf{SNo}), \mathsf{SBit}))$ [134]

$j : (\mathsf{A})\circ(\mathsf{ReTrans} = \mathsf{true} \to \mathsf{RQ} = \mathsf{RQ}_j|\mathsf{msg}(\mathsf{SFile}(\mathsf{SNo}), \mathsf{SBit}))$ [135]

auf q:

$i : \mathsf{ReTrans} = \mathsf{true} \to \mathsf{RQ} = \mathsf{RQ}_j|\mathsf{msg}(\mathsf{SFile}(\mathsf{SNo}), \mathsf{SBit})$ [136]

$i : \neg(\mathsf{ReTrans} = \mathsf{true})$ [137]

$\Box$ (130, 137)

$i : \mathsf{RQ} = \mathsf{RQ}_j|\mathsf{msg}(\mathsf{SFile}(\mathsf{SNo}), \mathsf{SBit})$ [138]

$\mathsf{RQ}_i = \mathsf{RQ}_j|\mathsf{msg}(\mathsf{SFile}_i(\mathsf{SNo}_i), \mathsf{SBit}_i)$ [138′]

aus RC1:

$i : (\mathsf{RIM} = \bot \wedge \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q) \to \mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})$ [139]

$i : \neg(\mathsf{RIM} = \bot \wedge \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q)$ [140]

$i : \neg(\mathsf{RIM} = \bot)$ [142]

$\mathsf{RIM}_i \neq \bot$ [142′]

$\Box$ (129, 142)

$i : \neg(\exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q)$ [143]

$i : \neg(\mathsf{RQ} = \mathsf{msg}(D_{10}, B_{10})|Q_{10})$ [144]

$i : \mathsf{RQ} \neq \mathsf{msg}(D_{10}, B_{10})|Q_{10}$ [144′]

$\Box^*$ (E2, 138′, 144′)

$i : \mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})$ [141]

$\Box^*$ (128, 141)

$\vdots$

von [145] (S. 273):

$q : [a, \{\ldots\}, e, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}), \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))\}, \infty]$ [94]

$e :\ \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))$ [92]

$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11})$ [145′]

|

aus RIM:

$e :\ \nabla RIM : \mathsf{A}(\mathsf{RIM} = RIM \text{ unless}^+ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [146]

$e :\ \mathsf{A}(\mathsf{RIM} = \mathsf{RIM}_e \text{ unless}^+ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [147]

$e :\ (\mathsf{A})(\mathsf{RIM} = \mathsf{RIM}_e \text{ unless } \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [148]

auf q:

$q : [a, \{\ldots\}, e, \{\mathsf{RIM} = \mathsf{RIM}_e, \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\}, \infty]$ [153]

↪ S. 278

$q : [a, \{\ldots\}, e, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}), \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})),$ [149]
$\mathsf{RIM} = \mathsf{RIM}_e, \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\},$
$k, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}), \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))\}, \infty]$

|

$k :\ \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [150]

$k :\ \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))$ [151]

$k :\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [152]

$k :\ \mathsf{RecCom} = \mathsf{true}$ [154]

aus [150]:

$k :\ \neg(\mathsf{RecCom} = \mathsf{true})$ [156]

$k :\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [157]

$\Box$ (154, 157)

$k :\ \mathsf{AckMsg} = \mathsf{true}$ [155]

Vorgängerzustand von k:

$q : [a, \{\ldots\}, e, \circ, k, \{\ldots\}, \infty]$ [158]

$\boxed{\text{wie [162] mit } e \text{ anstelle } l.}$

$q : [a, \{\ldots\}, e, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}),$ [159]
$\neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})), \mathsf{RIM} = \mathsf{RIM}_e\},$
$l, \circ, k, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$
$\neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))\}, \infty]$

|

$l :\ \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [160]

$l :\ \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))$ [161]

$l :\ \mathsf{RIM} = \mathsf{RIM}_e$ [162]

$\mathsf{RIM}_l = \mathsf{RIM}_e$ [162′]

↪ S. 277

$$\vdots$$

von [162] (S. 276):

$$q : [\,a, \{\ldots\}, e, \{\ldots\}, l, \circ, k, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}), \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))\}, \infty] \quad [159]$$

$$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11}) \quad [145']$$

$$k : \ \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})) \quad [151]$$

$$k : \ \mathsf{AckMsg} = \mathsf{true} \quad [155]$$

$$\mathsf{RIM}_l = \mathsf{RIM}_e \quad [162']$$

aus AM2:

$$l : \ \forall D, B : \nabla SQ : \ (\mathsf{RIM} = \mathsf{msg}(D, B) \to \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \to \mathsf{SQ} = SQ|\mathsf{msg}(\lambda, B) \wedge \mathsf{RIM} = \bot)) \quad [163]$$

$$l : \ \nabla SQ : \mathsf{RIM} = \mathsf{msg}(D_{12}, B_{12}) \to \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \to \mathsf{SQ} = SQ|\mathsf{msg}(\lambda, B_{12}) \wedge \mathsf{RIM} = \bot) \quad [164]$$

$$l : \ \mathsf{RIM} = \mathsf{msg}(D_{12}, B_{12}) \to \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \to \mathsf{SQ} = SQ_l|\mathsf{msg}(\lambda, B_{12}) \wedge \mathsf{RIM} = \bot) \quad [165]$$

Linker Zweig:

$$l : \ \neg(\mathsf{RIM} = \mathsf{msg}(D_{12}, B_{12})) \quad [166]$$

$$\mathsf{RIM}_l \neq \mathsf{msg}(D_{12}, B_{12}) \quad [166']$$

$$\boxed{\begin{array}{c} \square : \ \mathsf{RIM}_l \neq \mathsf{msg}(D_{12}, B_{12}) \quad [166'] \\ \mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11}) \quad [145'] \\ \mathsf{RIM}_l = \mathsf{RIM}_e \quad [162'] \\ \{D_{12} \leftarrow d_{11},\ B_{12} \leftarrow b_{11}\} \end{array}}$$

Rechter Zweig:

$$l : \ \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \to \mathsf{SQ} = \mathsf{SQ}_l|\mathsf{msg}(\lambda, b_{11}) \wedge \mathsf{RIM} = \bot) \quad [167]$$

$$l : \ (\mathsf{A})\circ(\mathsf{AckMsg} = \mathsf{true} \to \mathsf{SQ} = \mathsf{SQ}_l|\mathsf{msg}(\lambda, b_{11}) \wedge \mathsf{RIM} = \bot) \quad [168]$$

auf q:

$$k : \ \mathsf{AckMsg} = \mathsf{true} \to \mathsf{SQ} = \mathsf{SQ}_l|\mathsf{msg}(\lambda, b_{11}) \wedge \mathsf{RIM} = \bot \quad [169]$$

$$k : \ \neg(\mathsf{AckMsg} = \mathsf{true}) \quad [170]$$

$$\square \ (155, 170)$$

$$k : \ \mathsf{SQ} = \mathsf{SQ}_l|\mathsf{msg}(\lambda, b_{11}) \quad [171]$$

$$k : \ \mathsf{RIM} = \bot \quad [172]$$

$$\boxed{\begin{array}{l} \text{wie [94], [96] ff.,} \\ \text{mit } k \text{ anstelle } e \end{array}}$$

$\vdots$

von [153] (S. 276):

$q : [\,a, \{\ldots\}, e, \{\mathsf{RIM} = \mathsf{RIM}_e, \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\}, \infty]$ [153]

$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11})$ [145′]

Fairness bzgl. AckMsg:

$0 : \mathsf{R}((\Box\Diamond\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})) \rightarrow (\Diamond(\mathsf{AckMsg} = \mathsf{true})))$ [173]

auf q:

$e : (q)\Diamond(\neg(q\Diamond\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})))$ [174]

$q : [\,a, \{\ldots\}, e, \{\mathsf{RIM} = \mathsf{RIM}_e\},$ [176]
$m, \{\mathsf{RIM} = \mathsf{RIM}_e\}, \infty]$

$m : \mathsf{RIM} = \mathsf{RIM}_e$ [177]

$\mathsf{RIM}_m = \mathsf{RIM}_e$ [177′]

$m : q\,\neg(\Diamond\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))$ [178]

$m : \neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))$ [179]

$m : (q)\Box\neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))$ [180]

$e : (q)\Diamond(\mathsf{AckMsg} = \mathsf{true})$ [175]

$q : [\,a, \{\ldots\},$ [235]
$e, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\},$
$u, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\}, \infty]$

$u : \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [236]

$u : \mathsf{AckMsg} = \mathsf{true}$ [237]

aus [236]:

$u : \neg(\mathsf{RecCom} = \mathsf{true})$ [238]

$u : \neg(\mathsf{AckMsg} = \mathsf{true})$ [239]

$\Box$ (237, 239)

$q : [\,a, \{\ldots\}, e, \{\ldots\}, m, \{\mathsf{RIM} = \mathsf{RIM}_e, \neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))\}, \infty]$ [181]

aus AM1:

$m : (\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = \mathsf{flip}(B)) \rightarrow \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})$ [182]

$m : \neg(\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = \mathsf{flip}(B))$ [183]

$m : \neg(\mathsf{RIM} = \mathsf{msg}(D_{13}, B_{13}) \wedge \mathsf{RBit} = \mathsf{flip}(B_{13}))$ [185]

$m : \neg(\mathsf{RIM} = \mathsf{msg}(D_{13}, B_{13}))$ [186]

$\mathsf{RIM}_m \neq \mathsf{msg}(D_{13}, B_{13})$ [186′]

$\Box$:	$\mathsf{RIM}_m = \mathsf{RIM}_e$ [177′]
	$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11})$ [145′]
	$\mathsf{RIM}_m \neq \mathsf{msg}(D_{13}, B_{13})$ [186′]
	$\{D_{13} \leftarrow d_{11},\ B_{13} \leftarrow b_{11}\}$

$m : \neg(\mathsf{RBit} = \mathsf{flip}(b_{11}))$ [187]

$\mathsf{RBit}_m \neq \mathsf{flip}(b_{11})$ [187′]

aus RBit:

$m : \nabla RBit : \mathsf{A}(\mathsf{RBit} = RBit \text{ unless}^+ \mathsf{AccDat} = \mathsf{true})$ [188]

$m : \mathsf{A}(\mathsf{RBit} = \mathsf{RBit}_m \text{ unless}^+ \mathsf{AccDat} = \mathsf{true})$ [189]

$m : (\mathsf{A})(\mathsf{RBit} = \mathsf{RBit}_m \text{ unless } \mathsf{AccDat} = \mathsf{true})$ [190]

$\hookrightarrow$ S. 279

$m : \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})$ [184]

$\Box^*$ (179, 184)

$$\vdots$$

von [190] (S. 278):

$$q : [a, \{\ldots\}, e, \{\ldots\}, m, \{\mathsf{RIM} = \mathsf{RIM}_e, \neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))\}, \infty] \quad [181]$$

$$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11}) \quad [145']$$

$$\mathsf{RIM}_m = \mathsf{RIM}_e \quad [177']$$

$$\mathsf{RBit}_m \neq \mathsf{flip}(b_{11}) \quad [187']$$

$$m : \ (\mathsf{A})(\mathsf{RBit} = \mathsf{RBit}_m \text{ unless } \mathsf{AccDat} = \mathsf{true}) \quad [190]$$

auf q:

$$q : [a, \{\ldots\}, e, \{\ldots\}, \quad [191]$$
$$m, \{\mathsf{RIM} = \mathsf{RIM}_e, \neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})), \mathsf{RBit} = \mathsf{RBit}_m\},$$
$$n, \{\mathsf{RIM} = \mathsf{RIM}_e, \neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))\}, \infty]$$

$$n : \ \neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})) \quad [192]$$

$$n : \ \mathsf{RIM} = \mathsf{RIM}_e \quad [193]$$

$$\mathsf{RIM}_n = \mathsf{RIM}_e \quad [193']$$

$$n : \ \mathsf{AccDat} = \mathsf{true} \quad [194]$$

Vorgängerzustand von n:

$$q : [a, \{\ldots\}, e, \{\ldots\}, m, \circ, n, \{\ldots\}, \infty] \quad [196]$$

$$\boxed{\text{wie [197] mit } m \text{ anstelle } r \text{ und } \mathsf{RIM}_m = \mathsf{RIM}_e \ [177']}$$

$$q : [a, \{\ldots\}, e, \{\ldots\}, \quad [197]$$
$$m, \{\mathsf{RIM} = \mathsf{RIM}_e, \mathsf{RBit} = \mathsf{RBit}_m\}, r, \circ, n, \{\ldots\}, \infty]$$

$$r : \ \mathsf{RIM} = \mathsf{RIM}_e \quad [198]$$

$$r : \ \mathsf{RBit} = \mathsf{RBit}_m \quad [199]$$

$$\mathsf{RIM}_r = \mathsf{RIM}_e \quad [198']$$

$$\mathsf{RBit}_r = \mathsf{RBit}_m \quad [199']$$

aus AD2:

$$r : \ \forall D : \nabla RBit, RNo : \ \mathsf{RIM} = \mathsf{msg}(D, RBit) \rightarrow \quad [200]$$
$$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(RNo) = D \wedge \mathsf{RNo} = s(RNo) \wedge \mathsf{RBit} = \mathsf{flip}(RBit))$$

$$r : \ \nabla RBit, RNo : \ \mathsf{RIM} = \mathsf{msg}(D_{14}, RBit) \rightarrow \quad [201]$$
$$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(RNo) = D_{14} \wedge \mathsf{RNo} = s(RNo) \wedge \mathsf{RBit} = \mathsf{flip}(RBit))$$

$$r : \ \mathsf{RIM} = \mathsf{msg}(D_{14}, \mathsf{RBit}_r) \rightarrow \quad [202]$$
$$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(\mathsf{RNo}_r) = D_{14} \wedge \mathsf{RNo} = s(\mathsf{RNo}_r) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_r))$$

$\hookrightarrow$ S. 280

$$q : [a, \{\ldots\}, e, \{\ldots\}, \quad [195]$$
$$m, \{\mathsf{RIM} = \mathsf{RIM}_e, \mathsf{RBit} = \mathsf{RBit}_m,$$
$$\neg(\mathsf{AccDat} = \mathsf{true})\}, \infty]$$

$\hookrightarrow$ S. 281

$$\vdots$$

von [202] (S. 279):

$$q : [\,a, \{\ldots\}, e, \{\ldots\}, m, \{\mathsf{RIM} = \mathsf{RIM}_e, \mathsf{RBit} = \mathsf{RBit}_m\}, r, \circ, n, \{\ldots\}, \infty] \quad [197]$$

$$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11}) \quad [145']$$

$$\mathsf{RBit}_m \neq \mathsf{flip}(b_{11}) \quad [187']$$

$$n :\ \neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})) \quad [192]$$

$$\mathsf{RIM}_n = \mathsf{RIM}_e \quad [193']$$

$$n :\ \mathsf{AccDat} = \mathsf{true} \quad [194]$$

$$\mathsf{RBit}_r = \mathsf{RBit}_m \quad [199']$$

$$r :\ \mathsf{RIM} = \mathsf{msg}(D_{14}, \mathsf{RBit}_r) \rightarrow \quad [202]$$
$$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \mathsf{RFile}(\mathsf{RNo}_r) = D_{14} \wedge \mathsf{RNo} = s(\mathsf{RNo}_r) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_r))$$

$$r :\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{14}, \mathsf{RBit}_r)) \quad [203]$$

$$\mathsf{RIM}_r \neq \mathsf{msg}(D_{14}, \mathsf{RBit}_r) \quad [203']$$

$$\Box :\ \mathsf{RIM}_r = \mathsf{RIM}_e \quad [198']$$
$$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11}) \quad [145']$$
$$\mathsf{RBit}_r = \mathsf{RBit}_m \quad [199']$$
$$\mathsf{RBit}_m \neq \mathsf{flip}(b_{11}) \quad [187']$$
$$\mathsf{RIM}_r \neq \mathsf{msg}(D_{14}, \mathsf{RBit}_r) \quad [203']$$
$$\Box\ \{D_{14} \leftarrow d_{11}\}$$

$$r :\ \mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \quad [204]$$
$$\mathsf{RFile}(\mathsf{RNo}_r) = d_{11} \wedge \mathsf{RNo} = s(\mathsf{RNo}_r) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_r))$$

$$r :\ (\mathsf{A})\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow \quad [205]$$
$$\mathsf{RFile}(\mathsf{RNo}_r) = d_{11} \wedge \mathsf{RNo} = s(\mathsf{RNo}_r) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_r))$$

auf q:

$$n :\ \mathsf{AccDat} = \mathsf{true} \rightarrow \quad [206]$$
$$\mathsf{RFile}(\mathsf{RNo}_r) = d_{11} \wedge \mathsf{RNo} = s(\mathsf{RNo}_r) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_r))$$

$$n :\ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [207]$$
$$\Box\ (194, 207)$$

$$n :\ \mathsf{RFile}(\mathsf{RNo}_r) = d_{11} \quad [208]$$
$$n :\ \mathsf{RNo} = s(\mathsf{RNo}_r) \quad [209]$$
$$n :\ \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_r) \quad [210]$$
$$\mathsf{RBit}_n = \mathsf{flip}(\mathsf{RBit}_r) \quad [210']$$

aus AM1:

$$n :\ (\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = \mathsf{flip}(B)) \rightarrow \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}) \quad [211]$$

$$n :\ \neg(\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = \mathsf{flip}(B)) \quad [212]$$
$$n :\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{15}, B_{15}) \wedge \mathsf{RBit} = \mathsf{flip}(B_{15})) \quad [214]$$

$$n :\ \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}) \quad [213]$$
$$\Box^*\ (192, 213)$$

$$n :\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{15}, B_{15})) \quad [215]$$
$$\mathsf{RIM}_n \neq \mathsf{msg}(D_{15}, B_{15}) \quad [215']$$

$$\Box :\ \mathsf{RIM}_n = \mathsf{RIM}_e \quad [193']$$
$$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11}) \quad [145']$$
$$\mathsf{RIM}_n \neq \mathsf{msg}(D_{15}, B_{15}) \quad [215']$$
$$\Box\ \{D_{15} \leftarrow d_{11},\ B_{15} \leftarrow b_{11}\}$$

$$n :\ \neg(\mathsf{RBit} = \mathsf{flip}(b_{11})) \quad [216]$$
$$\mathsf{RBit}_n \neq \mathsf{flip}(b_{11}) \quad [216']$$

$$\Box :\ \mathsf{RBit}_n = \mathsf{flip}(\mathsf{RBit}_r) \quad [210']$$
$$\mathsf{RBit}_r = \mathsf{RBit}_m \quad [199']$$
$$\mathsf{RBit}_m \neq \mathsf{flip}(b_{11}) \quad [187']$$
$$\mathsf{RBit}_n \neq \mathsf{flip}(b_{11}) \quad [216']$$

$$\vdots$$

von [195] (S. 279):

$$q : [\,a, \{\ldots\}, e, \{\ldots\}, m, \{\mathsf{RIM} = \mathsf{RIM}_e, \mathsf{RBit} = \mathsf{RBit}_m, \neg(\mathsf{AccDat} = \mathsf{true})\}, \infty] \quad [195]$$

$$\mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11}) \quad [145']$$

$$\mathsf{RBit}_m \neq \mathsf{flip}(b_{11}) \quad [187']$$

$$|$$

Fairness bzgl. AccDat:

$$0 : \ \mathsf{R}((\Box\Diamond\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \rightarrow (\Diamond(\mathsf{AccDat} = \mathsf{true}))) \quad [217]$$

auf q:

$$m : \ (q)\Diamond(\neg(q\Diamond\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}))) \quad [218]$$

$$|$$

$$q : [\,a, \{\ldots\}, e, \{\ldots\}, \quad [220]$$
$$m, \{\mathsf{RIM} = \mathsf{RIM}_e, \mathsf{RBit} = \mathsf{RBit}_m\},$$
$$s, \{\mathsf{RIM} = \mathsf{RIM}_e, \mathsf{RBit} = \mathsf{RBit}_m, \}, \infty]$$

$$|$$

$$s : \ \mathsf{RIM} = \mathsf{RIM}_e \quad [221]$$

$$s : \ \mathsf{RBit} = \mathsf{RBit}_m \quad [222]$$

$$s : \ q\,\neg(\Diamond\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [223]$$

$$\mathsf{RIM}_s = \mathsf{RIM}_e \quad [221']$$

$$\mathsf{RBit}_s = \mathsf{RBit}_m \quad [222']$$

$$|$$

$$s : \ \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [224]$$

$$s : \ (q)\Box\neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [225]$$

$$|$$

aus AD1:

$$s : \ (\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = B) \rightarrow \mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}) \quad [226]$$

$$s : \ \neg(\exists D, B : \mathsf{RIM} = \mathsf{msg}(D, B) \wedge \mathsf{RBit} = B) \quad [227]$$

$$s : \ \neg(\mathsf{RIM} = \mathsf{msg}(D_{16}, B_{16}) \wedge \mathsf{RBit} = B_{16}) \quad [229]$$

$$s : \ \neg(\mathsf{RIM} = \mathsf{msg}(D_{16}, B_{16})) \quad [230]$$

$$\mathsf{RIM} \neq \mathsf{msg}(D_{16}, B_{16}) \quad [230']$$

$$\boxed{\begin{array}{l} \Box : \ \mathsf{RIM}_e = \mathsf{msg}(d_{11}, b_{11}) \quad [145'] \\ \quad \mathsf{RIM}_s = \mathsf{RIM}_e \quad [221'] \\ \quad \mathsf{RIM} \neq \mathsf{msg}(D_{16}, B_{16}) \quad [230'] \\ \quad \{D_{16} \leftarrow d_{11},\ B_{16} \leftarrow b_{11}\} \end{array}}$$

$$s : \ \neg(\mathsf{RBit} = b_{11}) \quad [231]$$

$$\mathsf{RBit}_s \neq b_{11} \quad [231']$$

$$\boxed{\begin{array}{l} \Box : \ \mathsf{RBit}_s \neq b_{11} \quad [231'] \\ \quad \mathsf{RBit}_s = \mathsf{RBit}_m \quad [222'] \\ \quad \mathsf{RBit}_m \neq \mathsf{flip}(b_{11}) \quad [187'] \end{array}}$$

$$s : \ \mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}) \quad [228]$$

$$\Box^* \ (224, 228)$$

$$m : \ (p)\Diamond(\mathsf{AccDat} = \mathsf{true}) \quad [219]$$

$$|$$

$$q : [\,a, \{\ldots\}, e, \{\ldots\}, \quad [232]$$
$$m, \{\neg(\mathsf{AccDat} = \mathsf{true})\},$$
$$t, \{\neg(\mathsf{AccDat} = \mathsf{true})\}, \infty]$$

$$|$$

$$t : \ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [233]$$

$$t : \ \mathsf{AccDat} = \mathsf{true} \quad [234]$$

$$\Box \ (233, 234)$$

Analog geht man im Induktionsschritt vor:

$$\vdots$$

von [4] (S. 268):

$0: \ \neg(\forall N : A(N))$ [1]

$0: \ A(n_0)$ [3]

$0: \ \neg(A(s(n_0)))$ [4]

$0: \ \neg(\mathsf{A}\Box(\forall D : \nabla SBit : (\mathsf{ARfSB} = s(n_0) \wedge \mathsf{SFile}(\mathsf{SNo}) = D) \rightarrow$ [7+]
$\rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D, SBit)))))$

$0: \ \neg(\forall D : \nabla SBit :$ [8+]
$(\mathsf{ARfSB} = s(n_0) \wedge \mathsf{SFile}(\mathsf{SNo}) = D) \rightarrow$
$\mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D, SBit))))$

$\boxed{\text{wie [9+] ff. mit 0 anstelle } a'}$

$0: \ (\mathsf{E})\neg(\Box(\forall D : \nabla SBit :$ [9+]
$(\mathsf{ARfSB} = s(n_0) \wedge \mathsf{SFile}(\mathsf{SNo}) = D) \rightarrow$
$\mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D, SBit)))))$

$p' : [0, \{B(s(n_0))\}, a', \emptyset, \infty]$ [10+]

man erhält

$\mathsf{ARfSB}_{a'} = s(n_0)$ [16′+]

$\mathsf{SFile}_{a'}(\mathsf{SNo}_{a'}) = d'_1$ [17′+]

$q' : [a', \emptyset, \infty]$ [18+]

$q' : [a', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'})),$ [38+]
$\mathsf{SFile}(\mathsf{SNo}_{a'}) = d'_1, \mathsf{SBit} = \mathsf{SBit}_{a'}, \mathsf{SNo} = \mathsf{SNo}_{a'}\}, \infty]$

$a': \ \nabla\mathsf{ARfSB} : \mathsf{A}(\mathsf{ARfSB} = ARfSB \text{ unless}^{+} \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [39+]

$a': \ (\mathsf{A})(\mathsf{ARfSB} = \mathsf{ARfSB}_{a'} \text{ unless } \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$ [41+]

$\hookrightarrow$ S. 283

$\vdots$

von [41+] (S. 282):

$$q' : [\,a', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1', \mathsf{SBit}_{a'})), \mathsf{SFile}(\mathsf{SNo}_{a'}) = d_1', \mathsf{SBit} = \mathsf{SBit}_{a'}, \mathsf{SNo} = \mathsf{SNo}_{a'}\}, \infty] \quad [38+]$$

$$\mathsf{ARfSB}_{a'} = s(n_0) \quad [16'+]$$

$$a' : \ (\mathsf{A})(\mathsf{ARfSB} = \mathsf{ARfSB}_{a'} \text{ unless } \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}) \quad [41+]$$

$$q' : [\,a', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1', \mathsf{SBit}_{a'})), \mathsf{SFile}(\mathsf{SNo}_{a'}) = d_1', \mathsf{SBit} = \mathsf{SBit}_{a'}, \quad [49+]$$
$$\mathsf{SNo} = \mathsf{SNo}_{a'}, \mathsf{ARfSB} = \mathsf{ARfSB}_{a'}, \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\}, \infty]$$

Mit demselben Vorgehen wie im Induktionsanfang bei [49] weist man nach, daß dieser Pfad nicht den Fairnessanforderungen entspricht.

$$q' : [\,a', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1', \mathsf{SBit}_{a'})), \mathsf{SFile}(\mathsf{SNo}_{a'}) = d_1', \mathsf{SBit} = \mathsf{SBit}_{a'}, \mathsf{SNo} = \mathsf{SNo}_{a'}, \quad [42+]$$
$$\mathsf{ARfSB} = \mathsf{ARfSB}_{a'}, \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\},$$
$$c, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1', \mathsf{SBit}_{a'})), \mathsf{SFile}(\mathsf{SNo}_{a'}) = d_1', \mathsf{SBit} = \mathsf{SBit}_{a'}, \mathsf{SNo} = \mathsf{SNo}_{a'}, \infty]$$

$$c' : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [43+]$$
$$c' : \ \neg(\mathsf{RIM} = \mathsf{msg}(d_1', \mathsf{SBit}_{a'})) \quad [44+]$$
$$c' : \ \mathsf{SFile}(\mathsf{SNo}_{a'}) = d_1' \quad [45+]$$
$$c' : \ \mathsf{SBit} = \mathsf{SBit}_{a'} \quad [46+]$$
$$c' : \ \mathsf{SNo} = \mathsf{SNo}_{a'} \quad [47+]$$
$$c' : \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true} \quad [48+]$$

$$\mathsf{RIM}_{c'} \neq \mathsf{msg}(d_1', \mathsf{SBit}_{a'})) \quad [44'+]$$
$$\mathsf{SFile}_{c'}(\mathsf{SNo}_{a'}) = d_1' \quad [45'+]$$
$$\mathsf{SBit}_{c'} = \mathsf{SBit}_{a'} \quad [46'+]$$
$$\mathsf{SNo}_{c'} = \mathsf{SNo}_{a'} \quad [47'+]$$

$$c' : \ \mathsf{RecCom} = \mathsf{true} \quad [50+] \qquad\qquad c' : \ \mathsf{ProcAck} = \mathsf{true} \quad [51+]$$
$$\square \ (43+, 51+)$$

Vorgängerzustand von c:

$$q' : [\,a', \circ, c', \{\ldots\}, \infty] \quad [52+]$$

wie [53+] mit a anstelle d' und $\mathsf{ARfSB}_{a'} = s(n_0)$ [16'+]

$$q' : [\,a', \{\ldots, \mathsf{SBit} = \mathsf{SBit}_{a'}, \mathsf{ARfSB} = \mathsf{ARfSB}_{a'}\}, d', \circ, \quad [53+]$$
$$c', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1', \mathsf{SBit}_{a'}))\}, \infty]$$
$$d' : \ \mathsf{SBit} = \mathsf{SBit}_{a'} \quad [54+]$$
$$d' : \ \mathsf{ARfSB} = \mathsf{ARfSB}_{a'} \quad [55+]$$
$$\mathsf{SBit}_{d'} = \mathsf{SBit}_{a'} \quad [54'+]$$
$$\mathsf{ARfSB}_{d'} = \mathsf{ARfSB}_{a'} \quad [55'+]$$

$\hookrightarrow$ S. 284

$$\vdots$$

von [55+] (S. 283):

$$q' : [\, a', \{\ldots, \mathsf{SBit} = \mathsf{SBit}_{a'}, \mathsf{ARfSB} = \mathsf{ARfSB}_{a'}\}, \quad [53+]$$
$$d', \circ, c', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'}))\}, \infty]$$
$$\mathsf{ARfSB}_{a'} = s(n_0) \quad [16'+]$$
$$\mathsf{RIM}_{c'} \neq \mathsf{msg}(d'_1, \mathsf{SBit}_{a'})) \quad [44'+]$$
$$\mathsf{SFile}_{c'}(\mathsf{SNo}_{a'}) = d'_1 \quad [45'+]$$
$$\mathsf{SBit}_{c'} = \mathsf{SBit}_{a'} \quad [46'+]$$
$$\mathsf{SNo}_{c'} = \mathsf{SNo}_{a'} \quad [47'+]$$
$$c' : \ \mathsf{RecCom} = \mathsf{true} \quad [50+]$$
$$\mathsf{ARfSB}_{d'} = \mathsf{ARfSB}_{a'} \quad [55'+]$$

aus RC1:

$$d' : \ \mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}) \rightarrow (\mathsf{RIM} = \bot \wedge \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q) \quad [56+]$$

$$d' : \ \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})) \quad [57+]$$
$$d' : \ (\mathsf{A})\neg(\circ(\mathsf{RecCom} = \mathsf{true})) \quad [60+]$$

auf q':

$$c' : \ \neg(\mathsf{RecCom} = \mathsf{true}) \quad [61+]$$
$$\square \ (50+, 61+)$$

$$d' : \ \mathsf{RIM} = \bot \quad [58+]$$
$$d' : \ \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q \quad [59+]$$
$$d' : \ \mathsf{RQ} = \mathsf{msg}(d'_4, b'_4)|q'_4 \quad [62+]$$
$$\mathsf{RIM}_{d'} = \bot \quad [58'+]$$
$$\mathsf{RQ}_{d'} = \mathsf{msg}(d'_4, b'_4)|q'_4 \quad [62'+]$$

aus RC2:

$$d' : \ \forall D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q \rightarrow \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = Q \wedge \mathsf{RIM} = \mathsf{msg}(D, B)) \quad [245]$$
$$d' : \ \mathsf{RQ} = \mathsf{msg}(D_{17}, B_{17})|Q_{17} \rightarrow \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = Q_{17} \wedge \mathsf{RIM} = \mathsf{msg}(D_{17}, B_{17})) \quad [246]$$

$$d' : \ \neg(\mathsf{RQ} = \mathsf{msg}(D_{17}, B_{17})|Q_{17}) \quad [247]$$
$$\square \ \{D_{17} \leftarrow d'_4, \ B_{17} \leftarrow b'_4, \ Q_{17} \leftarrow q'_4\}(62+, 247)$$

$$d' : \ \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = q'_5 \wedge \mathsf{RIM} = \mathsf{msg}(d'_5, b'_5)) \quad [248]$$
$$d' : \ (\mathsf{A})\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = q'_5 \wedge \mathsf{RIM} = \mathsf{msg}(d'_5, b'_5)) \quad [249]$$

auf q:

$$c' : \ \mathsf{RecCom} = \mathsf{true} \rightarrow \mathsf{RQ} = q'_5 \wedge \mathsf{RIM} = \mathsf{msg}(d'_5, b'_5) \quad [250]$$

$$c' : \ \neg(\mathsf{RecCom} = \mathsf{true}) \quad [251]$$
$$\square \ (61'+, 251)$$

$$c' : \ \mathsf{RQ} = q'_5 \quad [252]$$
$$c' : \ \mathsf{RIM} = \mathsf{msg}(d'_5, b'_5) \quad [253]$$
$$\mathsf{RQ}_{c'} = q'_5 \quad [252']$$
$$\mathsf{RIM}_{c'} = \mathsf{msg}(d'_5, b'_5) \quad [253']$$

$\hookrightarrow$ S. 285

$$\vdots$$

von [253] (S. 284):

$$q' : [\, a', \{\ldots, \mathsf{SBit} = \mathsf{SBit}_{a'}, \mathsf{ARfSB} = \mathsf{ARfSB}_{a'}\}, \qquad [53+]$$
$$d', \circ, c', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'}))\}, \infty]$$

$$\mathsf{ARfSB}_{a'} = s(n_0) \quad [16'+]$$
$$c' : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [43+]$$
$$\mathsf{RIM}_{c'} \neq \mathsf{msg}(d'_1, \mathsf{SBit}_{a'})) \quad [44'+]$$
$$\mathsf{SFile}_{c'}(\mathsf{SNo}_{a'}) = d'_1 \quad [45'+]$$
$$\mathsf{SBit}_{c'} = \mathsf{SBit}_{a'} \quad [46'+]$$
$$\mathsf{SNo}_{c'} = \mathsf{SNo}_{a'} \quad [47'+]$$
$$c' : \ \mathsf{RecCom} = \mathsf{true} \quad [50+]$$
$$\mathsf{ARfSB}_{d'} = \mathsf{ARfSB}_{a'} \quad [55'+]$$
$$\mathsf{RIM}_{c'} = \mathsf{msg}(d'_5, b'_5) \quad [253']$$

aus RC3:

$$d' : \ \forall D, B : \nabla ARSB, ARfSB : \mathsf{A}\circ(\ (\mathsf{RecCom} = \mathsf{true} \wedge \neg(\mathsf{ProcAck} = \mathsf{true}) \wedge \mathsf{RIM} = \mathsf{msg}(D, B)) \rightarrow \qquad [254]$$
$$((B = \mathsf{SBit} \rightarrow (\mathsf{ARSB} = p(ARSB) \wedge \mathsf{ARfSB} = ARfSB)) \wedge$$
$$(B = \mathsf{flip}(\mathsf{SBit}) \rightarrow (\mathsf{ARSB} = ARSB \wedge \mathsf{ARfSB} = p(ARfSB)))))$$

$$d' : \ \nabla ARSB, ARfSB : \mathsf{A}\circ(\ (\mathsf{RecCom} = \mathsf{true} \wedge \neg(\mathsf{ProcAck} = \mathsf{true}) \wedge \mathsf{RIM} = \mathsf{msg}(D_{18}, B_{18})) \rightarrow \qquad [255]$$
$$((B_{18} = \mathsf{SBit} \rightarrow (\mathsf{ARSB} = p(ARSB) \wedge \mathsf{ARfSB} = ARfSB)) \wedge$$
$$(B_{18} = \mathsf{flip}(\mathsf{SBit}) \rightarrow (\mathsf{ARSB} = ARSB \wedge \mathsf{ARfSB} = p(ARfSB)))))$$

$$d' : \ \mathsf{A}\circ(\ (\mathsf{RecCom} = \mathsf{true} \wedge \neg(\mathsf{ProcAck} = \mathsf{true}) \wedge \mathsf{RIM} = \mathsf{msg}(D_{18}, B_{18})) \rightarrow \qquad [256]$$
$$((B_{18} = \mathsf{SBit} \rightarrow (\mathsf{ARSB} = p(\mathsf{ARSB}_{d'}) \wedge \mathsf{ARfSB} = \mathsf{ARfSB}_{d'})) \wedge$$
$$(B_{18} = \mathsf{flip}(\mathsf{SBit}) \rightarrow (\mathsf{ARSB} = \mathsf{ARSB}_{d'} \wedge \mathsf{ARfSB} = p(\mathsf{ARfSB}_{d'})))))$$

$$d' : \ (\mathsf{A})\circ((\ldots) \rightarrow (\ldots)) \quad [257]$$

auf q':

$$c' : \ (\mathsf{RecCom} = \mathsf{true} \wedge \neg(\mathsf{ProcAck} = \mathsf{true}) \wedge \mathsf{RIM} = \mathsf{msg}(D_{18}, B_{18})) \rightarrow \quad [258]$$
$$((B_{18} = \mathsf{SBit} \rightarrow (\mathsf{ARSB} = p(\mathsf{ARSB}_{d'}) \wedge \mathsf{ARfSB} = \mathsf{ARfSB}_{d'})) \wedge$$
$$(B_{18} = \mathsf{flip}(\mathsf{SBit}) \rightarrow (\mathsf{ARSB} = \mathsf{ARSB}_{d'} \wedge \mathsf{ARfSB} = p(\mathsf{ARfSB}_{d'}))))$$

$$c' : \ \neg(\mathsf{RecCom} = \mathsf{true} \wedge \neg(\mathsf{ProcAck} = \mathsf{true}) \wedge \quad [259]$$
$$\wedge\ \mathsf{RIM} = \mathsf{msg}(D_{18}, B_{18}))$$
$$\Box^* \ \{D_{18} \leftarrow d'_5, \ B_{18} \leftarrow b'_5\}(43+, 50+, 253')$$

$\hookrightarrow$ S. 286

$\vdots$

von [258] (S. 285):

(rechter Zweig)

$$q' : [a', \{\ldots, \mathsf{SBit} = \mathsf{SBit}_{a'}, \mathsf{ARfSB} = \mathsf{ARfSB}_{a'}\}, \quad [53+]$$
$$d', \circ, c', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'}))\}, \infty]$$
$$\mathsf{ARfSB}_{a'} = s(n_0) \quad [16'+]$$
$$\mathsf{RIM}_{c'} \neq \mathsf{msg}(d'_1, \mathsf{SBit}_{a'})) \quad [44'+]$$
$$\mathsf{SFile}_{c'}(\mathsf{SNo}_{a'}) = d'_1 \quad [45'+]$$
$$\mathsf{SBit}_{c'} = \mathsf{SBit}_{a'} \quad [46'+]$$
$$\mathsf{SNo}_{c'} = \mathsf{SNo}_{a'} \quad [47'+]$$
$$\mathsf{ARfSB}_{d'} = \mathsf{ARfSB}_{a'} \quad [55'+]$$
$$\mathsf{RIM}_{c'} = \mathsf{msg}(d'_5, b'_5) \quad [253']$$

$$c' : \; b'_5 = \mathsf{SBit} \to (\mathsf{ARSB} = p(\mathsf{ARSB}_{d'}) \wedge \mathsf{ARfSB} = \mathsf{ARfSB}_{d'}) \quad [260]$$
$$c' : \; b'_5 = \mathsf{flip}(\mathsf{SBit}) \to (\mathsf{ARSB} = \mathsf{ARSB}_{d'} \wedge \mathsf{ARfSB} = p(\mathsf{ARfSB}_{d'})) \quad [261]$$

Linker Zweig:

$$c' : \; \neg(b'_5 = \mathsf{flip}(\mathsf{SBit})) \quad [262]$$
$$b'_5 \neq \mathsf{flip}(\mathsf{SBit}_{c'}) \quad [262']$$

Rechter Zweig:

$$c' : \; \mathsf{ARSB} = \mathsf{ARSB}_{d'} \quad [263]$$
$$c' : \; \mathsf{ARfSB} = p(\mathsf{ARfSB}_{d'}) \quad [264]$$
$$\mathsf{ARfSB}_{c'} = p(\mathsf{ARfSB}_{d'}) \quad [264']$$

$\hookrightarrow$ S. 287

aus Lemma 5:

$$c' : \; \forall D, B : (\mathsf{RIM} = \mathsf{msg}(D, B) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D, B)|Q') \to \quad [265]$$
$$((B = \mathsf{SBit} \to D = \mathsf{SFile}(\mathsf{SNo})) \wedge (B = \mathsf{flip}(\mathsf{SBit}) \to D = \mathsf{SFile}(p(\mathsf{SNo}))))$$
$$c' : \; (\mathsf{RIM} = \mathsf{msg}(D_{19}, B_{19}) \vee \exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{19}, B_{19})|Q') \to \quad [266]$$
$$((B_{19} = \mathsf{SBit} \to D = \mathsf{SFile}(\mathsf{SNo})) \wedge (B_{19} = \mathsf{flip}(\mathsf{SBit}) \to D = \mathsf{SFile}(p(\mathsf{SNo}))))$$

Linker Zweig:

$$c' : \; \neg(\mathsf{RIM} = \mathsf{msg}(D_{19}, B_{19})) \quad [267]$$
$$c' : \; \neg(\exists Q, Q' : \mathsf{RQ} = Q|\mathsf{msg}(D_{19}, B_{19})|Q') \quad [268]$$
$$\mathsf{RIM}_{c'} \neq \mathsf{msg}(D_{19}, B_{19}) \quad [267']$$
$$\Box \; \{D_{19} \leftarrow d'_5, \; B_{19} \leftarrow b'_5\}(253', 267')$$

Rechter Zweig:

$$c' : \; b'_5 = \mathsf{SBit} \to d'_5 = \mathsf{SFile}(\mathsf{SNo}) \quad [269]$$
$$c' : \; b'_5 = \mathsf{flip}(\mathsf{SBit}) \to d'_5 = \mathsf{SFile}(p(\mathsf{SNo})) \quad [270]$$

Linker Zweig:

$$c' : \; \neg(b'_5 = \mathsf{SBit}) \quad [271]$$
$$b'_5 \neq \mathsf{SBit}_{c'} \quad [271']$$
$$\Box \; (262', 271')$$

Rechter Zweig:

$$c' : \; d'_5 = \mathsf{SFile}(\mathsf{SNo}) \quad [272]$$
$$d'_5 = \mathsf{SFile}_{c'}(\mathsf{SNo}_{c'}) \quad [272']$$

$\Box$: $\mathsf{RIM}_{c'} \neq \mathsf{msg}(d'_1, \mathsf{SBit}_{a'}))$ [44'+]
$\mathsf{RIM}_{c'} = \mathsf{msg}(d'_5, b'_5)$ [253']
$\to d'_1 \neq d'_5 \vee \mathsf{SBit}_{a'} \neq b'_5$

$b'_5 \neq \mathsf{flip}(\mathsf{SBit}_{c'})$ [262']	$d'_5 = \mathsf{SFile}_{c'}(\mathsf{SNo}_{c'})$ [272]
$\mathsf{SBit}_{c'} = \mathsf{SBit}_{a'}$ [46'+]	$\mathsf{SFile}_{c'}(\mathsf{SNo}_{a'}) = d'_1$ [45'+]
$\to \mathsf{SBit}_{a'} = b'_5$	$\mathsf{SNo}_{c'} = \mathsf{SNo}_{a'}$ [47'+]
	$\to d'_1 = d'_5$

$$\vdots$$

von [264] (S. 286):

$$q' : [\,a', \{\ldots, \mathsf{SBit} = \mathsf{SBit}_{a'}, \mathsf{ARfSB} = \mathsf{ARfSB}_{a'}\}, \quad [53+]$$
$$d', \circ, c', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'}))\}, \infty]$$
$$\mathsf{ARfSB}_{a'} = s(n_0) \quad [16'+]$$
$$\mathsf{SFile}_{c'}(\mathsf{SNo}_{a'}) = d'_1 \quad [45'+]$$
$$\mathsf{SBit}_{c'} = \mathsf{SBit}_{a'} \quad [46'+]$$
$$\mathsf{SNo}_{c'} = \mathsf{SNo}_{a'} \quad [47'+]$$
$$\mathsf{ARfSB}_{d'} = \mathsf{ARfSB}_{a'} \quad [55'+]$$
$$\mathsf{ARfSB}_{c'} = p(\mathsf{ARfSB}_{d'}) \quad [264']$$

Ind.Vor.:

$$0: \; A(n_0) \quad [4]$$
$$0: \; \mathsf{A}\Box(\forall D : \nabla SBit : (\mathsf{ARfSB} = n_0 \wedge \mathsf{SFile}(\mathsf{SNo}) = D) \rightarrow \quad [273]$$
$$\mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D, SBit)))$$

entlang p' und q' nach c' bringen:

$$c': \; \forall D : \nabla SBit : (\mathsf{ARfSB} = n_0 \wedge \mathsf{SFile}(\mathsf{SNo}) = D) \rightarrow \quad [274]$$
$$\mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D, SBit))$$

$$c': \; \nabla SBit : (\mathsf{ARfSB} = n_0 \wedge \mathsf{SFile}(\mathsf{SNo}) = D_{20}) \rightarrow \quad [275]$$
$$\mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D, SBit))$$

$$c': \; (\mathsf{ARfSB} = n_0 \wedge \mathsf{SFile}(\mathsf{SNo}) = D_{20}) \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D_{20}, \mathsf{SBit}_{c'})) \quad [276]$$

$$c': \; \neg(\mathsf{ARfSB} = n_0 \wedge \mathsf{SFile}(\mathsf{SNo}) = D_{20}) \quad [277]$$

$$\boxed{\begin{array}{ll} \Box^*: & \mathsf{ARfSB}_{c'} = p(\mathsf{ARfSB}_{d'}) \quad [264'] \\ & \mathsf{ARfSB}_{d'} = \mathsf{ARfSB}_{a'} \quad [55'+] \\ & \mathsf{ARfSB}_{a'} = s(n_0) \quad [16'+] \\ & \mathsf{SFile}_{c'}(\mathsf{SNo}_{a'}) = d'_1 \quad [45'+] \\ & \mathsf{SNo}_{c'} = \mathsf{SNo}_{a'} \quad [47'+] \\ & \{D_{20} \leftarrow d'_1\} \end{array}}$$

$$c': \; \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'})) \quad [278]$$
$$c': \; (\mathsf{A})\Diamond(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'})) \quad [279]$$

auf q':

$$q' : [\,a', \{\ldots\}, d', \circ, \quad [280]$$
$$c', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'}))\},$$
$$w', \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'}))\}, \infty]$$

$$w': \; \neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{a'})) \quad [281]$$
$$w': \; \mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d'_1, \mathsf{SBit}_{c'}) \quad [282]$$

$$\boxed{\begin{array}{ll} \Box^*: & \mathsf{SBit}_{c'} = \mathsf{SBit}_{a'} \quad [46'+] \\ & (281, 282) \end{array}}$$

18 Theorem 2: Aktuelles Datum wird abgespeichert

$$\mathsf{A}\Box(\forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit)))$$

Als nach außen sichtbare Aussage folgt daraus

$$\mathsf{A}\Box(\forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit)))$$

Beweisskizze:

Als erstes wird die negierte Behauptung aufgelöst. Die Semantik des Tableaux bringt es mit sich, daß a der *erste* Zustand, in dem die Behauptung nicht gilt, ist: Ausgehend von a gibt es einen Pfad q, auf dem kein Knoten erreichbar ist, in dem $\mathsf{RFile}(\mathsf{SNo}_a) = \mathsf{SFile}(\mathsf{SNo}_a)$ und $\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})$ ist. Im weiteren wird dieser Pfad untersucht:

SFile bleibt immer unverändert. SBit und SNo bleiben unverändert, bis irgendwann ProcAck angewendet wird ([27],[30]).

1.Fall: Es gibt einen (ersten) Folgezustand b ([34]), in dem ProcAck angewendet wird:
Bis unmittelbar vor diesem bleiben SBit und SNo unverändert und in dessen Vorgängerzustand d ist $\mathsf{Bit}(\mathsf{SIM}_d) = \mathsf{SBit}_d$ ([47]). Mit Korollar 3 folgt daraus unter anderem, daß $\mathsf{RFile}_d(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo}_d)$ und $\mathsf{RBit}_d = \mathsf{flip}(\mathsf{SBit}_d)$ ist.

2.Fall: Es gibt keinen Folgezustand, in dem ProcAck angewendet wird, damit bleiben SBit und SNo immer unverändert ([35]).

Mit derselben Argumentationskette wie in Korollar 3 zeigt man, daß $\mathsf{RBit}_a = \mathsf{SBit}_a$ ist ([57]), denn aus $\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a)$ würde $\mathsf{RNo}_a = \mathsf{SNo}_a + 1$, $\mathsf{RFile}(\mathsf{RNo}_a - 1) \neq \bot$ und $\mathsf{RFile}_a(\mathsf{RNo}_a - 1) = \mathsf{RFile}_a(\mathsf{SNo}_a)$ folgen.

RBit bleibt unverändert, bis AccDat angewendet wird.

Ist dies in einem Folgegzustand f der Fall ([67]), so stellt man fest, daß in dessen Vorgängerzustand g $\mathsf{RBit}_g = \mathsf{SBit}_g$ und in f $\mathsf{RBit}_f = \mathsf{flip}(\mathsf{SBit}_f)$ [89] und damit mit der o.g. Argumentationskette $\mathsf{RFile}_f(\mathsf{RNo}_f - 1) = \mathsf{RFile}_f(\mathsf{SNo}_f)$ ist.

Der Fall, daß AccDat nie angewendet wird, kann auf einem fairen Pfad nur eintreten, wenn es einen Folgezustand h von a gibt, ab dem AccDat nie mehr anwendbar ist [113]. Anwendung von Lemma 7 auf h ergibt, daß auf q ein Zustand k erreichbar ist, in dem $\mathsf{Bit}(\mathsf{RIM}_k) = \mathsf{SBit}_k$ ist. Nachdem bereits festgestellt wurde, daß RBit und SBit unverändert bleiben, gilt also hier $\mathsf{Bit}(\mathsf{RIM}_k) = \mathsf{RBit}_k$ – und es ist AccDat anwendbar.

$$0:\ \neg(\mathsf{A}\Box(\forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit)))) \quad [1]$$

$$p : [\,0, \emptyset, \infty] \quad [2]$$

$$0:\ p\,\neg(\Box(\forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit)))) \quad [3]$$

$$0:\ p\,\Diamond\neg(\forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit))) \quad [3.2]$$

$$0:\ \neg(\forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \rightarrow \quad [4]$$
$$\mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit)))$$

$\boxed{\text{wie [6] ff. mit } 0 = a, \text{ [5] nicht verwenden.}}$

$$0:\ \forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit)) \quad [5]$$

$$0:\ (p)\Diamond\neg(\forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit))) \quad [6]$$

$$p : [\,0, \{[5]\}, a, \emptyset, \infty] \quad [7]$$

$$a:\ \neg(\forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit))) \quad [8]$$

$$a:\ \neg(\nabla SNo, SBit : \mathsf{SFile}(SNo) = d_1 \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(SBit))) \quad [9]$$

$$a:\ \neg(\mathsf{SFile}(\mathsf{SNo}_a) = d_1 \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a))) \quad [10]$$

$$a:\ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [11]$$

$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [11']$$

$$a:\ \neg\mathsf{A}\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [12]$$

$$q : [\,a, \emptyset, \infty] \quad [13]$$

$$a:\ q\,\neg(\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a))) \quad [14]$$

$$a:\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [15]$$

$$a:\ (q)\neg(\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a))) \quad [16]$$

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a))\}, \infty] \quad [17]$$

aus SData:

$$a:\ \forall D, N : \mathsf{SFile}(N) = D \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N) = D) \quad [18]$$

$$a:\ \mathsf{SFile}(N_2) = D_2 \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N_2) = D_2) \quad [19]$$

$$a:\ \neg(\mathsf{SFile}(N_2) = D_2) \quad [20]$$

$$\mathsf{SFile}_a(N_2) \neq D_2 \quad [20']$$

$$\Box\ \{N_2 \leftarrow \mathsf{SNo}_a, D_2 \leftarrow d_1\}(11', 20')$$

$$a:\ \mathsf{A}\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1) \quad [21]$$

$$a:\ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [22]$$

$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [22']$$

$$a:\ (\mathsf{A})\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1) \quad [23]$$

auf q:

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, (\mathsf{A})\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1)\}, \infty] \quad [24]$$

$\hookrightarrow$ S. 290

$$\vdots$$

von [24] (S. 289):

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, (\mathsf{A})\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1)\}, \infty] \quad [24]$$

$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [11']$$

$$a : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [15]$$

$$|$$

aus SBit:

$$a : \ \nabla SBit : \mathsf{A}(\mathsf{SBit} = SBit \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [25]$$

$$a : \ \mathsf{A}(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [26]$$

$$a : \ (\mathsf{A})(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}) \quad [27]$$

aus SNo:

$$a : \ \nabla SNo : \mathsf{A}(\mathsf{SNo} = SNo \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [28]$$

$$a : \ \mathsf{A}(\mathsf{SNo} = \mathsf{SNo}_a \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [29]$$

$$a : \ (\mathsf{A})(\mathsf{SNo} = \mathsf{SNo}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}) \quad [30]$$

[27] und [30] auflösen:

$$\begin{aligned} q : [\,a, \{&\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \quad [35]\\ &\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true}),\\ &(\mathsf{A})(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}),\\ &(\mathsf{A})(\mathsf{SNo} = \mathsf{SNo}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true})\}, \infty] \end{aligned}$$

↪ S. 293

$$\begin{aligned} q : [\,a, \{&\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \quad [31]\\ &\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true}),\\ &(\mathsf{A})(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}), (\mathsf{A})(\mathsf{SNo} = \mathsf{SNo}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true})\},\\ b, \{&\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1\}, \infty] \end{aligned}$$

$$|$$

$$b : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [32]$$

$$b : \ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [33]$$

$$b : \ \mathsf{ProcAck} = \mathsf{true} \quad [34]$$

↪ S. 291

$$\vdots$$

von [34] (S. 290):

$$q : [\, a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \quad [31]$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\},$$
$$b, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1\}, \infty]$$
$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [11']$$
$$a : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [15]$$

Vorgängerzustand d von b betrachten:

$$q : [\, a, \circ, \quad [36]$$
$$b, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)),$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1\}, \infty]$$

wie [37] mit a anstelle d und
$a : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a))$ [15]
$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1$ [11′]

$$q : [\, a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \quad [37]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a\},$$
$$d, \circ, b, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)),$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1\}, \infty]$$
$$d : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [38]$$
$$d : \ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [39]$$
$$d : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [40]$$
$$d : \ \mathsf{SNo} = \mathsf{SNo}_a \quad [41]$$
$$\mathsf{SFile}_d(\mathsf{SNo}_a) = d_1 \quad [39']$$
$$\mathsf{SBit}_d = \mathsf{SBit}_a \quad [40']$$
$$\mathsf{SNo}_d = \mathsf{SNo}_a \quad [41']$$

aus PA1:

$$d : \ \mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}) \rightarrow \exists D : \mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit}) \quad [42]$$

$$d : \ \neg\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}) \quad [43]$$
$$d : \ (\mathsf{A})\neg\circ(\mathsf{ProcAck} = \mathsf{true}) \quad [45]$$

auf q:

$$b : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [46]$$
$$\Box \ (34, 46)$$

$$d : \ \exists D : \mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit}) \quad [44]$$
$$d : \ \mathsf{SIM} = \mathsf{msg}(d_3, \mathsf{SBit}) \quad [47]$$
$$\mathsf{SIM}_d = \mathsf{msg}(d_3, \mathsf{SBit}_d) \quad [47']$$

$\hookrightarrow$ S. 292

$$\vdots$$

von [47] (S. 291):

$$q : [a, \{\ldots\}, d, \circ, b, \{\ldots\}, \infty] \quad [37]$$
$$d : \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \land \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [38]$$
$$\mathsf{SFile}_d(\mathsf{SNo}_a) = d_1 \quad [39']$$
$$\mathsf{SBit}_d = \mathsf{SBit}_a \quad [40']$$
$$\mathsf{SNo}_d = \mathsf{SNo}_a \quad [41']$$
$$\mathsf{SIM}_d = \mathsf{msg}(d_3, \mathsf{SBit}_d) \quad [47']$$

mit Korollar 3:

$$d : \forall D : \mathsf{SIM} = \mathsf{msg}(D, SBit) \to (\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \land \mathsf{RNo} = s(\mathsf{SNo}) \land \mathsf{RFile}(\mathsf{SNo}) = \mathsf{SFile}(\mathsf{SNo})) \quad [48]$$

$$d : \mathsf{SIM} = \mathsf{msg}(D_4, \mathsf{SBit}) \to (\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \land \mathsf{RNo} = s(\mathsf{SNo}) \land \mathsf{RFile}(\mathsf{SNo}) = \mathsf{SFile}(\mathsf{SNo})) \quad [49]$$

$$d : \neg(\mathsf{SIM} = \mathsf{msg}(D_4, \mathsf{SBit})) \quad [50]$$
$$\mathsf{SIM}_d \neq \mathsf{msg}(D_4, \mathsf{SBit}_d) \quad [50']$$
$$\Box \ \{D_4 \leftarrow d_3\}(47', 50')$$

$$d : \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \quad [51]$$
$$d : \mathsf{RNo} = s(\mathsf{SNo}) \quad [52]$$
$$d : \mathsf{RFile}(\mathsf{SNo}) = \mathsf{SFile}(\mathsf{SNo}) \quad [53]$$
$$\mathsf{RBit}_d = \mathsf{flip}(\mathsf{SBit}_d) \quad [51']$$
$$\mathsf{RNo}_d = s(\mathsf{SNo}_d) \quad [52']$$
$$\mathsf{RFile}_d(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo}_d) \quad [53']$$

aus [38]:

$$d : \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1) \quad [54]$$
$$\mathsf{RFile}_d(\mathsf{SNo}_a) \neq d_1 \quad [54']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{RFile}_d(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo}_d) \quad [53'] \\ & \mathsf{SNo}_d = \mathsf{SNo}_a \quad [41'] \\ & \mathsf{SFile}_d(\mathsf{SNo}_a) = d_1 \quad [54'] \\ & \mathsf{RFile}_d(\mathsf{SNo}_a) \neq d_1 \quad [39'] \end{array}}$$

$$d : \neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [55]$$
$$\mathsf{RBit}_d \neq \mathsf{flip}(\mathsf{SBit}_a) \quad [55']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{RBit}_d = \mathsf{flip}(\mathsf{SBit}_d) \quad [51'] \\ & \mathsf{SBit}_d = \mathsf{SBit}_a \quad [40'] \\ & \mathsf{RBit}_d \neq \mathsf{flip}(\mathsf{SBit}_a) \quad [55'] \end{array}}$$

$$\vdots$$

von [35] (S. 290):

$$q : [\, a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \quad [35]$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\}, \infty]$$

$$|$$

$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [11']$$
$$a : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [15]$$

$$|$$

aus BS:

$$a : \ \mathsf{RBit} = \mathsf{SBit} \vee \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \quad [56]$$

$$a : \ \mathsf{RBit} = \mathsf{SBit} \quad [57]$$
$$\mathsf{RBit}_a = \mathsf{SBit}_a \quad [57']$$

$$a : \ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \quad [58]$$
$$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a) \quad [58']$$

$\hookrightarrow$ S. 299

$$|$$

aus RBit:

$$a : \ \nabla RBit : \mathsf{A}(\mathsf{RBit} = RBit \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \quad [59]$$
$$a : \ \mathsf{A}(\mathsf{RBit} = RBit_a \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \quad [60]$$
$$a : \ (\mathsf{A})(\mathsf{RBit} = \mathsf{RBit}_a \ \mathsf{unless} \ \mathsf{AccDat} = \mathsf{true}) \quad [61]$$

$$q : [\, a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \quad [62]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a,$$
$$\mathsf{SNo} = \mathsf{SNo}_a, \mathsf{RBit} = \mathsf{RBit}_a\},$$
$$f, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)),$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a\}, \infty]$$

$$|$$

$$f : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [63]$$
$$f : \ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [64]$$
$$f : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [65]$$
$$f : \ \mathsf{SNo} = \mathsf{SNo}_a \quad [66]$$
$$f : \ \mathsf{AccDat} = \mathsf{true} \quad [67]$$
$$\mathsf{SFile}_f(\mathsf{SNo}_a) = d_1 \quad [64']$$
$$\mathsf{SBit}_f = \mathsf{SBit}_a \quad [65']$$
$$\mathsf{SNo}_f = \mathsf{SNo}_a \quad [66']$$

$\hookrightarrow$ S. 294

$$q : [\, a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)), \quad [68]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a,$$
$$\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SNo} = \mathsf{SNo}_a,$$
$$\mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{AccDat} = \mathsf{true})\}, \infty]$$

$\hookrightarrow$ S. 297

$\vdots$

von [67] (S. 293):

$$q : [\,a, \{\mathsf{SNo} = \mathsf{SNo}_a, \mathsf{RBit} = \mathsf{RBit}_a\}, f, \{\ldots\}, \infty] \quad [62]$$

$$\mathsf{RBit}_a = \mathsf{SBit}_a \quad [57']$$

$$f :\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [63]$$

$$\mathsf{SFile}_f(\mathsf{SNo}_a) = d_1 \quad [64']$$

$$\mathsf{SBit}_f = \mathsf{SBit}_a \quad [65']$$

$$\mathsf{SNo}_f = \mathsf{SNo}_a \quad [66']$$

$$f :\ \mathsf{AccDat} = \mathsf{true} \quad [67]$$

Vorgängerzustand von f betrachten:

$$q : [\,a, \circ, f, \{\ldots\}, \infty] \quad [69]$$

$\boxed{\text{wie [70] mit } a \text{ anstelle } g}$

$$q : [\,a, \{\mathsf{SNo} = \mathsf{SNo}_a, \mathsf{RBit} = \mathsf{SBit}_a\} \quad [70]$$
$$g, \circ, f, \{\ldots\}, \infty]$$

$$g :\ \mathsf{SNo} = \mathsf{SNo}_a \quad [71]$$

$$g :\ \mathsf{RBit} = \mathsf{SBit}_a \quad [72]$$

$$\mathsf{SNo}_g = \mathsf{SNo}_a \quad [71']$$

$$\mathsf{RBit}_g = \mathsf{RBit}_a \quad [72']$$

aus AD1:

$$g :\ \mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}) \rightarrow \exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit}) \quad [73]$$

$$g :\ \neg\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}) \quad [74]$$

$$g :\ (\mathsf{A})\neg\circ(\mathsf{AccDat} = \mathsf{true}) \quad [76]$$

auf q:

$$f :\ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [77]$$

$$\Box\ (67, 77)$$

$$g :\ \exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit}) \quad [75]$$

$$g :\ \mathsf{RIM} = \mathsf{msg}(d_5, \mathsf{RBit}) \quad [78]$$

$$\mathsf{RIM}_g = \mathsf{msg}(d_5, \mathsf{RBit}_g) \quad [78']$$

aus AD2:

$$g :\ \forall D : \nabla RBit, RNo : \mathsf{RIM} = \mathsf{msg}(D, RBit) \rightarrow \quad [79]$$
$$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(RNo) = D \wedge \mathsf{RNo} = s(RNo) \wedge \mathsf{RBit} = \mathsf{flip}(RBit)))$$

$$g :\ \nabla RBit, RNo : \mathsf{RIM} = \mathsf{msg}(D_6, RBit) \rightarrow \quad [80]$$
$$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(RNo) = D_6 \wedge \mathsf{RNo} = s(RNo) \wedge \mathsf{RBit} = \mathsf{flip}(RBit)))$$

$$g :\ \mathsf{RIM} = \mathsf{msg}(D_6, \mathsf{RBit}_g) \rightarrow \quad [81]$$
$$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(\mathsf{RNo}_g) = D_6 \wedge \mathsf{RNo} = s(\mathsf{RNo}_g) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_g)))$$

$\hookrightarrow$ S. 295

$\vdots$

von [81] (S. 294):

$q : [\,a, \{\ldots\}, g, \circ, f, \{\ldots\}, \infty]$ [70]

$\mathsf{RBit}_a = \mathsf{SBit}_a$ [57′]

$f:\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a))$ [63]

$\mathsf{SFile}_f(\mathsf{SNo}_a) = d_1$ [64′]

$\mathsf{SBit}_f = \mathsf{SBit}_a$ [65′]

$\mathsf{SNo}_f = \mathsf{SNo}_a$ [66′]

$f:\ \mathsf{AccDat} = \mathsf{true}$ [67]

$\mathsf{RBit}_g = \mathsf{RBit}_a$ [72′]

$\mathsf{RIM}_g = \mathsf{msg}(d_5, \mathsf{RBit}_g)$ [78′]

$g:\ \mathsf{RIM} = \mathsf{msg}(D_6, \mathsf{RBit}_g) \rightarrow$ [81]
$\quad \mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(\mathsf{RNo}_g) = D_6 \wedge \mathsf{RNo} = s(\mathsf{RNo}_g) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_g)))$

$g:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_6, \mathsf{RBit}_g))$ [82]

$\mathsf{RIM}_g \neq \mathsf{msg}(D_6, \mathsf{RBit}_g)$ [82′]

$\Box\ \{D_6 \leftarrow d_5\}(78', 82')$

$g:\ \mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(\mathsf{RNo}_g) = d_5 \wedge \mathsf{RNo} = s(\mathsf{RNo}_g) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_g)))$ [83]

$g:\ (\mathsf{A})\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(\mathsf{RNo}_g) = d_5 \wedge \mathsf{RNo} = s(\mathsf{RNo}_g) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_g)))$ [84]

auf q:

$g:\ \mathsf{AccDat} = \mathsf{true} \rightarrow (\mathsf{RFile}(\mathsf{RNo}_g) = d_5 \wedge \mathsf{RNo} = s(\mathsf{RNo}_g) \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_g))$ [85]

$f:\ \neg(\mathsf{AccDat} = \mathsf{true})$ [86]

$\Box\ (67, 86)$

$f:\ \mathsf{RFile}(\mathsf{RNo}_g) = d_5$ [87]

$f:\ \mathsf{RNo} = s(\mathsf{RNo}_g)$ [88]

$f:\ \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_g)$ [89]

$\mathsf{RFile}_f(\mathsf{RNo}_g) = d_5$ [87′]

$\mathsf{RNo}_f = s(\mathsf{RNo}_g)$ [88′]

$\mathsf{RBit}_f = \mathsf{flip}(\mathsf{RBit}_g)$ [89′]

aus [63]:

$f:\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1)$ [90]

$\mathsf{RFile}_f(\mathsf{SNo}_a) \neq d_1$ [90′]

Lemma 4:

$f:\ (\mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}) \wedge$ [92]
$\quad (\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo}))$

$f:\ \mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}$ [93]

$f:\ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo})$ [94]

$\hookrightarrow$ S. 296

$f:\ \neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a))$ [91]

$\mathsf{RBit}_f \neq \mathsf{flip}(\mathsf{SBit}_a)$ [91′]

$\Box:\ \mathsf{RBit}_f = \mathsf{flip}(\mathsf{RBit}_g)$ [89′]
$\quad \mathsf{RBit}_g = \mathsf{RBit}_a$ [72′]
$\quad \mathsf{RBit}_a = \mathsf{SBit}_a$ [57′]
$\quad \mathsf{RBit}_f \neq \mathsf{flip}(\mathsf{SBit}_a))$ [91′]

$\vdots$

von [94] (S. 295):

$$q : [\,a, \{\ldots\}, g, \circ, f, \{\ldots\}, \infty]\quad [70]$$
$$\mathsf{SFile}_f(\mathsf{SNo}_a) = d_1\quad [64']$$
$$\mathsf{SBit}_f = \mathsf{SBit}_a\quad [65']$$
$$\mathsf{SNo}_f = \mathsf{SNo}_a\quad [66']$$
$$\mathsf{RBit}_g = \mathsf{SBit}_a\quad [72']$$
$$\mathsf{RNo}_f = s(\mathsf{RNo}_g)\quad [88']$$
$$\mathsf{RBit}_f = \mathsf{flip}(\mathsf{RBit}_g)\quad [89']$$
$$\mathsf{RFile}_f(\mathsf{SNo}_a) \neq d_1\quad [90']$$
$$f:\ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo})\quad [94]$$

$$f:\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}))\quad [95]$$
$$\mathsf{SBit}_f \neq \mathsf{flip}(\mathsf{RBit}_f)\quad [95']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{RBit}_f = \mathsf{flip}(\mathsf{RBit}_g)\quad [89'] \\ & \mathsf{RBit}_g = \mathsf{SBit}_a\quad [72'] \\ & \mathsf{SBit}_f = \mathsf{SBit}_a\quad [65'] \\ & \mathsf{SBit}_f \neq \mathsf{flip}(\mathsf{RBit}_f)\quad [95'] \end{array}}$$

$$f:\ \mathsf{RNo} = s(\mathsf{SNo})\quad [96]$$
$$\mathsf{RNo}_f = s(\mathsf{SNo}_f)\quad [96']$$

Lemma 6:

$$f:\ \forall N : \mathsf{RNo} = s(N) \rightarrow \mathsf{RFile}(N) \neq \bot\quad [97]$$
$$f:\ \mathsf{RNo} = s(N_7) \rightarrow \mathsf{RFile}(N_7) \neq \bot\quad [98]$$

$$f:\ \neg(\mathsf{RNo} = s(N_7))\quad [99]$$
$$\mathsf{RNo}_f \neq s(N_7)\quad [99']$$
$$\Box\ \{N_7 \leftarrow \mathsf{RNo}_g\}(88', 99')$$

$$f:\ \mathsf{RFile}(\mathsf{RNo}_g) \neq \bot\quad [100]$$
$$\mathsf{RFile}_f(\mathsf{RNo}_g) \neq \bot\quad [100']$$

Theorem 1:

$$f:\ \forall N : \mathsf{RFile}(N) = \bot \vee \mathsf{RFile}(N) = \mathsf{SFile}(N)\quad [101]$$
$$f:\ \mathsf{RFile}(N_8) = \bot \vee \mathsf{RFile}(N_8) = \mathsf{SFile}(N_8)\quad [102]$$

$$f:\ \mathsf{RFile}(N_8) = \bot\quad [103]$$
$$\mathsf{RFile}_f(N_8) = \bot\quad [103']$$
$$\Box\ \{N_8 \leftarrow \mathsf{RNo}_g\}(100', 103')$$

$$f:\ \mathsf{RFile}(\mathsf{RNo}_g) = \mathsf{SFile}(\mathsf{RNo}_g)\quad [104]$$
$$\mathsf{RFile}_f(\mathsf{RNo}_g) = \mathsf{SFile}_f(\mathsf{RNo}_g)\quad [104']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{SNo}_f = \mathsf{SNo}_a\quad [66'] \\ & \mathsf{RNo}_f = s(\mathsf{SNo}_f)\quad [96'] \\ & \mathsf{RNo}_f = s(\mathsf{RNo}_g)\quad [88'] \\ \hline & \rightarrow \mathsf{SNo}_a = \mathsf{RNo}_g \\ & \mathsf{SFile}_f(\mathsf{SNo}_a) = d_1\quad [64'] \\ & \mathsf{RFile}_f(\mathsf{RNo}_g) = \mathsf{SFile}_f(\mathsf{RNo}_g)\quad [104'] \\ & \mathsf{RFile}_f(\mathsf{SNo}_a) \neq d_1\quad [90'] \end{array}}$$

$\vdots$

von [68] (S. 293):

$$q : [\,a, \{\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true}), \quad [68]$$
$$\mathsf{SNo} = \mathsf{SNo}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{AccDat} = \mathsf{true})\}, \infty]$$

$|$

$$\mathsf{RBit}_a = \mathsf{SBit}_a \quad [57']$$

$|$

Fairness bzgl. AccDat:

$$a: \ \mathsf{R}((\Box\Diamond\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \to (\Diamond(\mathsf{AccDat} = \mathsf{true}))) \quad [105]$$

auf q:

$$a: \ (q)\Diamond(\neg(q\Diamond\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}))) \quad [106]$$

$|$

$$q : [\,a, \{\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \quad [108]$$
$$\mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true}),$$
$$\mathsf{RBit} = \mathsf{SBit}_a\},$$
$$h, \{\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a,$$
$$\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SNo} = \mathsf{SNo}_a,$$
$$\mathsf{RBit} = \mathsf{RBit}_a\}, \infty]$$

$|$

$$h: \ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [109]$$
$$h: \ \mathsf{SBit} = \mathsf{SBit}_a \quad [110]$$
$$h: \ \mathsf{SNo} = \mathsf{SNo}_a \quad [111]$$
$$h: \ \mathsf{RBit} = \mathsf{RBit}_a \quad [112]$$
$$\mathsf{SFile}_h(\mathsf{SNo}_a) = d_1 \quad [109']$$
$$\mathsf{SBit}_h = \mathsf{SBit}_a \quad [110']$$
$$\mathsf{SNo}_h = \mathsf{SNo}_a \quad [111']$$
$$\mathsf{RBit}_h = \mathsf{RBit}_a \quad [112']$$
$$h: \ q\neg(\Diamond\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [113]$$
$$h: \ \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [114]$$
$$h: \ (q)\Box\neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [115]$$

$$a: \ (q)\Diamond(\mathsf{AccDat} = \mathsf{true}) \quad [107]$$

$|$

$$q : [\,a, \{\ldots, \neg(\mathsf{AccDat} = \mathsf{true}), \ldots\}, \quad [134]$$
$$l, \{\ldots, \neg(\mathsf{AccDat} = \mathsf{true}), \ldots\}, \infty]$$

$|$

$$l: \ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [135]$$
$$l: \ \mathsf{AccDat} = \mathsf{true} \quad [136]$$
$$\Box \ (135, 136)$$

$$q : [\,a, \{\ldots\}, h, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}))\}, \infty] \quad [116]$$

$|$

aus Lemma 7:

$$h: \ \forall D : \nabla SBit : \mathsf{SFile}(\mathsf{SNo}) = D \to \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D, SBit)) \quad [117]$$
$$h: \ \nabla SBit : \mathsf{SFile}(\mathsf{SNo}) = D_9 \to \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D_9, SBit)) \quad [118]$$
$$h: \ \mathsf{SFile}(\mathsf{SNo}) = D_9 \to \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D_9, \mathsf{SBit}_h)) \quad [119]$$

$\hookrightarrow$ S. 298

$$\vdots$$

von [119] (S. 297):

$$q : [\, a, \{\ldots\}, h, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}))\}, \infty] \quad [116]$$

$$\mathsf{RBit}_a = \mathsf{SBit}_a \quad [57']$$

$$\mathsf{SFile}_h(\mathsf{SNo}_a) = d_1 \quad [109']$$

$$\mathsf{SNo}_h = \mathsf{SNo}_a \quad [111']$$

$$h : \ \mathsf{SFile}(\mathsf{SNo}) = D_9 \rightarrow \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D_9, \mathsf{SBit}_h)) \quad [119]$$

$$h : \ \neg(\mathsf{SFile}(\mathsf{SNo}) = D_9) \quad [120]$$

$$\mathsf{SFile}_h(\mathsf{SNo}_h) \neq D_9) \quad [120']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{SFile}_h(\mathsf{SNo}_a) = d_1 \quad [109'] \\ & \mathsf{SNo}_h = \mathsf{SNo}_a \quad [111'] \\ & \{D_9 \leftarrow d_1\} \end{array}}$$

$$h : \ \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D_9, \mathsf{SBit}_h)) \quad [121]$$

$$h : \ (\mathsf{A})\Diamond(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(D_9, \mathsf{SBit}_h)) \quad [122]$$

auf q:

$$q : [\, a, \{\ldots\}, h, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}))\}, \quad [123]$$

$$i, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}))\}, \infty]$$

$$i : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [124]$$

$$i : \ \mathsf{RBit} = \mathsf{RBit}_a \quad [125]$$

$$i : \ \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [126]$$

$$i : \ \mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a) \quad [127]$$

$$\mathsf{RBit}_i = \mathsf{RBit}_a \quad [125']$$

$$i : \ \mathsf{ProcAck} = \mathsf{true} \quad [128]$$

$$\Box \ (124, 128)$$

$$i : \ \mathsf{RIM} = \mathsf{msg}(d_1, \mathsf{SBit}_a) \quad [129]$$

$$\mathsf{RIM}_i = \mathsf{msg}(d_1, \mathsf{SBit}_a) \quad [129']$$

aus AD1:

$$i : \ (\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit})) \rightarrow \mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}) \quad [130]$$

$$i : \ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit})) \quad [131]$$

$$i : \ \neg(\mathsf{RIM} = \mathsf{msg}(D_{10}, \mathsf{RBit})) \quad [133]$$

$$\mathsf{RIM}_i \neq \mathsf{msg}(D_{10}, \mathsf{RBit}_i) \quad [133']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{RIM}_i = \mathsf{msg}(d_1, \mathsf{SBit}_a) \quad [129'] \\ & \mathsf{RBit}_i = \mathsf{RBit}_a \quad [125'] \\ & \mathsf{RBit}_a = \mathsf{SBit}_a \quad [57'] \\ & \{D_{10} \leftarrow d_1\} \end{array}}$$

$$i : \ \mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true}) \quad [132]$$

$$\Box^* \ (126, 132)$$

$\vdots$

von [58] (S. 293):

$q : [\,a, \{\ldots\}, \infty]$ [35]

$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1$ [11′]

$a :\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a))$ [15]

$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a)$ [58′]

aus [15]:

$a :\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1)$ [137] $\qquad$ $a :\ \neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a))$ [138]

$\mathsf{RFile}_a(\mathsf{SNo}_a) \neq d_1$ [137′] $\qquad$ $\mathsf{RBit}_a \neq \mathsf{flip}(\mathsf{SBit}_a)$ [138′]

$\qquad\qquad\qquad\qquad$ $\square\ (58', 138')$

mit Lemma 4:

$a :\ (\mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}) \wedge (\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo}))$ [139]

$a :\ \mathsf{SBit} = \mathsf{RBit} \rightarrow \mathsf{RNo} = \mathsf{SNo}$ [140]

$a :\ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \rightarrow \mathsf{RNo} = s(\mathsf{SNo})$ [141]

$a :\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}))$ [142] $\qquad$ $a :\ \mathsf{RNo} = s(\mathsf{SNo})$ [143]

$\mathsf{SBit}_a \neq \mathsf{flip}(\mathsf{RBit}_a)$ [142′] $\qquad$ $\mathsf{RNo}_a = s(\mathsf{SNo}_a)$ [143′]

$\square\ (58', 142')$

Lemma 6:

$a :\ \forall N : \mathsf{RNo} = s(N) \rightarrow \mathsf{RFile}(N) \neq \bot$ [144]

$a :\ \mathsf{RNo} = s(N_{11}) \rightarrow \mathsf{RFile}(N_{11}) \neq \bot$ [145]

$a :\ \neg(\mathsf{RNo} = s(N_{11}))$ [146] $\qquad$ $a :\ \mathsf{RFile}(\mathsf{SNo}_a) \neq \bot$ [147]

$\mathsf{RNo}_a \neq s(N_{11})$ [146′] $\qquad$ $\mathsf{RFile}_a(\mathsf{SNo}_a) \neq \bot$ [147′]

$\square\ \{N_{11} \leftarrow \mathsf{SNo}_a\}(143', 146')$

Theorem 1:

$a :\ \forall N : \mathsf{RFile}(N) = \bot \vee \mathsf{RFile}(N) = \mathsf{SFile}(N)$ [148]

$a :\ \mathsf{RFile}(N_{12}) = \bot \vee \mathsf{RFile}(N_{12}) = \mathsf{SFile}(N_{12})$ [149]

$a :\ \mathsf{RFile}(N_{12}) = \bot$ [150] $\qquad$ $a :\ \mathsf{RFile}(\mathsf{SNo}_a) = \mathsf{SFile}(\mathsf{SNo}_a)$ [151]

$\mathsf{RFile}_a(N_{12}) = \bot$ [150′] $\qquad$ $\mathsf{RFile}_a(\mathsf{SNo}_a) = \mathsf{SFile}_a(\mathsf{SNo}_a)$ [151′]

$\square\ \{N_{12} \leftarrow \mathsf{SNo}_a\}(147', 150')$

$$\boxed{\begin{array}{ll} \square : & \mathsf{RFile}_a(\mathsf{SNo}_a) = \mathsf{SFile}_a(\mathsf{SNo}_a)\ \ [151'] \\ & \mathsf{RFile}_a(\mathsf{SNo}_a) \neq d_1\ \ [137'] \\ & \mathsf{SFile}_a(\mathsf{SNo}_a) = d_1\ \ [11'] \end{array}}$$

19 Lemma 8: Verhalten von SQ

Lemma 8 macht eine analoge Aussage zu Lemma 7 über das Verhalten von SQ.

Angenommen wird eine Situation, in der SBit = flip(RBit) ist (also AccDat schon stattgefunden hat). Gezeigt wird, daß dann irgendwann eine Nachricht beim Sender ankommt, die das entsprechende Kontrollbit besitzt.

$$\forall N : \mathsf{A}\Box(\nabla SBit : (\mathsf{ASfSB} = N \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})) \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, SBit)))$$

Wie schon bei Lemma 7 ist N ein reiner Hilfsparameter und man erhält die Aussage

$$\mathsf{A}\Box(\nabla SBit : \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, SBit)))$$

Beweis:

Der Beweis verwendet Induktion über die natürlichen Zahlen. Mit $A(n)$ wird die Induktionsaussage der Behauptung für festes n bezeichnet, mit $B(n)$ die darin enthaltene modallogische Aussage für einen festen Zustand.

Induktionsanfang ASfSB = 0 [2]: Es gibt also einen Zustand a, in dem die Aussage für 0 nicht gilt. Nach Voraussetzung ist $\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a)$ [16]. Aus der Annahme, daß nach a ProcAck nicht mehr angewendet wird ergibt sich ([22]-[28]), daß SBit nicht mehr verändert wird.
RBit bleibt ebenfalls unverändert, bis in einem Zustand c AccDat ausgeführt wird [34], so lange gilt also auch RBit = flip(SBit). Dazu muß im Vorgängerzustand d $\mathsf{Bit}(\mathsf{RIM}_d) = \mathsf{RBit}_d = \mathsf{flip}(\mathsf{SBit}_d)$ sein. Ist dieses wiederum der Fall, so wäre nach Lemma 3 $\mathsf{RBit}_d = \mathsf{SBit}_d$.

Damit ergibt sich [35], daß RBit = flip(SBit) nie verändert wird.

ARfSB ändert sich nur, wenn AckMsg mit Nebenbedingung RBit = SBit oder SendCom oder ProcAck ausgeführt wird. Da RBit = flip(SBit) ist, und nach Voraussetzung ProcAck nicht ausgeführt werden soll, bleibt nur SendCom. Wegen ARfSB = 0 liest SendCom eine Nachricht mit Kontrollbit SBit, was in der angenommenen Situation nicht geschehen sollte.

Somit muß also ARfSB unverändert bleiben, d.h. insbesondere SendCom nie ausgeführt werden. Nach Fairnessvoraussetzung müßte es einen Zustand g [105] geben, ab dem SendCom nie mehr ausführbar ist.

Ist $\mathsf{SIM}_g = \perp$ [113], so ist SIM in allen Folgezuständen gleich $\perp$, da ClMsg nicht anwendbar ist, und SendCom nach Annahme nicht anwendbar sein soll ([115] ff.). Mit Lemma 7 erreicht man einen Folgezustand k, in dem RIM_k eine Nachricht mit $\mathsf{Bit}(\mathsf{RIM}_k) = \mathsf{SBit}_k = \mathsf{flip}(\mathsf{RBit}_k)$ enthält. Diese Situation bleibt unverändert, bis AckMsg ausgeführt wird, was nach Fairnessannahme ([149] ff.) auch irgendwann in einem Zustand l [148],[154] (RecCom ist nicht anwendbar, [153]) der Fall ist. Die Ausführung von AckMsg plaziert eine Nachricht in SQ, womit SendCom ausführbar wäre.

Ist $\mathsf{SIM}_g \neq \perp$ [196], so bleibt SIM $\neq \perp$, bis ClMsg ausgeführt wird [206]. Dies führt zu einem Folgezustand s, in dem $\mathsf{SIM}_s = \perp$ [209] ist, womit man nun genau so weit ist, wie eben mit g [113]. Die Annahme, ClMsg würde nie ausgeführt [204], ist ebenfalls unfair: Es müßte einen Folgezustand m geben, ab dem ClMsg nie mehr ausführbar ist. Da SIM $\neq \perp$ ist, ist – und bleibt – ClMsg ausführbar.

$$0:\ \neg(\forall N : A(N)) \quad [1]$$

$$0:\ \neg(A(0)) \quad [2]$$

$$0:\ \neg(\mathsf{A}\Box(\nabla SBit : (\mathsf{ASfSB} = 0 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})) \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, SBit)))) \quad [5]$$

$$0:\ A(n_0) \quad [3]$$

$$0:\ \neg(A(s(n_0))) \quad [4]$$

$\hookrightarrow$ S. 315

$$p : [\,0, \emptyset, \infty] \quad [6]$$

$$0:\ p\,\neg(\Box(\nabla SBit : (\mathsf{ASfSB} = 0 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})) \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, SBit)))) \quad [7]$$

$$0:\ \neg(\nabla SBit : (\mathsf{ASfSB} = 0 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})) \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, SBit))) \quad [8]$$

$\boxed{\text{wie [9] ff. mit 0 anstelle } a}$

$$0:\ (p)\neg(\Box(\nabla SBit : (\mathsf{ASfSB} = 0 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})) \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, SBit)))) \quad [9]$$

$$p : [\,0, \{B(0)\}, a, \emptyset, \infty] \quad [10]$$

$$a:\ \neg(\nabla SBit : (\mathsf{ASfSB} = 0 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})) \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, SBit))) \quad [11]$$

$$a:\ \neg((\mathsf{ASfSB} = 0 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})) \rightarrow \mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a))) \quad [13]$$

$$a:\ \mathsf{ASfSB} = 0 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \quad [14]$$

$$a:\ \neg\mathsf{A}\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)) \quad [15]$$

$$a:\ \mathsf{ASfSB} = 0 \quad [16]$$

$$a:\ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \quad [17]$$

$$\mathsf{ASfSB}_a = 0 \quad [16']$$

$$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a) \quad [17']$$

$$q : [\,a, \emptyset, \infty] \quad [18]$$

$$a:\ q\,\neg\Diamond^{+}(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)) \quad [19]$$

$$a:\ (q)\Box\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)) \quad [20]$$

$$q : [\,a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a))\}, \infty] \quad [21]$$

$\hookrightarrow$ S. 302

$\vdots$

von [21] (S. 301):

$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a))\}, \infty] \quad [21]$

$\mathsf{ASfSB}_a = 0 \quad [16']$

$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a) \quad [17']$

aus SBit:

$a : \ \nabla SBit : \mathsf{A}(\mathsf{SBit} = SBit \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [22]$

$a : \ \mathsf{A}(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [23]$

$a : \ (\mathsf{A})(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}) \quad [24]$

$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \ldots\}, \quad [25]$
$b, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \ldots\}, \infty]$

u.a.:

$b : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [26]$

$b : \ \mathsf{ProcAck} = \mathsf{true} \quad [27]$

$\Box \ (26, 27)$

$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)), \quad [28]$
$\mathsf{SBit} = \mathsf{SBit}_a\}, \infty]$

aus RBit:

$a : \ \nabla RBit : \mathsf{A}(\mathsf{RBit} = RBit \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \quad [29]$

$a : \ \mathsf{A}(\mathsf{RBit} = \mathsf{RBit}_a \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \quad [30]$

$a : \ (\mathsf{A})(\mathsf{RBit} = \mathsf{RBit}_a \ \mathsf{unless} \ \mathsf{AccDat} = \mathsf{true}) \quad [31]$

auf q:

$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)), \quad [32]$
$\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{AccDat} = \mathsf{true})\},$
$c, \{\mathsf{SBit} = \mathsf{SBit}_a\}, \infty]$

$c : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [33]$

$c : \ \mathsf{AccDat} = \mathsf{true} \quad [34]$

$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)), \quad [35]$
$\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{AccDat} = \mathsf{true}\}, \infty]$

$\hookrightarrow$ S. 304

Vorgängerzustand von c betrachten:

$q : [\, a, \circ, c, \{\ldots\}, \infty] \quad [36]$

$\boxed{\text{wie [37] mit } a \text{ anstelle } d.}$

$q : [\, a, \{\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a\}, \quad [37]$
$d, \circ, c, \{\mathsf{SBit} = \mathsf{SBit}_a\}, \infty]$

$d : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [38]$

$d : \ \mathsf{RBit} = \mathsf{RBit}_a \quad [39]$

$\mathsf{SBit}_d = \mathsf{SBit}_a \quad [38']$

$\mathsf{RBit}_d = \mathsf{RBit}_a \quad [39']$

$\hookrightarrow$ S. 303

$$\vdots$$

von [39] (S. 302):

$$q : [\, a, \{\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a\}, d, \circ, c, \{\mathsf{SBit} = \mathsf{SBit}_a\}, \infty] \quad [37]$$
$$c : \ \mathsf{AccDat} = \mathsf{true} \quad [34]$$
$$\mathsf{SBit}_d = \mathsf{SBit}_a \quad [38']$$
$$\mathsf{RBit}_d = \mathsf{RBit}_a \quad [39']$$

aus AD1:

$$d : \ (\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \to (\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit})) \quad [40]$$

$$d : \ \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [41]$$
$$d : \ (\mathsf{A})\circ(\neg(\mathsf{AccDat} = \mathsf{true})) \quad [43]$$

auf q:

$$c : \ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [44]$$
$$\square \ (34, 44)$$

$$d : \ \exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit}) \quad [42]$$
$$d : \ \mathsf{RIM} = \mathsf{msg}(d_2, \mathsf{RBit}) \quad [45]$$
$$\mathsf{RIM}_d = \mathsf{msg}(d_2, \mathsf{RBit}_d) \quad [45']$$

mit Lemma 3:

$$d : \ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit})) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', \mathsf{RBit})|Q')) \to \quad [46]$$
$$(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}) \to \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}))$$

$$d : \ \neg((\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit})) \vee \quad [47]$$
$$(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', \mathsf{RBit})|Q'))$$

$$d : \ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit})) \quad [49]$$
$$d : \ \neg(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', \mathsf{RBit})|Q') \quad [50]$$
$$d : \ \neg(\mathsf{RIM} = \mathsf{msg}(D_3, \mathsf{RBit})) \quad [51]$$
$$\mathsf{RIM}_d \neq \mathsf{msg}(D_3, \mathsf{RBit}_d) \quad [51']$$
$$\square \ \{D_3 \leftarrow d_2\}(45', 51')$$

$$d : \ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}_d) \to \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}) \quad [48]$$

$$d : \ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit})) \quad [52]$$
$$\mathsf{SBit}_d \neq \mathsf{flip}(\mathsf{RBit}_d) \quad [52]$$

$$\boxed{\begin{array}{ll} \square : & \mathsf{SBit}_d = \mathsf{SBit}_a \quad [38'] \\ & \mathsf{RBit}_d = \mathsf{RBit}_a \quad [39'] \\ & \mathsf{SBit}_d \neq \mathsf{flip}(\mathsf{RBit}_d) \quad [52] \end{array}}$$

$$d : \ \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}) \quad [53]$$
$$\mathsf{RBit}_d = \mathsf{flip}(\mathsf{RBit}_d) \quad [53']$$
$$\square$$

$\vdots$

von [35] (S. 302):

$$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)), \quad [35]$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{AccDat} = \mathsf{true}\}, \infty]$$
$$\mathsf{ASfSB}_a = 0 \quad [16']$$
$$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a) \quad [17']$$

$|$

aus SQF:

$$a : \ \nabla ARfSB : \mathsf{A}(\mathsf{ASfSB} = ARfSB \ \mathsf{unless}^+ \quad [54]$$
$$((\mathsf{AckMsg} = \mathsf{true} \wedge \mathsf{RBit} = \mathsf{SBit}) \vee \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}))$$

$|$

$$a : \ \mathsf{A}(\mathsf{ASfSB} = \mathsf{ARfSB}_a \ \mathsf{unless}^+ \ ((\mathsf{AckMsg} = \mathsf{true} \wedge \mathsf{RBit} = \mathsf{SBit}) \vee \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})) \quad [55]$$
$$a : \ (\mathsf{A})(\mathsf{ASfSB} = \mathsf{ARfSB}_a \ \mathsf{unless} \ ((\mathsf{AckMsg} = \mathsf{true} \wedge \mathsf{RBit} = \mathsf{SBit}) \vee \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})) \quad [56]$$

$$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)), \quad [63]$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{AccDat} = \mathsf{true}\}, \mathsf{ASfSB} = \mathsf{ASfSB}_a,$$
$$\neg((\mathsf{AckMsg} = \mathsf{true} \wedge \mathsf{RBit} = \mathsf{SBit}) \vee \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\}, \infty]$$

$\hookrightarrow$ S. 307

$$q : [\, a, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)), \quad [57]$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{AccDat} = \mathsf{true}), \mathsf{ASfSB} = \mathsf{ASfSB}_a,$$
$$\neg((\mathsf{AckMsg} = \mathsf{true} \wedge \mathsf{RBit} = \mathsf{SBit}) \vee \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})\},$$
$$e, \{\neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)),$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{AccDat} = \mathsf{true})\}, \infty]$$

$|$

$$e : \ \neg(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)) \quad [58]$$
$$e : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [59]$$
$$e : \ \mathsf{RBit} = \mathsf{RBit}_a \quad [60]$$
$$e : \ \mathsf{ASfSB} = \mathsf{ASfSB}_a \quad [61]$$
$$e : \ (\mathsf{AckMsg} = \mathsf{true} \wedge \mathsf{RBit} = \mathsf{SBit}) \vee \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true} \quad [62]$$

$|$

$$\mathsf{SBit}_e = \mathsf{SBit}_a \quad [59']$$
$$\mathsf{RBit}_e = \mathsf{RBit}_a \quad [60']$$
$$\mathsf{ASfSB}_e = \mathsf{ASfSB}_a \quad [61']$$

aus [58]:

$$e : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [64]$$
$$e : \ \neg(\mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_a)) \quad [65]$$
$$\mathsf{SIM}_e \neq \mathsf{msg}(\lambda, \mathsf{SBit}_a) \quad [65']$$

$\hookrightarrow$ S. 305

$\vdots$

von [65] (S. 304):

$q : [\,a, \{\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{ASfSB} = \mathsf{ASfSB}_a\}, e, \{\mathsf{SBit} = \mathsf{SBit}_a\}, \infty]$ [57]

$\mathsf{ASfSB}_a = 0$ [16′]

$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a)$ [17′]

$\mathsf{SBit}_e = \mathsf{SBit}_a$ [59′]

$\mathsf{RBit}_e = \mathsf{RBit}_a$ [60′]

$\mathsf{ASfSB}_e = \mathsf{ASfSB}_a$ [61′]

$e :$ $(\mathsf{AckMsg} = \mathsf{true} \wedge \mathsf{RBit} = \mathsf{SBit}) \vee \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true}$ [62]

$e :$ $\neg(\mathsf{ProcAck} = \mathsf{true})$ [64]

$\mathsf{SIM}_e \neq \mathsf{msg}(\lambda, \mathsf{SBit}_a)$ [65′]

$e :$ $\mathsf{AckMsg} = \mathsf{true}$ [66]

$e :$ $\mathsf{RBit} = \mathsf{SBit}$ [67]

$\mathsf{RBit}_e = \mathsf{SBit}_e$ [67′]

$\Box :$ $\mathsf{RBit}_e = \mathsf{SBit}_e$ [67]
$\mathsf{SBit}_e = \mathsf{SBit}_a$ [59′]
$\mathsf{RBit}_e = \mathsf{RBit}_a$ [60′]
$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a)$ [17′]

$e :$ $\mathsf{SendCom} = \mathsf{true}$ [68]

Vorgängerzustand von e:

$q : [\,a, \circ, e, \{\mathsf{SBit} = \mathsf{SBit}_a\}, \infty]$ [70]

$\boxed{\text{wie [71] mit } a \text{ anstelle } f}$

$q : [\,a, \{\ldots\}, f, \circ, e, \{\ldots\}, \infty]$ [71]

$f :$ $\mathsf{SBit} = \mathsf{SBit}_a$ [72]

$f :$ $\mathsf{ASfSB} = \mathsf{ASfSB}_a$ [73]

$\mathsf{SBit}_f = \mathsf{SBit}_a$ [72′]

$\mathsf{ASfSB}_f = \mathsf{ASfSB}_a$ [73′]

aus SC1:

$f :$ $\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}) \rightarrow (\mathsf{SIM} = \bot \wedge \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q)$ [74]

$f :$ $\neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))$ [75]

$f :$ $(\mathsf{A})\circ(\neg(\mathsf{SendCom} = \mathsf{true}))$ [77]

auf q:

$e :$ $\neg(\mathsf{SendCom} = \mathsf{true})$ [78]

$\Box$ (68, 78)

$f :$ $\mathsf{SIM} = \bot \wedge \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q$ [76]

$f :$ $\mathsf{SIM} = \bot$ [79]

$f :$ $\exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q$ [80]

$f :$ $\mathsf{SQ} = \mathsf{msg}(d_4, b_4)|q_4$ [81]

$\mathsf{SQ}_f = \mathsf{msg}(d_4, b_4)|q_4$ [81′]

$\hookrightarrow$ S. 306

$e :$ $\mathsf{ProcAck} = \mathsf{true}$ [69]

$\Box$ (64, 69)

$$\vdots$$

von [81] (S. 305):

$$q : [\,a, \{\ldots\}, f, \circ, e, \{\ldots\}, \infty]\quad [71]$$
$$\mathsf{ASfSB}_a = 0\quad [16']$$
$$\mathsf{SIM}_e \neq \mathsf{msg}(\lambda, \mathsf{SBit}_a)\quad [65']$$
$$e:\ \mathsf{SendCom} = \mathsf{true}\quad [68]$$
$$\mathsf{SBit}_f = \mathsf{SBit}_a\quad [72']$$
$$\mathsf{ASfSB}_f = \mathsf{ASfSB}_a\quad [73']$$
$$\mathsf{SQ}_f = \mathsf{msg}(d_4, b_4)|q_4\quad [81']$$

aus SQ0F:

$$f:\ \mathsf{ASfSB} = 0 \to (\mathsf{SQ} = \varepsilon \vee \exists D, Q : \mathsf{SQ} = \mathsf{msg}(\lambda, \mathsf{flip}(\mathsf{SBit}))|Q)\quad [82]$$

$$f:\ \neg(\mathsf{ASfSB} = 0)\quad [83]$$
$$\mathsf{ASfSB}_f \neq 0\quad [83']$$
$$\boxed{\begin{array}{ll}\Box: & \mathsf{ASfSB}_f = \mathsf{ASfSB}_a\quad [73'] \\ & \mathsf{ASfSB}_a = 0\quad [16']\end{array}}$$

$$f:\ \mathsf{SQ} = \varepsilon \vee \exists Q : \mathsf{SQ} = \mathsf{msg}(\lambda, \mathsf{flip}(\mathsf{SBit}))|Q\quad [84]$$

$$f:\ \mathsf{SQ} = \varepsilon\quad [85]$$
$$\mathsf{SQ}_f = \varepsilon\quad [85']$$
$$\Box\ (\mathrm{E3}, 81', 85')$$

$$f:\ \exists Q : \mathsf{SQ} = \mathsf{msg}(\lambda, \mathsf{SBit})|Q\quad [86]$$
$$f:\ \mathsf{SQ} = \mathsf{msg}(\lambda, \mathsf{SBit})|q_5\quad [87]$$
$$\mathsf{SQ}_f = \mathsf{msg}(\lambda, \mathsf{SBit}_f)|q_5\quad [87']$$

aus SC2:

$$f:\ \forall D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q \to \mathsf{A}\circ(\mathsf{SendCom} = \mathsf{true} \to \mathsf{SQ} = Q \wedge \mathsf{SIM} = \mathsf{msg}(D, B))\quad [88]$$
$$f:\ \mathsf{SQ} = \mathsf{msg}(D_6, B_6)|Q_6 \to \mathsf{A}\circ(\mathsf{SendCom} = \mathsf{true} \to \mathsf{SQ} = Q_6 \wedge \mathsf{SIM} = \mathsf{msg}(D_6, B_6))\quad [89]$$

$$f:\ \neg(\mathsf{SQ} = \mathsf{msg}(D_6, B_6)|Q_6)\quad [90]$$
$$\mathsf{SQ}_f \neq \mathsf{msg}(D_6, B_6)|Q_6\quad [90']$$
$$\Box\ \{D_6 \leftarrow \lambda,\ B_6 \leftarrow \mathsf{SBit}_f,\ Q_6 \leftarrow q_5\}(87', 90')$$

$$f:\ \mathsf{A}\circ(\mathsf{SendCom} = \mathsf{true} \to \mathsf{SQ} = q_5 \wedge \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_f))\quad [91]$$
$$f:\ (\mathsf{A})\circ(\mathsf{SendCom} = \mathsf{true} \to \mathsf{SQ} = q_5 \wedge \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_f))\quad [92]$$

auf q:

$$e:\ \mathsf{SendCom} = \mathsf{true} \to \mathsf{SQ} = q_5 \wedge \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_f)\quad [93]$$

$$e:\ \neg(\mathsf{SendCom} = \mathsf{true})\quad [94]$$
$$\Box\ (68, 94)$$

$$e:\ \mathsf{SQ} = q_5\quad [95]$$
$$e:\ \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_f)\quad [96]$$
$$\mathsf{SIM}_e = \mathsf{msg}(\lambda, \mathsf{SBit}_f)\quad [96']$$
$$\boxed{\begin{array}{ll}\Box: & \mathsf{SIM}_e = \mathsf{msg}(\lambda, \mathsf{SBit}_f)\quad [96'] \\ & \mathsf{SBit}_f = \mathsf{SBit}_a\quad [72'] \\ & \mathsf{SIM}_e \neq \mathsf{msg}(\lambda, \mathsf{SBit}_a)\quad [65']\end{array}}$$

$\vdots$

von [63] (S. 304):

$q : [\,a, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{SendCom} = \mathsf{true})\}, \infty]$ [63]

$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a)$ [17′]

|

Fairness bzgl. SendCom:

$a : \ \mathsf{R}((\Box\Diamond\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})) \rightarrow (\Diamond(\mathsf{SendCom} = \mathsf{true})))$ [97]

auf q:

$a : \ (q)\Diamond(\neg(q\ \Diamond\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})))$ [98]

|

$q : [\,a, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SBit} = \mathsf{SBit}_a,$ [100]
$\mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{SendCom} = \mathsf{true})\},$
$g, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SBit} = \mathsf{SBit}_a,$
$\mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{SendCom} = \mathsf{true})\}, \infty]$

|

$g : \ \neg(\mathsf{ProcAck} = \mathsf{true})$ [101]

$g : \ \mathsf{SBit} = \mathsf{SBit}_a$ [102]

$g : \ \mathsf{RBit} = \mathsf{RBit}_a$ [103]

$g : \ \neg(\mathsf{ProcAck} = \mathsf{true})$ [104]

$g : \ q\ \neg(\Diamond\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))$ [105]

|

$\mathsf{SBit}_g = \mathsf{SBit}_a$ [102′]

$\mathsf{RBit}_g = \mathsf{RBit}_a$ [103′]

$g : \ \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))$ [106]

$g : \ (q)\Box\neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))$ [107]

|

$a : \ (q)\Diamond(\mathsf{SendCom} = \mathsf{true})$ [99]

|

$q : [\,a, \{\neg(\mathsf{SendCom} = \mathsf{true})\},$ [227]
$v, \{\neg(\mathsf{SendCom} = \mathsf{true})\}, \infty]$

|

$v : \ \neg(\mathsf{SendCom} = \mathsf{true})$ [228]

$v : \ \mathsf{SendCom} = \mathsf{true}$ [229]

$\Box$ (228, 229)

$q : [\,a, \{\ldots\},$ [108]
$g, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{SendCom} = \mathsf{true}), \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))\}, \infty]$

aus SIM:

$g : \ \nabla SIM : \mathsf{A}(\mathsf{SIM} = \mathsf{SIM}\ \mathsf{unless}^+\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})$ [109]

$g : \ \mathsf{A}(\mathsf{SIM} = \mathsf{SIM}_g\ \mathsf{unless}^+\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})$ [110]

$g : \ (\mathsf{A})(\mathsf{SIM} = \mathsf{SIM}_g\ \mathsf{unless}\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})$ [111]

|

aus F2S:

$g : \ \mathsf{SIM} = \bot \vee \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)$ [112]

$g : \ \mathsf{SIM} = \bot$ [113]

$\mathsf{SIM}_g = \bot$ [113′]

$\hookrightarrow$ S. 308

$g : \ \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)$ [114]

$g : \ \mathsf{SIM} = \mathsf{msg}(d_{11}, b_{11})$ [196]

$\mathsf{SIM}_g = \mathsf{msg}(d_{11}, b_{11})$ [196′]

$\hookrightarrow$ S. 314

$$\vdots$$

von [113] (S. 307):

$$q : [a, \{\ldots\}, \quad [108]$$
$$g, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{SendCom} = \mathsf{true}), \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))\}, \infty]$$
$$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a) \quad [17']$$
$$\mathsf{SBit}_g = \mathsf{SBit}_a \quad [102']$$
$$\mathsf{RBit}_g = \mathsf{RBit}_a \quad [103']$$
$$g: \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})) \quad [106]$$
$$g: (\mathsf{A})(\mathsf{SIM} = \mathsf{SIM}_g \text{ unless } \mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true}) \quad [111]$$
$$\mathsf{SIM}_g = \bot \quad [113']$$

$$q : [a, \{\ldots\}, \quad [115]$$
$$g, \{\neg(\mathsf{SendCom} = \mathsf{true}), \mathsf{SIM} = \mathsf{SIM}_g\},$$
$$h, \{\neg(\mathsf{SendCom} = \mathsf{true}), \}, \infty]$$
$$h: \neg(\mathsf{SendCom} = \mathsf{true}) \quad [116]$$
$$h: \mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true} \quad [117]$$

$$h: \mathsf{SendCom} = \mathsf{true} \quad [119]$$
$$\square \ (116, 119)$$

$$h: \mathsf{CIMsg} = \mathsf{true} \quad [120]$$

Vorgängerzustand von h betrachten:

$$q : [a, \{\ldots\}, g, \circ, h, \{\ldots\}, \infty] \quad [121]$$

wie [122] mit g anstelle i.

$$q : [a, \{\ldots\}, g, \{\mathsf{SIM} = \mathsf{SIM}_g\}, i, \circ, h, \{\ldots\}, \infty] \quad [122]$$
$$i: \mathsf{SIM} = \mathsf{SIM}_g \quad [123]$$
$$\mathsf{SIM}_i = \mathsf{SIM}_g \quad [123']$$

aus CM1:

$$i: (\mathsf{E}\circ(\mathsf{CIMsg} = \mathsf{true})) \rightarrow (\exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)) \quad [124]$$

$$i: \neg(\mathsf{E}\circ(\mathsf{CIMsg} = \mathsf{true})) \quad [125]$$
$$i: (\mathsf{A})\neg(\circ(\mathsf{CIMsg} = \mathsf{true})) \quad [127]$$

auf q:

$$h: \neg(\mathsf{CIMsg} = \mathsf{true}) \quad [128]$$
$$\square \ (120, 128)$$

$$i: \exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B) \quad [126]$$
$$i: \mathsf{SIM} = \mathsf{msg}(d_7, b_7) \quad [129]$$
$$\mathsf{SIM}_i = \mathsf{msg}(d_7, b_7) \quad [129']$$

$$\boxed{\begin{array}{ll} \square : & \mathsf{SIM}_i = \mathsf{msg}(d_7, b_7) \quad [129'] \\ & \mathsf{SIM}_i = \mathsf{SIM}_g \quad [123'] \\ & \mathsf{SIM}_g = \bot \quad [113'] \end{array}}$$

$$q : [a, \{\ldots\}, \quad [118]$$
$$g, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RBit} = \mathsf{RBit}_a,$$
$$\neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})), \mathsf{SIM} = \mathsf{SIM}_g,$$
$$\neg(\mathsf{SendCom} = \mathsf{true} \vee \mathsf{CIMsg} = \mathsf{true})\}, \infty]$$

↪ S. 309

$$\vdots$$

von [118] (S. 308):

$$q : [\,a, \{\ldots\}, g, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})), \mathsf{SIM} = \mathsf{SIM}_g\}, \infty] \quad [118]$$

$$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a) \quad [17']$$

$$\mathsf{SBit}_g = \mathsf{SBit}_a \quad [102']$$

$$\mathsf{RBit}_g = \mathsf{RBit}_a \quad [103']$$

$$g : \ \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})) \quad [106]$$

$$\mathsf{SIM}_g = \perp \quad [113']$$

$$|$$

mit Lemma 7:

$$g : \ \nabla SBit, SFile, SNo : \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(SFile(SNo), SBit)) \quad [130]$$

$$g : \ \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g)) \quad [131]$$

$$g : \ (\mathsf{A})\Diamond(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g)) \quad [132]$$

auf q:

$$\begin{aligned} q : [\,a, \{\ldots\},& \qquad [133] \\ & g, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})), \mathsf{SIM} = \mathsf{SIM}_g\}, \\ & k, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})), \mathsf{SIM} = \mathsf{SIM}_g\}, \infty] \end{aligned}$$

$$|$$

$$k : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [134]$$

$$k : \ \mathsf{RBit} = \mathsf{RBit}_a \quad [135]$$

$$k : \ \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})) \quad [136]$$

$$k : \ \mathsf{SIM} = \mathsf{SIM}_g \quad [137]$$

$$k : \ \mathsf{ProcAck} = \mathsf{true} \vee \mathsf{RIM} = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g) \quad [138]$$

$$\mathsf{RBit}_k = \mathsf{RBit}_a \quad [135']$$

$$\mathsf{SIM}_k = \mathsf{SIM}_g \quad [137']$$

aus [138]:

$$k : \ \mathsf{ProcAck} = \mathsf{true} \quad [139] \qquad\qquad k : \ \mathsf{RIM} = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g) \quad [140]$$

$$\Box\ (134, 139) \qquad\qquad \mathsf{RIM}_k = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g) \quad [140']$$

$$|$$

aus RIM:

$$k : \ \nabla RIM : \mathsf{A}(\mathsf{RIM} = RIM \ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}) \quad [141]$$

$$k : \ \mathsf{A}(\mathsf{RIM} = \mathsf{RIM}_k \ \mathsf{unless}^+\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}) \quad [142]$$

$$k : \ (\mathsf{A})(\mathsf{RIM} = \mathsf{RIM}_k \ \mathsf{unless}\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}) \quad [143]$$

$\hookrightarrow$ S. 310

$\vdots$

von [143] (S. 309):

$q : [\,a, \{\ldots\}, g, \{\mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})), \mathsf{SIM} = \mathsf{SIM}_g\},$ [133]
$k, \{\mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})), \mathsf{SIM} = \mathsf{SIM}_g\}, \infty]$

|

$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a)$ [17′]
$\mathsf{SBit}_g = \mathsf{SBit}_a$ [102′]
$\mathsf{SIM}_g = \bot$ [113′]
$\mathsf{RIM}_k = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g)$ [140′]
$k :$ $(\mathsf{A})(\mathsf{RIM} = \mathsf{RIM}_k$ unless $\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [143]

$q : [\,a, \{\ldots\}, g, \{\ldots\},$ [144]
$k, \{\mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})),$
$\mathsf{SIM} = \mathsf{SIM}_g, \mathsf{RIM} = \mathsf{RIM}_k\},$
$l, \{\mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})),$
$\mathsf{SIM} = \mathsf{SIM}_g\}, \infty]$

|

$l :$ $\mathsf{RBit} = \mathsf{RBit}_a$ [145]
$l :$ $\neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))$ [146]
$l :$ $\mathsf{SIM} = \mathsf{SIM}_g$ [147]
$l :$ $\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [148]
$\mathsf{RBit}_l = \mathsf{RBit}_a$ [145′]
$\mathsf{SIM}_l = \mathsf{SIM}_g$ [147′]

$q : [\,a, \{\ldots\}, g, \{\ldots\},$ [149]
$k, \{\mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})),$
$\mathsf{SIM} = \mathsf{SIM}_g, \mathsf{RIM} = \mathsf{RIM}_k,$
$\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\}, \infty]$

↪ S. 313

Vorgängerzustand von l betrachten:

$q : [\,a, \{\ldots\}, g, \{\ldots\}, k, \circ, l, \{\ldots\}, \infty]$ [150]

$\boxed{\text{wie [151] mit } k \text{ anstelle } m}$

$q : [\,a, \{\ldots\}, g, \{\ldots\},$ [151]
$k, \{\ldots, \mathsf{RIM} = \mathsf{RIM}_k\},$
$m, \circ, l, \{\ldots\}, \infty]$

|

$m :$ $\mathsf{RIM} = \mathsf{RIM}_k$ [152]
$\mathsf{RIM}_m = \mathsf{RIM}_k$ [152′]

↪ S. 311

$$\vdots$$

von [152] (S. 310):

$q : [\,a, \{\ldots\}, g, \{\ldots\}, k, \{\ldots\}, m, \circ, l, \{\ldots\}, \infty]$ [151]

$|$

$\mathsf{SIM}_g = \bot$ [113′]

$\mathsf{RIM}_k = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g)$ [140′]

$\mathsf{SIM}_l = \mathsf{SIM}_g$ [147′]

$l :\ \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))$ [146]

$l :\ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true}$ [148]

$\mathsf{RIM}_m = \mathsf{RIM}_k$ [152′]

aus [148]:

$l :\ \mathsf{RecCom} = \mathsf{true}$ [153]

$|$

aus RC1:

$m :\ \mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}) \rightarrow (\mathsf{RIM} = \bot \wedge \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q)$ [155]

$m :\ \neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))$ [156]

$m :\ (\mathsf{A})\neg(\mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true}))$ [158]

auf q:

$l :\ \neg(\mathsf{RecCom} = \mathsf{true})$ [159]

$\square$ (153, 159)

$m :\ \mathsf{RIM} = \bot$ [157]

$m :\ \exists D, B, Q : \mathsf{RQ} = \mathsf{msg}(D, B)|Q$ [160]

$\mathsf{RIM}_m = \bot$ [157′]

$\square :\ \mathsf{RIM}_m = \bot$ [157′]
$\mathsf{RIM}_m = \mathsf{RIM}_k$ [152′]
$\mathsf{RIM}_k = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g)$ [140′]

$l :\ \mathsf{AckMsg} = \mathsf{true}$ [154]

$\hookrightarrow$ S. 312

$\vdots$

von [154] (S. 311):

$q : [a, \{\ldots\}, g, \{\ldots\}, k, \{\ldots\}, m, \circ, l, \{\ldots\}, \infty]$ [151]

$\mathsf{SIM}_g = \perp$ [113′]

$\mathsf{RIM}_k = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g)$ [140′]

$l : \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))$ [146]

$\mathsf{SIM}_l = \mathsf{SIM}_g$ [147′]

$\mathsf{RIM}_m = \mathsf{RIM}_k$ [152′]

$l : \mathsf{AckMsg} = \mathsf{true}$ [154]

aus AM2:

$m : \forall D, B : \nabla SQ : \mathsf{RIM} = \mathsf{msg}(D, B) \to \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \to (\mathsf{SQ} = SQ|\mathsf{msg}(\lambda, B) \wedge \mathsf{RIM} = \perp))$ [161]

$m : \nabla SQ : \mathsf{RIM} = \mathsf{msg}(D_9, B_9) \to \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \to (\mathsf{SQ} = SQ|\mathsf{msg}(\lambda, B_9) \wedge \mathsf{RIM} = \perp))$ [162]

$m : \mathsf{RIM} = \mathsf{msg}(D_9, B_9) \to \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \to (\mathsf{SQ} = \mathsf{SQ}_m|\mathsf{msg}(\lambda, B_9) \wedge \mathsf{RIM} = \perp))$ [163]

$m : \neg(\mathsf{RIM} = \mathsf{msg}(D_9, B_9))$ [164]

$\mathsf{RIM}_m \neq \mathsf{msg}(D_9, B_9)$ [164′]

$\square$: $\mathsf{RIM}_m = \mathsf{RIM}_k$ [152′]
$\mathsf{RIM}_k = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g)$ [140′]
$\{D_9 \leftarrow \mathsf{SFile}_g(\mathsf{SNo}_g),\ B_9 \leftarrow \mathsf{SBit}_g\}$

$m : \mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \to (\mathsf{SQ} = \mathsf{SQ}_m|\mathsf{msg}(\lambda, \mathsf{SBit}_g) \wedge \mathsf{RIM} = \perp))$ [165]

$m : (\mathsf{A})\circ(\mathsf{AckMsg} = \mathsf{true} \to (\mathsf{SQ} = \mathsf{SQ}_m|\mathsf{msg}(\lambda, \mathsf{SBit}_g) \wedge \mathsf{RIM} = \perp))$ [166]

auf q:

$l : \mathsf{AckMsg} = \mathsf{true} \to (\mathsf{SQ} = \mathsf{SQ}_m|\mathsf{msg}(\lambda, \mathsf{SBit}_g) \wedge \mathsf{RIM} = \perp)$ [167]

$l : \neg(\mathsf{AckMsg} = \mathsf{true})$ [168]

$\square$ (154, 168)

$l : \mathsf{SQ} = \mathsf{SQ}_m|\mathsf{msg}(\lambda, \mathsf{SBit}_g) \wedge \mathsf{RIM} = \perp$ [169]

$l : \mathsf{SQ} = \mathsf{SQ}_m|\mathsf{msg}(\lambda, \mathsf{SBit}_g)$ [170]

$\mathsf{SQ}_l = \mathsf{SQ}_m|\mathsf{msg}(\lambda, \mathsf{SBit}_g)$ [170′]

$l : \mathsf{RIM} = \perp$ [171]

aus SC1:

$l : (\mathsf{SIM} = \perp \wedge \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q) \to \mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})$ [172]

$l : \neg(\mathsf{SIM} = \perp \wedge \exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q)$ [173]

$l : \mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})$ [174]

$\square^*$ (146, 174)

$l : \neg(\mathsf{SIM} = \perp)$ [175]

$\mathsf{SIM}_l \neq \perp$ [175′]

$\square$: $\mathsf{SIM}_l \neq \perp$ [175′]
$\mathsf{SIM}_l = \mathsf{SIM}_g$ [147′]
$\mathsf{SIM}_g = \perp$ [113′]

$l : \neg(\exists D, B, Q : \mathsf{SQ} = \mathsf{msg}(D, B)|Q)$ [176]

$l : \neg(\mathsf{SQ} = \mathsf{msg}(D_{20}, B_{20})|Q_{20})$ [177]

$l : \mathsf{SQ}_l \neq \mathsf{msg}(D_{20}, B_{20})|Q_{20}$ [177′]

$\square$ (E2, 170′, 177′)

$$\vdots$$

von [149] (S. 310):

$q : [\,a, \{\ldots\}, g, \{\ldots\}, k, \{\mathsf{RBit} = \mathsf{RBit}_a, \mathsf{RIM} = \mathsf{RIM}_k, \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\}, \infty]$ [149]

$\mathsf{RIM}_k = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g)$ [140′]

$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a)$ [17′]

$\mathsf{SBit}_g = \mathsf{SBit}_a$ [102′]

|

Fairness bzgl. AckMsg:

$k :\ \mathsf{R}((\Box\Diamond\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})) \rightarrow (\Diamond(\mathsf{AckMsg} = \mathsf{true})))$ [178]

auf q:

$k :\ (q)\Diamond(\neg(q\ \Diamond\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})))$ [179]

|

$q : [\,a, \{\ldots\}, g, \{\ldots\},$ [181]
$k, \{\mathsf{RBit} = \mathsf{RBit}_a, \mathsf{RIM} = \mathsf{RIM}_k\},$
$n, \{\mathsf{RBit} = \mathsf{RBit}_a, \mathsf{RIM} = \mathsf{RIM}_k\}, \infty]$

|

$n :\ \mathsf{RBit} = \mathsf{RBit}_a$ [182]

$n :\ \mathsf{RIM} = \mathsf{RIM}_k$ [183]

$n :\ \neg(q\ \Diamond\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))$ [184]

$\mathsf{RBit}_n = \mathsf{RBit}_a$ [182′]

$\mathsf{RIM}_n = \mathsf{RIM}_k$ [183′]

|

$n :\ \neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))$ [185]

$n :\ (q)\neg(\mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true}))$ [186]

|

aus AM1:

$n :\ (\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{flip}(\mathsf{RBit}))) \rightarrow \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})$ [187]

$n :\ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{flip}(\mathsf{RBit})))$ [188]

$n :\ \neg(\mathsf{RIM} = \mathsf{msg}(D_{10}, \mathsf{flip}(\mathsf{RBit}))$ [190]

$\mathsf{RIM}_n \neq \mathsf{msg}(D_{10}, \mathsf{flip}(\mathsf{RBit}_n)$ [190′]

$\Box :\ \mathsf{RIM}_n = \mathsf{RIM}_k$ [183′]
$\mathsf{RIM}_k = \mathsf{msg}(\mathsf{SFile}_g(\mathsf{SNo}_g), \mathsf{SBit}_g)$ [140′]
$\mathsf{RBit}_n = \mathsf{RBit}_a$ [182′]
$\mathsf{RBit}_a = \mathsf{flip}(\mathsf{SBit}_a)$ [17′]
$\mathsf{SBit}_g = \mathsf{SBit}_a$ [102′]
$\{D_{10} \leftarrow \mathsf{SFile}_g(\mathsf{SNo}_g)\}$

$n :\ \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})$ [189]

$\Box\ (185, 189)$

$k :\ (q)\Diamond(\mathsf{AckMsg} = \mathsf{true})$ [180]

|

$q : [\,a, \{\ldots\}, g, \{\ldots\},$ [191]
$k, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\},$
$r, \{\neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})\}, \infty]$

|

$r :\ \neg(\mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$ [192]

$r :\ \mathsf{AckMsg} = \mathsf{true}$ [193]

aus [192]:

$r :\ \neg(\mathsf{RecCom} = \mathsf{true})$ [194]

$r :\ \neg(\mathsf{AckMsg} = \mathsf{true})$ [195]

$\Box\ (193, 195)$

$\vdots$

von [196] (S. 307):

$q : [\,a, \{\ldots\},$ [108]
$\quad g, \{\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{SendCom} = \mathsf{true})\}, \infty]$

$g :\ (\mathsf{A})(\mathsf{SIM} = \mathsf{SIM}_g \text{ unless } \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})$ [111]

$\mathsf{SIM}_g = \mathsf{msg}(d_{11}, b_{11})$ [196′]

$q : [\,a, \{\ldots\},$ [197]
$\quad g, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SBit} = \mathsf{SBit}_a,$
$\quad\quad \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{SendCom} = \mathsf{true}),$
$\quad\quad \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})), \mathsf{SIM} = \mathsf{SIM}_g\},$
$\quad s, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SBit} = \mathsf{SBit}_a,$
$\quad\quad \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{SendCom} = \mathsf{true}),$
$\quad\quad \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))\}, \infty]$

$s :\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [198]

$s :\ \mathsf{SBit} = \mathsf{SBit}_a$ [199]

$s :\ \mathsf{RBit} = \mathsf{RBit}_a$ [200]

$\mathsf{SBit}_s = \mathsf{SBit}_a$ [199′]

$\mathsf{RBit}_s = \mathsf{RBit}_a$ [200′]

$s :\ \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))$ [201]

$s :\ \neg(\mathsf{SendCom} = \mathsf{true})$ [202]

$s :\ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true}$ [203]

$s :\ \mathsf{SendCom} = \mathsf{true}$ [205]
$\square$ (202, 205)

$s :\ \mathsf{ClMsg} = \mathsf{true}$ [206]

aus CM2:

$s :\ \mathsf{ClMsg} = \mathsf{true} \rightarrow \mathsf{SIM} = \bot$ [207]

$s :\ \neg(\mathsf{ClMsg} = \mathsf{true})$ [208]
$\square$ (108, 208)

$s :\ \mathsf{SIM} = \bot$ [209]

$\mathsf{SIM}_s = \bot$ [209′]

wie [113] mit s anstelle g und
$\mathsf{SBit}_s = \mathsf{SBit}_a$ [199′]
$\mathsf{RBit}_s = \mathsf{RBit}_a$ [200′]
$s :\ \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true}))$ [201]
$\mathsf{SIM}_s = \bot$ [209′]

$q : [\,a, \{\ldots\},$ [204]
$\quad g, \{\neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{SBit} = \mathsf{SBit}_a,$
$\quad\quad \mathsf{RBit} = \mathsf{RBit}_a, \neg(\mathsf{SendCom} = \mathsf{true}),$
$\quad\quad \neg(\mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})), \mathsf{SIM} = \mathsf{SIM}_g,$
$\quad\quad \neg(\mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})\}, \infty]$

$\hookrightarrow$ S. 315

$$\vdots$$

von [204] (S. 314):

$$q : [\,a, \{\ldots\}, g, \{\mathsf{SIM} = \mathsf{SIM}_g, \neg(\mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})\}, \infty] \quad [204]$$

$$\mathsf{SIM}_g = \mathsf{msg}(d_{11}, b_{11}) \quad [196']$$

Fairness bzgl. ClMsg:

$$g : \ \mathsf{R}((\Box\Diamond \mathsf{E}\circ(\mathsf{ClMsg} = \mathsf{true})) \to (\Diamond(\mathsf{ClMsg} = \mathsf{true}))) \quad [210]$$

auf q:

$$g : \ (q)\Diamond(\neg(q \Diamond \mathsf{E}\circ(\mathsf{ClMsg} = \mathsf{true}))) \quad [211]$$

$$q : [\,a, \{\ldots\}, g, \{\mathsf{SIM} = \mathsf{SIM}_g\}, t, \{\mathsf{SIM} = \mathsf{SIM}_g\}, \infty] \quad [213]$$

$$t : \ \mathsf{SIM} = \mathsf{SIM}_g \quad [214]$$

$$\mathsf{SIM}_t = \mathsf{SIM}_g \quad [214']$$

$$t : \ \neg(q \Diamond \mathsf{E}\circ(\mathsf{ClMsg} = \mathsf{true})) \quad [215]$$

$$t : \ \neg(\mathsf{E}\circ(\mathsf{ClMsg} = \mathsf{true})) \quad [216]$$

$$t : \ (q)\Box\neg(\mathsf{E}\circ(\mathsf{ClMsg} = \mathsf{true})) \quad [217]$$

aus CM1:

$$t : \ (\exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)) \to \mathsf{E}\circ(\mathsf{ClMsg} = \mathsf{true}) \quad [218]$$

$$t : \ \neg(\exists D, B : \mathsf{SIM} = \mathsf{msg}(D, B)) \quad [219]$$

$$t : \ \neg(\mathsf{SIM} = \mathsf{msg}(D_{12}, B_{12})) \quad [221]$$

$$\mathsf{SIM}_t \neq \mathsf{msg}(D_{12}, B_{12}) \quad [221']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{SIM}_t = \mathsf{SIM}_g \quad [214'] \\ & \mathsf{SIM}_g = \mathsf{msg}(d_{11}, b_{11}) \quad [196'] \\ & \{D_{12} \leftarrow d_{11}, \ B_{12} \leftarrow b_{11}\} \end{array}}$$

$$t : \ \mathsf{E}\circ(\mathsf{ClMsg} = \mathsf{true}) \quad [220]$$

$$\Box^* \ (216, 220)$$

$$g : \ (q)\Diamond(\mathsf{ClMsg} = \mathsf{true}) \quad [212]$$

$$q : [\,a, \{\ldots\}, g, \{\neg(\mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})\}, u, \{\neg(\mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})\}, \infty] \quad [222]$$

$$u : \ \neg(\mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true}) \quad [223]$$

$$u : \ \mathsf{ClMsg} = \mathsf{true} \quad [224]$$

aus [223]:

$$u : \ \neg(\mathsf{SendCom} = \mathsf{true}) \quad [225]$$

$$u : \ \neg(\mathsf{ClMsg} = \mathsf{true}) \quad [226]$$

$$\Box \ (224, 226)$$

Induktionsschritt ((S. 301):):

Den Induktionsschritt erhält man aus dem Induktionsanfang wie schon in Lemma 7: Man unterscheidet, ob SendCom angewendet wird. Ist dies nicht der Fall weist man wie im Induktionsanfang nach, daß die Berechnung unfair ist. Anderenfalls wird mit SendCom entweder eine Nachricht mit dem gesuchten Kontrollbit SBit empfangen, oder die Anzahl der "alten" Nachrichten mit Kontrollbit flip(SBit) verringert sich.

20 Theorem 3: Garantie einer Quittung für aktuelles Datum

$$\mathsf{A}\Box(\forall D : \nabla SBit, SNo : \mathsf{SFile}(SNo) = D \to \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \land \exists D' : \mathsf{SIM} = \mathsf{msg}(D', SBit)))$$

Beweisskizze:

Als erstes wird die negierte Behauptung aufgelöst. Damit gibt es einen *ersten* Zustand a, in dem die Behauptung nicht gilt: Ausgehend von a gibt es einen Pfad q, auf dem kein Zustand erreichbar ist, in dem $\mathsf{RFile}(\mathsf{SNo}_a) = \mathsf{SFile}_a(\mathsf{SNo}_a)$ und eine Nachricht d existiert, so daß $\mathsf{SIM} = \mathsf{msg}(d, \mathsf{SBit}_a)$ ist. Im weiteren wird dieser Pfad untersucht:

SFile bleibt immer unverändert [23], SBit bleibt unverändert, bis irgendwann ProcAck angewendet wird.

Der Fall, in dem es einen (ersten) Folgezustand b ([31]) gibt, in dem ProcAck angewendet wird, verhält sich analog zu Theorem 2:
Bis unmittelbar vor diesem bleiben SBit und SNo unverändert und in dessen Vorgängerzustand d ist $\mathsf{Bit}(\mathsf{SIM}_d) = \mathsf{SBit}_d$ ([52]). Mit Korollar 3 folgt daraus unter anderem, daß $\mathsf{RFile}_d(\mathsf{SNo}_d) = \mathsf{SFile}_d(SNo_d) = \mathsf{SFile}_a(\mathsf{SNo}_a)$ ist [60].

Wird ProcAck nie angewendet, so bleibt SBit im weiteren Verlauf des Pfades q unverändert [31].
In diesem Fall erhält man aus Theorem 2 einen Folgezustand e, in dem $\mathsf{RFile}_e(\mathsf{SNo}_e) = \mathsf{SFile}_e(\mathsf{SNo}_e) = \mathsf{SFile}_a(\mathsf{SNo}_a)$ und $\mathsf{RBit}_e = \mathsf{flip}(\mathsf{SBit}_a) = \mathsf{flip}(\mathsf{SBit}_e)$ ist ([75]).
Im weiteren Verlauf des Pfades bleiben RBit und RFile unverändert ([84]): Beide können nur durch AccDat verändert werden, und dieses ist, wie in [83]-[103] festgestellt wird, nicht anwendbar, da der Empfänger keine entsprechende Nachricht mit $\mathsf{Bit}(\mathsf{RIM}) = \mathsf{RBit}$ erhalten kann.

In e ist Lemma 8 anwendbar, das aussagt, daß im weiteren Verlauf von q ein Zustand i erreichbar ist, in dem $\mathsf{Bit}(\mathsf{SIM}_i) = \mathsf{SBit}_e = \mathsf{SBit}_a$ ist ([128]). Nachdem oben bereits festgestellt wurde, daß RFile dabei unverändert bleibt, hat man den gesuchten Zustand erreicht.

$$0: \neg(\mathsf{A}\Box(\forall D: \nabla SBit, SNo: \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}(\Diamond(\mathsf{RFile}(SNo) = D \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', SBit)))) \quad [1]$$

$$p: [\,0, \emptyset, \infty] \quad [2]$$

$$0: \; p\,\neg(\Box(\forall D: \nabla SBit, SNo: \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', SBit)))) \quad [3]$$

$$0: \; \neg(\forall D: \nabla SBit, SNo: \mathsf{SFile}(SNo) = D \rightarrow \quad [4]$$
$$\mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', SBit)))$$

$\boxed{\text{wie [6] ff. mit } 0 = a\text{, [5] nicht verwenden.}}$

$$0: \; \forall D: \nabla SBit, SNo: \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', SBit)) \quad [5]$$

$$0: \; (p)\neg(\Box(\forall D: \nabla SBit, SNo: \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', SBit)))) \quad [6]$$

$$p: [\,0, \{[5]\}, a, \emptyset, \infty] \quad [7]$$

$$a: \; \neg(\forall D: \nabla SBit, SNo: \mathsf{SFile}(SNo) = D \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', SBit))) \quad [8]$$

$$a: \; \neg(\nabla SBit, SNo: \mathsf{SFile}(SNo) = d_1 \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = d_1 \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', SBit))) \quad [9]$$

$$a: \; \neg(\mathsf{SFile}(\mathsf{SNo}_a) = d_1 \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a))) \quad [10]$$

$$a: \; \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [11]$$

$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [11']$$

$$a: \; \neg(\mathsf{A}\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a))) \quad [12]$$

$$q: [\,a, \emptyset, \infty] \quad [13]$$

$$a: \; q\,\neg(\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a))) \quad [14]$$

$$a: \; \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)) \quad [15]$$

$$a: \; (q)\neg(\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a))) \quad [16]$$

$$q: [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a))\}, \infty] \quad [17]$$

aus SData:

$$a: \; \forall D, N: \mathsf{SFile}(N) = D \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N) = D) \quad [18]$$

$$a: \; \mathsf{SFile}(N_2) = D_2 \rightarrow \mathsf{A}\Box(\mathsf{SFile}(N_2) = D_2) \quad [19]$$

$$a: \; \neg(\mathsf{SFile}(N_2) = D_2) \quad [20]$$

$$\mathsf{SFile}_a(N_2) \neq D_2 \quad [20']$$

$$\Box \; \{N_2 \leftarrow \mathsf{SNo}_a, D_2 \leftarrow d_1\}(11', 20')$$

$$a: \; \mathsf{A}\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1) \quad [21]$$

$$a: \; \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [22]$$

$$a: \; (\mathsf{A})\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1) \quad [23]$$

$$q: [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D': \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \quad [24]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, (\mathsf{A})\Box(\mathsf{SFile}(\mathsf{SNo}_a) = d_1)\}, \infty]$$

↪ S. 318

$\vdots$

von [24] (S. 317):

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1\}, \infty] \quad [24]$$

$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [11']$$

$$a : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)) \quad [15]$$

aus SBit:

$$a : \ \nabla SBit : \mathsf{A}(\mathsf{SBit} = SBit \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [25]$$

$$a : \ \mathsf{A}(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [26]$$

$$a : \ (\mathsf{A})(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}) \quad [27]$$

auf q:

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \quad [32]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\}, \infty]$$

↪ S. 321

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \quad [28]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\},$$
$$b, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)),$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1\}, \infty]$$

$$b : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)) \quad [29]$$

$$b : \ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [30]$$

$$b : \ \mathsf{ProcAck} = \mathsf{true} \quad [31]$$

aus SNo:

$$a : \ \nabla SNo : \mathsf{A}(\mathsf{SNo} = SNo \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [33]$$

$$a : \ \mathsf{A}(\mathsf{SNo} = SNo_a \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [34]$$

$$a : \ (\mathsf{A})(\mathsf{SNo} = SNo_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}) \quad [35]$$

$$q : [\,a, \{\ldots, \neg(\mathsf{ProcAck} = \mathsf{true}), \ldots\}, \quad [36]$$
$$c, \{\ldots, \neg(\mathsf{ProcAck} = \mathsf{true}), \ldots\},$$
$$b, \{\ldots\}, \infty]$$

$$c : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [37]$$

$$c : \ \mathsf{ProcAck} = \mathsf{true} \quad [38]$$

$$\Box^* \ (37, 38)$$

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \quad [39]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a,$$
$$\neg(\mathsf{ProcAck} = \mathsf{true})\},$$
$$b, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)),$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1\}, \infty]$$

$$b : \ \mathsf{A}(\mathsf{SNo} = \mathsf{SNo}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}) \quad [40]$$

↪ S. 319

$\vdots$

von [40] (S. 318):

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \quad [39]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\},$$
$$b, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1\}, \infty]$$

$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1$ [11′]

$a:\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a))$ [15]

$b:\ \mathsf{ProcAck} = \mathsf{true}$ [31]

Vorgängerzustand von b betrachten:

$q : [\,a, \circ, b, \{\ldots\}, \infty]$ [41]

wie [42] mit a anstelle d und
$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1$ [11′]
$a:\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a))$ [15]

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \quad [42]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a\},$$
$$d, \circ, b, \{\ldots\}, \infty]$$

$d:\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a))$ [43]

$d:\ \mathsf{SFile}(\mathsf{SNo}_a) = d_1$ [44]

$d:\ \mathsf{SBit} = \mathsf{SBit}_a$ [45]

$d:\ \mathsf{SNo} = \mathsf{SNo}_a$ [46]

$\mathsf{SFile}_d(\mathsf{SNo}_a) = d_1$ [44′]

$\mathsf{SBit}_d = \mathsf{SBit}_a$ [45′]

$\mathsf{SNo}_d = \mathsf{SNo}_a$ [46′]

aus PA1:

$d:\ \mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}) \rightarrow \exists D : \mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit})$ [47]

$d:\ \neg\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true})$ [48]

$d:\ (\mathsf{A})\neg\circ(\mathsf{ProcAck} = \mathsf{true})$ [50]

auf q:

$b:\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [51]

$\square$ (31, 51)

$d:\ \exists D : \mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit})$ [49]

$d:\ \mathsf{SIM} = \mathsf{msg}(d_3, \mathsf{SBit})$ [52]

$\mathsf{SIM}_d = \mathsf{msg}(d_3, \mathsf{SBit}_d)$ [52′]

aus [43]:

$d:\ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1)$ [53]

$\mathsf{RFile}_d(\mathsf{SNo}_a) \neq d_1$ [53′]

$\hookrightarrow$ S. 320

$d:\ \neg(\exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a))$ [54]

$d:\ \neg(\mathsf{SIM} = \mathsf{msg}(D'_5, \mathsf{SBit}_a))$ [61]

$\mathsf{SIM}_d \neq \mathsf{msg}(D'_5, \mathsf{SBit}_a)$ [61′]

$\square$: $\mathsf{SIM}_d = \mathsf{msg}(d_3, \mathsf{SBit}_d)$ [52′]
$\mathsf{SBit}_d = \mathsf{SBit}_a$ [45′]
$\{D'_5 \leftarrow d_3\}$

$\vdots$

von [53] (S. 319):

$q : [a, \{\ldots\}, d, \circ, b, \{\ldots\}, \infty]$ [42]

$\mathsf{SFile}_d(\mathsf{SNo}_a) = d_1$ [44′]

$\mathsf{SNo}_d = \mathsf{SNo}_a$ [46′]

$\mathsf{SIM}_d = \mathsf{msg}(d_3, \mathsf{SBit}_d)$ [52′]

$\mathsf{RFile}_d(\mathsf{SNo}_a) \neq d_1$ [53′]

|

mit Korollar 3:

$d : \forall D : (\mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit}) \rightarrow (\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \mathsf{RNo} = s(\mathsf{SNo}) \wedge \mathsf{RFile}(\mathsf{SNo}) = \mathsf{SFile}(\mathsf{SNo})))$ [55]

$d : \mathsf{SIM} = \mathsf{msg}(D_4, \mathsf{SBit}) \rightarrow (\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \mathsf{RNo} = s(\mathsf{SNo}) \wedge \mathsf{RFile}(\mathsf{SNo}) = \mathsf{SFile}(\mathsf{SNo}))$ [56]

$d : \neg(\mathsf{SIM} = \mathsf{msg}(D_4, \mathsf{SBit}))$ [57]

$\mathsf{SIM}_d \neq \mathsf{msg}(D_4, \mathsf{SBit}_d))$ [57′]

$\square\ \{D_4 \leftarrow d_3\}(52', 57')$

$d : \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})$ [58]

$d : \mathsf{RNo} = s(\mathsf{SNo})$ [59]

$d : \mathsf{RFile}(\mathsf{SNo}) = \mathsf{SFile}(\mathsf{SNo})$ [60]

$\mathsf{RBit}_d = \mathsf{flip}(\mathsf{SBit}_d)$ [58′]

$\mathsf{RNo}_d = s(\mathsf{SNo}_d)$ [59′]

$\mathsf{RFile}_d(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo})_d$ [60′]

$\square$:	$\mathsf{RFile}_d(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo})_d$ [60′]
	$\mathsf{SNo}_d = \mathsf{SNo}_a$ [46′]
	$\mathsf{SFile}_d(\mathsf{SNo}_a) = d_1$ [44′]
	$\mathsf{RFile}_d(\mathsf{SNo}_a) \neq d_1$ [53′]

$$\vdots$$

von [32] (S. 318):

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \quad [32]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\}, \infty]$$
$$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [11']$$
$$a: \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)) \quad [15]$$

mit Theorem 2:

$$a: \ \forall D : \nabla SNo, SBit : \mathsf{SFile}(SNo) = D \to \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D \wedge \mathsf{RBit} = \mathsf{flip}(SBit)) \quad [62]$$
$$a: \ \nabla SNo, SBit : \mathsf{SFile}(SNo) = D_6 \to \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = D_6 \wedge \mathsf{RBit} = \mathsf{flip}(SBit)) \quad [63]$$
$$a: \ \mathsf{SFile}(SNo_a) = D_6 \to \mathsf{A}\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = D_6 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [64]$$

$$a: \ \neg(\mathsf{SFile}(\mathsf{SNo}_a) = D_6) \quad [65]$$
$$\mathsf{SFile}_a(\mathsf{SNo}_a) \neq D_6 \quad [65']$$
$$\Box \ \{D_6 \leftarrow d_1\}, (11', 65')$$

$$a: \ \mathsf{A}\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [66]$$

$$a: \ \mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a) \quad [67]$$

wie [70] mit a anstelle e und
$\mathsf{SFile}_a(\mathsf{SNo}_a) = d_1 \quad [11']$
[68],[69] nicht verwenden

$$a: \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [68]$$
$$a: \ (\mathsf{A})\Diamond(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)) \quad [69]$$

auf q:

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \quad [70]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\},$$
$$e, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)),$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\}, \infty]$$

$$e: \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)) \quad [71]$$
$$e: \ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [72]$$
$$e: \ \mathsf{SBit} = \mathsf{SBit}_a \quad [73]$$
$$e: \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [74]$$
$$e: \ \mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a) \quad [75]$$

$$e: \ \mathsf{RFile}(\mathsf{SNo}_a) = d_1 \quad [76]$$
$$e: \ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a) \quad [77]$$

$\hookrightarrow$ S. 322

$$\vdots$$

von [77] (S. 321):

$$q : [\,a, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \quad [70]$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\},$$
$$e, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)),$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\}, \infty]$$

$$|$$

$$\mathsf{SFile}_e(\mathsf{SNo}_a) = d_1 \quad [72']$$
$$\mathsf{SBit}_e = \mathsf{SBit}_a \quad [73']$$
$$\mathsf{RFile}_e(\mathsf{SNo}_a) = d_1 \quad [76']$$
$$\mathsf{RBit}_e = \mathsf{flip}(\mathsf{SBit}_a) \quad [77']$$

$$|$$

aus RBit:

$$e : \ \nabla RBit : \mathsf{A}(\mathsf{RBit} = RBit \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \quad [78]$$
$$e : \ \mathsf{A}(\mathsf{RBit} = \mathsf{RBit}_e \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true}) \quad [79]$$
$$e : \ (\mathsf{A})(\mathsf{RBit} = \mathsf{RBit}_e \ \mathsf{unless} \ \mathsf{AccDat} = \mathsf{true}) \quad [80]$$

auf q:

$$q : [\,a, \{\ldots\}, \quad [81]$$
$$e, \{\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{RBit}_e\},$$
$$f, \{\ldots\}, \infty]$$

$$|$$

$$f : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [82]$$
$$\mathsf{SBit}_f = \mathsf{SBit}_a \quad [82']$$
$$f : \ \mathsf{AccDat} = \mathsf{true} \quad [83]$$

$$q : [\,a, \{\ldots\}, \quad [84]$$
$$e, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)),$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true}),$$
$$\mathsf{RBit} = \mathsf{RBit}_e, \neg(\mathsf{AccDat} = \mathsf{true})\}, \infty]$$

$\hookrightarrow$ S. 324

Vorgängerzustand von f betrachten:

$$q : [\,a, \{\ldots\}, e, \circ, f, \{\ldots\}, \infty] \quad [85]$$

$$\boxed{\begin{array}{l} \text{wie [86] mit } e \text{ anstelle } g \text{ und} \\ \mathsf{SBit}_e = \mathsf{SBit}_a \quad [73'] \\ \mathsf{RBit}_e = \mathsf{flip}(\mathsf{SBit}_a) \quad [77'] \end{array}}$$

$$q : [\,a, \{\ldots\}, e, \{\mathsf{SBit} = \mathsf{SBit}_a, \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a)\}, \quad [86]$$
$$g, \circ, f, \{\ldots\}, \infty]$$

$$|$$

$$g : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [87]$$
$$g : \ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}_a) \quad [88]$$
$$\mathsf{SBit}_g = \mathsf{SBit}_a \quad [87']$$
$$\mathsf{RBit}_g = \mathsf{flip}(\mathsf{SBit}_a) \quad [88']$$

$\hookrightarrow$ S. 323

$$\vdots$$

von [88] (S. 322):

$$q : [\,a, \{\ldots\}, e, \{\ldots\}, g, \circ, f, \{\ldots\}, \infty] \quad [86]$$

$$f:\ \mathsf{AccDat} = \mathsf{true} \quad [83]$$

$$\mathsf{SBit}_g = \mathsf{SBit}_a \quad [87']$$

$$\mathsf{RBit}_g = \mathsf{flip}(\mathsf{SBit}_a) \quad [88']$$

aus AD1:

$$g:\ (\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \to \exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit}) \quad [89]$$

$$g:\ \neg(\mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})) \quad [90]$$

$$g:\ (\mathsf{A})\circ\neg(\mathsf{AccDat} = \mathsf{true}) \quad [92]$$

auf q:

$$f:\ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [93]$$

$$\Box\ (83, 93)$$

$$g:\ \exists D : \mathsf{RIM} = \mathsf{msg}(D, \mathsf{RBit}) \quad [91]$$

$$g:\ \mathsf{RIM} = \mathsf{msg}(d_7, \mathsf{RBit}) \quad [94]$$

$$\mathsf{RIM}_g = \mathsf{msg}(d_7, \mathsf{RBit}_g) \quad [94']$$

mit Lemma 3:

$$g:\ \forall B : ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B)) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B)|Q')) \to \quad [95]$$
$$(\mathsf{SBit} = \mathsf{flip}(B) \to \mathsf{RBit} = \mathsf{flip}(B))$$

$$g:\ ((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_8)) \vee (\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_8)|Q')) \to \quad [96]$$
$$(\mathsf{SBit} = \mathsf{flip}(B_8) \to \mathsf{RBit} = \mathsf{flip}(B_8))$$

$$g:\ \neg((\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_8)) \vee \quad [97]$$
$$(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_8)|Q'))$$

$$g:\ \neg(\exists D : \mathsf{RIM} = \mathsf{msg}(D, B_8)) \quad [99]$$

$$g:\ \neg(\exists Q, Q', D' : \mathsf{RQ} = Q|\mathsf{msg}(D', B_8)|Q') \quad [100]$$

$$g:\ \neg(\mathsf{RIM} = \mathsf{msg}(D_8, B_8)) \quad [101]$$

$$\mathsf{RIM} \neq \mathsf{msg}(D_8, B_8) \quad [101']$$

$$\Box\ \{D_8 \leftarrow d_7,\ B_8 \leftarrow \mathsf{RBit}_g\}(94', 101')$$

$$g:\ \mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}_g) \to \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_g) \quad [98]$$

$$g:\ \neg(\mathsf{SBit} = \mathsf{flip}(\mathsf{RBit}_g)) \quad [102]$$

$$\mathsf{SBit}_g \neq \mathsf{flip}(\mathsf{RBit}_g) \quad [102']$$

$$\boxed{\begin{array}{ll} \Box: & \mathsf{SBit}_g = \mathsf{SBit}_a \quad [87'] \\ & \mathsf{RBit}_g = \mathsf{flip}(\mathsf{SBit}_a) \quad [88'] \end{array}}$$

$$g:\ \mathsf{RBit} = \mathsf{flip}(\mathsf{RBit}_g) \quad [103]$$

$$\mathsf{RBit}_g = \mathsf{flip}(\mathsf{RBit}_g) \quad [103']$$

$$\Box$$

$\vdots$

von [84] (S. 322):

$$q : [\,a, \{\ldots\}, e, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \quad [84]$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RBit} = \mathsf{RBit}_e, \neg(\mathsf{AccDat} = \mathsf{true})\}, \infty]$$

$$\mathsf{SBit}_e = \mathsf{SBit}_a \quad [73']$$
$$\mathsf{RFile}_e(\mathsf{SNo}_a) = d_1 \quad [76']$$
$$\mathsf{RBit}_e = \mathsf{flip}(\mathsf{SBit}_a) \quad [77']$$

aus RData:

$$e : \ \forall D, N : \mathsf{RFile}(N) = D \to \mathsf{A}(\mathsf{RFile}(N) = D \ \mathsf{unless}^+ \ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(N))) \quad [104]$$
$$e : \ \mathsf{RFile}(N_9) = D_9 \to \mathsf{A}(\mathsf{RFile}(N_9) = D_9 \ \mathsf{unless}^+ \ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(N_9))) \quad [105]$$

$$e : \ \neg(\mathsf{RFile}(N_9) = D_9) \quad [106]$$
$$\mathsf{RFile}_e(N_9) \neq D_9 \quad [106']$$
$$\Box \ \{N_9 \leftarrow \mathsf{SNo}_a, \ D_9 \leftarrow d_1\}(76', 106')$$

$$e : \ \mathsf{A}(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \ \mathsf{unless}^+ \quad [107]$$
$$(\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(\mathsf{SNo}_a)))$$

$$e : \ (\mathsf{A})(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \ \mathsf{unless} \ (\mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(\mathsf{SNo}_a))) \quad [108]$$

$$q : [\,a, \{\ldots\}, \quad [109]$$
$$e, \{\neg(\mathsf{AccDat} = \mathsf{true}), \mathsf{RFile}(\mathsf{SNo}_a) = d_1\},$$
$$h, \{\neg(\mathsf{AccDat} = \mathsf{true})\}, \infty]$$
$$h : \ \neg(\mathsf{AccDat} = \mathsf{true}) \quad [110]$$
$$h : \ \mathsf{AccDat} = \mathsf{true} \wedge \mathsf{RNo} = s(\mathsf{SNo}_a) \quad [111]$$
$$h : \ \mathsf{AccDat} = \mathsf{true} \quad [113]$$
$$h : \ \mathsf{RNo} = s(\mathsf{SNo}_a) \quad [114]$$
$$\Box \ (110, 113)$$

$$q : [\,a, \{\ldots\}, \quad [112]$$
$$e, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)),$$
$$\mathsf{SFile}(\mathsf{SNo}_a) = d_1, \mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true}),$$
$$\mathsf{RBit} = \mathsf{RBit}_e, \neg(\mathsf{AccDat} = \mathsf{true}), \mathsf{RFile}(\mathsf{SNo}_a) = d_1\}, \infty]$$

Lemma 8:

$$e : \ \nabla SBit : \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \to \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, SBit)) \quad [115]$$
$$e : \ \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \to \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_e)) \quad [116]$$

$$e : \ \neg(\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})) \quad [117]$$
$$\mathsf{RBit}_e \neq \mathsf{flip}(\mathsf{SBit}_e) \quad [117']$$
$$\boxed{\begin{array}{l} \Box : \ \mathsf{RBit}_e = \mathsf{flip}(\mathsf{SBit}_a) \quad [77'] \\ \quad\ \ \mathsf{SBit}_e = \mathsf{SBit}_a \quad [73'] \end{array}}$$

$$e : \ \mathsf{A}\Diamond^+(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_e)) \quad [118]$$
$$e : \ (\mathsf{A})\Diamond(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_e)) \quad [119]$$

$\hookrightarrow$ S. 325

$$\vdots$$

von [119] (S. 324):

$$q : [\,a, \{\ldots\}, e, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \quad [112]$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RFile}(\mathsf{SNo}_a) = d_1\}, \infty]$$

$$|$$

$$\mathsf{SBit}_e = \mathsf{SBit}_a \quad [73']$$
$$e : \ (\mathsf{A})\Diamond(\mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_e)) \quad [119]$$

auf q:

$$q : [\,a, \{\ldots\}, e, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1, \quad [120]$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RFile}(\mathsf{SNo}_a) = d_1\},$$
$$i, \{\neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)), \mathsf{SFile}(\mathsf{SNo}_a) = d_1,$$
$$\mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{ProcAck} = \mathsf{true}), \mathsf{RFile}(\mathsf{SNo}_a) = d_1\}, \infty]$$

$$|$$

$$i : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1 \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)) \quad [121]$$
$$i : \ \mathsf{SFile}(\mathsf{SNo}_a) = d_1 \quad [122]$$
$$i : \ \mathsf{SBit} = \mathsf{SBit}_a \quad [123]$$
$$i : \ \neg(\mathsf{ProcAck} = \mathsf{true}) \quad [124]$$
$$i : \ \mathsf{RFile}(\mathsf{SNo}_a) = d_1 \quad [125]$$
$$\mathsf{SFile}_i(\mathsf{SNo}_a) = d_1 \quad [122']$$
$$\mathsf{SBit}_i = \mathsf{SBit}_a \quad [123']$$
$$\mathsf{RFile}_i(\mathsf{SNo}_a) = d_1 \quad [125']$$
$$i : \ \mathsf{ProcAck} = \mathsf{true} \vee \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_e) \quad [126]$$

Left branch:

$$i : \ \mathsf{ProcAck} = \mathsf{true} \quad [127]$$
$$\Box \ (124, 127)$$

Right branch:

$$i : \ \mathsf{SIM} = \mathsf{msg}(\lambda, \mathsf{SBit}_e) \quad [128]$$
$$\mathsf{SIM}_i = \mathsf{msg}(\lambda, \mathsf{SBit}_e) \quad [128']$$

aus [121]:

Left branch:

$$i : \ \neg(\mathsf{RFile}(\mathsf{SNo}_a) = d_1) \quad [129]$$
$$\mathsf{RFile}_i(\mathsf{SNo}_a) \neq d_1 \quad [129']$$
$$\Box \ (129, 125)$$

Right branch:

$$i : \ \neg(\exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_a)) \quad [130]$$
$$i : \ \neg(\mathsf{SIM} = \mathsf{msg}(D'_{10}, \mathsf{SBit}_a)) \quad [131]$$
$$\mathsf{SIM}_i \neq \mathsf{msg}(D'_{10}, \mathsf{SBit}_a) \quad [131']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{SIM}_i = \mathsf{msg}(\lambda, \mathsf{SBit}_e) \quad [128'] \\ & \mathsf{SBit}_e = \mathsf{SBit}_a \quad [73'] \\ & \{D'_{10} \leftarrow \lambda\} \end{array}}$$

21 Theorem 4: Fortschritt zum nächsten Datum

Im Startzustand 0 (dort sei $\mathsf{SNo} = 0$) gilt

$$\forall N : (\mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(N) = \mathsf{SFile}(N) \wedge (\mathsf{SNo} = s(N) \vee (\mathsf{SNo} = N \wedge \mathsf{ready}))))$$

Insbesondere folgt daraus

$$\mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(N) = \mathsf{SFile}(N))$$

Beweisskizze:

Diesmal beweist man die Aussage mit Induktion über N. Wieder wird die Aussage für festes N als $A(N)$ bezeichnet.

Die Negation der Aussage bedeutet, daß es ein n_0 gibt, für das es einen Pfad p gibt, auf dem das Element $\mathsf{SFile}(n_0) \neq \bot$ nie abgespeichert wird oder SNo weder $= s(n_0)$ wird, noch bei $\mathsf{SNo} = n_0$ ready wahr wird [13].

SFile bleibt in allen Folgezuständen unverändert. Nach Induktionsvoraussetzung existiert ein Zustand a auf p, in dem $\mathsf{SFile}(p(n_0))$ abgespeichert wird, und $\mathsf{SNo} = s(p(n_0)) = n_0$ wird, oder bei $\mathsf{SNo} = p(n_0)$ ready wahr ist [32]. Letzteres ist nicht möglich, da $\mathsf{SFile}(s(p(n_0))) \neq \bot$ ist. Es ist also $\mathsf{SNo}_a = s(p(n_0)) = n_0$ [35].

SBit und SNo bleiben unverändert, bis $\mathsf{ProcAck}$ ausgeführt wird. Ist dies in einem Folgezustand b der Fall [46], so ist in dessen Vorgängerzustand c $\mathsf{Bit}(\mathsf{SIM}_c) = \mathsf{SBit}_c$. Mit Korollar 3 erhält man, daß dann $\mathsf{RFile}_c(\mathsf{SNo}_c) = \mathsf{SFile}_c(\mathsf{SNo}_c) = \mathsf{SFile}_0(\mathsf{SNo}_a)$ schon abgespeichert ist und nach Korollar 4 persistent bleibt, also $\mathsf{RFile}_b(\mathsf{SNo}_c) = \mathsf{SFile}_0(n_0)$ ist. Nach Annahme ist also weder $\mathsf{SNo}_c = s(n_0)$ noch $\mathsf{SNo}_c = n_0 \wedge \mathsf{ready}$ [77],[78]. Da in dem Schritt von c nach b $\mathsf{ProcAck}$ angewendet worden ist, folgt jedoch, daß, ja nachdem, ob $\mathsf{SFile}(s(n_0)) = \mathit{bot}$ ist, genau einer dieser beiden Fälle eintritt.

Die Annahme, daß $\mathsf{ProcAck}$ nie ausgeführt wird, ist unfair: Dazu müßte ein Zustand d existieren, ab dem $\mathsf{ProcAck}$ nie mehr ausführbar ist [103]. Theorem 3 garantiert, daß SIM irgendwann in einem weiteren Folgezustand e eine Quittung für das Element $\mathsf{SFile}_d(\mathsf{SNo}_d)$ enthalten muß [114], also $\mathsf{Bit}(\mathsf{SIM}_e) = \mathsf{SBit}_e$ ist, womit $\mathsf{ProcAck}$ ausführbar wäre.

$$0:\ \mathsf{SNo} = 0 \quad [1]$$
$$0:\ \neg(\forall N : A(N)) \quad [2]$$

$$0:\ \neg(A(0)) \quad [3]$$

$\boxed{\text{analog zum Ind.Schritt.}}$

$$0:\ A(p(n_0)) \quad [4]$$
$$0:\ \neg(A(n_0) \quad [5]$$

$$0:\ \neg(\mathsf{SFile}(n_0) \neq \bot \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready})))) \quad [6]$$
$$0:\ \mathsf{SFile}(n_0) \neq \bot \quad [7]$$
$$\mathsf{SFile}_0(n_0) \neq \bot \quad [7']$$
$$0:\ \neg(\mathsf{A}\Diamond(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready})))) \quad [8]$$
$$p : [\,0, \emptyset, \infty] \quad [9]$$
$$0:\ p\,\neg(\Diamond(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready})))) \quad [10]$$
$$0:\ \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))) \quad [11]$$
$$0:\ (p)\,\neg(\Diamond(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready})))) \quad [12]$$
$$p : [\,0, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready})))\}, \infty] \quad [13]$$

aus SData:

$$0:\ \forall N : \nabla SFile : \mathsf{A}\Box(\mathsf{SFile}(N) = SFile(N)) \quad [14]$$
$$0:\ \nabla SFile : \mathsf{A}\Box(\mathsf{SFile}(N_1) = SFile(N_1)) \quad [15]$$
$$0:\ \mathsf{A}\Box(\mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)) \quad [16]$$
$$0:\ \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1) \quad [17]$$
$$0:\ (\mathsf{A})\Box(\mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)) \quad [18]$$

auf p:

$$p : [\,0, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))), \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)\}, \infty] \quad [19]$$

Ind.Vor. für $p(n_0)$ [4]:

$$0:\ (\mathsf{SFile}(p(n_0)) \neq \bot) \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(p(n_0)) = \mathsf{SFile}(p(n_0)) \wedge (\mathsf{SNo} = s(p(n_0)) \vee (\mathsf{SNo} = p(n_0) \wedge \mathsf{ready}))) \quad [20]$$

$$0:\ \neg(\mathsf{SFile}(p(n_0)) \neq \bot) \quad [21]$$
$$\mathsf{SFile}_0(p(n_0)) = \bot \quad [21']$$

mit F4S:

$$0:\ \forall N : \mathsf{SFile}(N) = \bot \rightarrow \mathsf{SFile}(s(N)) = \bot \quad [23]$$
$$0:\ \mathsf{SFile}(N_2) = \bot \rightarrow \mathsf{SFile}(s(N_2)) = \bot \quad [24]$$

$$0:\ \neg(\mathsf{SFile}(N_2) = \bot) \quad [25]$$
$$\mathsf{SFile}_0(N_2) \neq \bot \quad [25']$$
$$\Box\ \{N_2 \leftarrow p(n_0)\}(21', 25')$$

$$0:\ \mathsf{SFile}(s(p(n_0))) = \bot \quad [26]$$
$$\mathsf{SFile}_0(s(p(n_0))) = \bot \quad [26']$$
$$\Box\ (7', 26')$$

$$0:\ \mathsf{A}\Diamond(\mathsf{RFile}(p(n_0)) = \mathsf{SFile}(p(n_0)) \wedge (\mathsf{SNo} = s(p(n_0)) \vee (\mathsf{SNo} = p(n_0) \wedge \mathsf{ready}))) \quad [22]$$

$\hookrightarrow$ S. 328

$\vdots$

von [22] (S. 327):

$$p : [\,0, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))), \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)\}, \infty] \quad [19]$$

$$\mathsf{SFile}_0(n_0) \neq \bot \quad [7']$$

$$0 : \ \mathsf{A}\Diamond(\mathsf{RFile}(p(n_0)) = \mathsf{SFile}(p(n_0)) \wedge (\mathsf{SNo} = s(p(n_0)) \vee (\mathsf{SNo} = p(n_0) \wedge \mathsf{ready}))) \quad [22]$$

aus [22]:

$$0 : \ \mathsf{RFile}(p(n_0)) = \mathsf{SFile}(p(n_0)) \wedge (\mathsf{SNo} = s(p(n_0)) \vee (\mathsf{SNo} = p(n_0) \wedge \mathsf{ready})) \quad [27]$$

wie [35] mit 0 anstelle a und
$0 : \ \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready})))$ [11]

$$0 : \ (\mathsf{A})\Diamond(\mathsf{RFile}(p(n_0)) = \mathsf{SFile}(p(n_0)) \wedge (\mathsf{SNo} = s(p(n_0)) \vee (\mathsf{SNo} = p(n_0) \wedge \mathsf{ready}))) \quad [28]$$

auf p:

$$p : [\,0, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))), \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)\}, \quad [29]$$
$$a, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))), \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)\}, \infty]$$

$$a : \ \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))) \quad [30]$$

$$a : \ \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1) \quad [31]$$

$$\mathsf{SFile}_a(N_1) = \mathsf{SFile}_0(N_1) \quad [31']$$

$$a : \ \mathsf{RFile}(p(n_0)) = \mathsf{SFile}(p(n_0)) \wedge (\mathsf{SNo} = s(p(n_0)) \vee (\mathsf{SNo} = p(n_0) \wedge \mathsf{ready})) \quad [32]$$

$$a : \ \mathsf{RFile}(p(n_0)) = \mathsf{SFile}(p(n_0)) \quad [33]$$

$$\mathsf{RFile}_a(p(n_0)) = \mathsf{SFile}_a(p(n_0)) \quad [33']$$

$$a : \ \mathsf{SNo} = s(p(n_0)) \vee (\mathsf{SNo} = p(n_0) \wedge \mathsf{ready}) \quad [34]$$

$$a : \ \mathsf{SNo} = s(p(n_0)) \quad [35]$$

$$\mathsf{SNo}_a = s(p(n_0)) \quad [35']$$

aus SBit:

$$a : \ \nabla SBit : \mathsf{A}(\mathsf{SBit} = SBit \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [37]$$

$$a : \ \mathsf{A}(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true}) \quad [38]$$

$$a : \ (\mathsf{A})(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless} \ \mathsf{ProcAck} = \mathsf{true}) \quad [39]$$

$\hookrightarrow$ S. 329

$$a : \ \mathsf{SNo} = p(n_0) \wedge \mathsf{ready} \quad [36]$$

$$a : \ \mathsf{SNo} = p(n_0) \quad [125]$$

$$\mathsf{SNo}_a = p(n_0) \quad [125']$$

$$a : \ \mathsf{ready} = \mathsf{true} \quad [126]$$

aus Korollar 2:

$$a : \ \mathsf{ready} = \mathsf{true} \rightarrow (\mathsf{SFile}(s(\mathsf{SNo})) = \bot \wedge \ldots) \quad [127]$$

$$a : \ \neg(\mathsf{ready} = \mathsf{true}) \quad [128]$$

$$\Box \ (126, 128)$$

$$a : \ \mathsf{SFile}(s(\mathsf{SNo})) = \bot \quad [129]$$

$$a : \ \ldots \quad [130]$$

$$\mathsf{SFile}_a(s(\mathsf{SNo}_a)) = \bot \quad [129']$$

$\Box : \ \mathsf{SNo}_a = p(n_0)$ [125']
$\mathsf{SFile}_0(n_0) \neq \bot$ [7']
$\mathsf{SFile}_a(N_1) = \mathsf{SFile}_0(N_1)$ [31']
aus [69] : $\{N_1 \leftarrow n_0\}$

$$\vdots$$

von [39] (S. 328):

$$p: [\,0, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))), \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)\}, \quad [29]$$
$$a, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))), \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)\}, \infty]$$

$$|$$

$$\mathsf{SFile}_0(n_0) \neq \bot \quad [7']$$
$$a: \ \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))) \quad [30]$$
$$\mathsf{SFile}_a(N_1) = \mathsf{SFile}_0(N_1) \quad [31']$$
$$\mathsf{SNo}_a = s(p(n_0)) \quad [35']$$
$$a: \ (\mathsf{A})(\mathsf{SBit} = \mathsf{SBit}_a \ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true}) \quad [39]$$

$$|$$

aus SNo:

$$a: \ \nabla SNo: \mathsf{A}(\mathsf{SNo} = SNo\ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true}) \quad [40]$$
$$a: \ \mathsf{A}(\mathsf{SNo} = \mathsf{SNo}_a\ \mathsf{unless}^{+}\ \mathsf{ProcAck} = \mathsf{true}) \quad [41]$$
$$a: \ (\mathsf{A})(\mathsf{SNo} = \mathsf{SNo}_a\ \mathsf{unless}\ \mathsf{ProcAck} = \mathsf{true}) \quad [42]$$

[39] und [42] auflösen:

$$\begin{array}{l} p: [\,0, \{\ldots\}, \qquad\qquad [43] \\ \quad a, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge \\ \qquad (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))), \\ \quad\ \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1), \mathsf{SBit} = \mathsf{SBit}_a, \\ \quad\ \mathsf{SNo} = \mathsf{SNo}_a\}, \\ \quad b, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge \\ \qquad (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))), \\ \quad\ \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)\}, \infty] \end{array}$$

$$\begin{array}{l} p: [\,0, \{\ldots\}, \qquad\qquad [47] \\ \quad a, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge \\ \qquad \mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))), \\ \quad\ \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1), \mathsf{SBit} = \mathsf{SBit}_a, \\ \quad\ \mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\}, \infty] \end{array}$$

$\hookrightarrow$ S. 333

$$b: \ \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))) \quad [44]$$
$$b: \ \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1) \quad [45]$$
$$b: \ \mathsf{ProcAck} = \mathsf{true} \quad [46]$$
$$\mathsf{SFile}_b(N_1) = \mathsf{SFile}_0(N_1) \quad [45']$$

Vorgängerzustand von b betrachten:

$$p: [\,0, \{\ldots\}, a, \circ, b, \{\ldots\}, \infty] \quad [48]$$

$\hookrightarrow$ S. 330

$$\boxed{\begin{array}{l} \text{wie [49] mit } a \text{ anstelle } c \text{ und} \\ a: \ \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge \qquad [30] \\ \qquad (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))) \\ \mathsf{SFile}_a(N_1) = \mathsf{SFile}_0(N_1) \quad [31'] \end{array}}$$

$\vdots$

von [46] (S. 329): (rechter Zweig)

$p : [0, \{\ldots\},$ [49]

$a, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))),$

$\mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1), \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a\},$

$c, \circ,$

$b, \{\neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready}))),$

$\mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)\}, \infty]$

|

$\mathsf{SFile}_0(n_0) \neq \perp$ [7′]

$\mathsf{SNo}_a = s(p(n_0))$ [35′]

$b: \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready})))$ [44]

$\mathsf{SFile}_b(N_1) = \mathsf{SFile}_0(N_1)$ [45′]

$b: \mathsf{ProcAck} = \mathsf{true}$ [46]

|

$c: \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready})))$ [50]

$c: \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)$ [51]

$c: \mathsf{SBit} = \mathsf{SBit}_a$ [52]

$c: \mathsf{SNo} = \mathsf{SNo}_a$ [53]

$\mathsf{SFile}_c(N_1) = \mathsf{SFile}_0(N_1)$ [51′]

$\mathsf{SBit}_c = \mathsf{SBit}_a$ [52′]

$\mathsf{SNo}_c = \mathsf{SNo}_a$ [53′]

|

aus PA1:

$c: \mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}) \to \exists D : \mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit})$ [54]

Linker Zweig:

$c: \neg\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true})$ [55]

$c: (\mathsf{A})\neg\circ(\mathsf{ProcAck} = \mathsf{true})$ [57]

auf p:

$b: \neg(\mathsf{ProcAck} = \mathsf{true})$ [58]

$\Box$ (46, 58)

Rechter Zweig:

$c: \exists D : \mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit})$ [56]

$c: \mathsf{SIM} = \mathsf{msg}(d_3, \mathsf{SBit})$ [59]

$\mathsf{SIM}_c = \mathsf{msg}(d_3, \mathsf{SBit}_c)$ [59′]

|

mit Korollar 3:

$c: \forall D : (\mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit}) \to (\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \mathsf{RNo} = s(\mathsf{SNo}) \wedge \mathsf{RFile}(\mathsf{SNo}) = \mathsf{SFile}(\mathsf{SNo})))$ [60]

$c: \mathsf{SIM} = \mathsf{msg}(D_4, \mathsf{SBit}) \to (\mathsf{RBit} = \mathsf{flip}(\mathsf{SBit}) \wedge \mathsf{RNo} = s(\mathsf{SNo}) \wedge \mathsf{RFile}(\mathsf{SNo}) = \mathsf{SFile}(\mathsf{SNo}))$ [61]

Linker Zweig:

$c: \neg(\mathsf{SIM} = \mathsf{msg}(D_4, \mathsf{SBit}))$ [62]

$\mathsf{SIM}_c \neq \mathsf{msg}(D_4, \mathsf{SBit}_c)$ [62′]

$\Box\ \{D_4 \leftarrow d_3\}(59', 62)$

Rechter Zweig:

$c: \mathsf{RBit} = \mathsf{flip}(\mathsf{SBit})$ [63]

$c: \mathsf{RNo} = s(\mathsf{SNo})$ [64]

$c: \mathsf{RFile}(\mathsf{SNo}) = \mathsf{SFile}(\mathsf{SNo})$ [65]

$\mathsf{RBit}_c = \mathsf{flip}(\mathsf{SBit})$ [63′]

$\mathsf{RNo}_c = s(\mathsf{SNo})$ [64′]

$\mathsf{RFile}_c(\mathsf{SNo}_c) = \mathsf{SFile}_c(\mathsf{SNo}_c)$ [65′]

$\hookrightarrow$ S. 331

$\vdots$

von [65] (S. 330):

$p : [\,0, \{\ldots\}, a, \{\ldots\}, c, \circ, b, \{\ldots\}, \infty]$ [49]

$\mathsf{SFile}_0(n_0) \neq \bot$ [7′]

$\mathsf{SNo}_a = s(p(n_0))$ [35′]

$b :\ \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0) \wedge (\mathsf{SNo} = s(n_0) \vee (\mathsf{SNo} = n_0 \wedge \mathsf{ready})))$ [44]

$\mathsf{SFile}_b(N_1) = \mathsf{SFile}_0(N_1)$ [45′]

$b :\ \mathsf{ProcAck} = \mathsf{true}$ [46]

$\mathsf{SFile}_c(N_1) = \mathsf{SFile}_0(N_1)$ [51′]

$\mathsf{SNo}_c = \mathsf{SNo}_a$ [53′]

$\mathsf{RFile}_c(\mathsf{SNo}_c) = \mathsf{SFile}_c(\mathsf{SNo}_c)$ [65′]

mit Korollar 4:

$c :\ \forall N : \nabla RFile : \mathsf{RFile}(N) \neq \bot \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N) = RFile(N))$ [66]

$c :\ \nabla RFile : \mathsf{RFile}(N_5) \neq \bot \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N_5) = RFile(N_5))$ [67]

$c :\ \mathsf{RFile}(N_5) \neq \bot \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N_5) = \mathsf{RFile}_c(N_5))$ [68]

$c :\ \neg(\mathsf{RFile}(N_5) \neq \bot)$ [69]

$\mathsf{RFile}_c(N_5) = \bot$ [69′]

$\Box :$ $\mathsf{RFile}_c(N_5) = \bot$ [69′]
$\mathsf{RFile}_c(\mathsf{SNo}_c) = \mathsf{SFile}_c(\mathsf{SNo}_c)$ [65′]
$\mathsf{SFile}_c(N_1) = \mathsf{SFile}_0(N_1)$ [51′]
$\mathsf{SFile}_0(n_0) \neq \bot$ [7′]
$\mathsf{SNo}_a = s(p(n_0))$ [35′]
$\mathsf{SNo}_c = \mathsf{SNo}_a$ [53′]
$\{N_1 \leftarrow n_0,\ N_5 \leftarrow n_0\}$

$c :\ \mathsf{A}\Box(\mathsf{RFile}(n_0) = \mathsf{SFile}_c(n_0))$ [70]

$c :\ \mathsf{RFile}(n_0) = \mathsf{SFile}_0(n_0)$ [71]

$c :\ (\mathsf{A})\Box(\mathsf{RFile}(n_0) = \mathsf{SFile}_0(n_0))$ [72]

auf p:

$b :\ \mathsf{A}\Box(\mathsf{RFile}(n_0) = \mathsf{SFile}_0(n_0))$ [73]

$b :\ \mathsf{RFile}(n_0) = \mathsf{SFile}_0(n_0)$ [74]

$b :\ (\mathsf{A})\Box(\mathsf{RFile}(n_0) = \mathsf{SFile}_0(n_0))$ [75]

$\mathsf{RFile}_b(n_0) = \mathsf{SFile}_0(n_0)$ [74′]

aus [44]:

$b :\ \neg(\mathsf{RFile}(n_0) = \mathsf{SFile}(n_0))$ [76]

$\mathsf{RFile}_b(n_0) \neq \mathsf{SFile}_b(n_0)$ [76′]

$\Box :$ $\mathsf{RFile}_b(n_0) = \mathsf{SFile}_0(n_0)$ [74′]
$\mathsf{SFile}_b(N_1) = \mathsf{SFile}_0(N_1)$ [45′]
aus [69] : $\{N_1 \leftarrow n_0\}$
$\mathsf{RFile}_b(n_0) \neq \mathsf{SFile}_b(n_0)$ [76′]

$b :\ \neg(\mathsf{SNo} = s(n_0))$ [77]

$\mathsf{SNo}_b \neq s(n_0)$ [77′]

$b :\ \neg(\mathsf{SNo} = n_0 \wedge \mathsf{ready} = \mathsf{true})$ [78]

$\hookrightarrow$ S. 332

$\vdots$

von [78] (S. 331):

$p : [\,0, \{\ldots\}, a, \{\ldots\}, c, \circ, b, \{\ldots\}, \infty]$ [49]

$\mathsf{SNo}_a = s(p(n_0))$ [35′]

$b:$ $\mathsf{ProcAck} = \mathsf{true}$ [46]

$\mathsf{SNo}_c = \mathsf{SNo}_a$ [53′]

$\mathsf{SNo}_b \neq s(n_0)$ [77′]

$b:$ $\neg(\mathsf{SNo} = n_0 \wedge \mathsf{ready} = \mathsf{true})$ [78]

mit PA2:

$$c:\ \nabla SBit, RQ, SNo : \mathsf{A}\circ(\mathsf{ProcAck} = \mathsf{true} \rightarrow \quad [79]$$
$$(\mathsf{SFile}(s(SNo)) \neq \bot \rightarrow \ \mathsf{RQ} = RQ|\mathsf{msg}(\mathsf{SFile}(s(SNo)), \mathsf{flip}(SBit))$$
$$\wedge\ \mathsf{SNo} = s(SNo) \wedge \mathsf{SBit} = \mathsf{flip}(SBit) \wedge \mathsf{ready} = \mathsf{false}) \wedge$$
$$(\mathsf{SFile}(s(SNo)) = \bot \rightarrow \ \mathsf{RQ} = RQ \wedge \mathsf{SNo} = SNo \wedge \mathsf{SBit} = SBit \wedge \mathsf{ready} = \mathsf{true}))$$

$$c:\ \mathsf{A}\circ(\mathsf{ProcAck} = \mathsf{true} \rightarrow \quad [80]$$
$$(\mathsf{SFile}(s(\mathsf{SNo}_c)) \neq \bot \rightarrow \ \mathsf{RQ} = \mathsf{RQ}_c|\mathsf{msg}(\mathsf{SFile}(s(\mathsf{SNo}_c)), \mathsf{flip}(\mathsf{SBit}_c))$$
$$\wedge\ \mathsf{SNo} = s(\mathsf{SNo}_c) \wedge \mathsf{SBit} = \mathsf{flip}(\mathsf{SBit}_c) \wedge \mathsf{ready} = \mathsf{false}) \wedge$$
$$(\mathsf{SFile}(s(\mathsf{SNo}_c)) = \bot \rightarrow \ \mathsf{RQ} = \mathsf{RQ}_c \wedge \mathsf{SNo} = \mathsf{SNo}_c \wedge \mathsf{SBit} = \mathsf{SBit}_c \wedge \mathsf{ready} = \mathsf{true}))$$

$$b:\ \mathsf{ProcAck} = \mathsf{true} \rightarrow \quad [81]$$
$$(\mathsf{SFile}(s(\mathsf{SNo}_c)) \neq \bot \rightarrow \ \mathsf{RQ} = \mathsf{RQ}_c|\mathsf{msg}(\mathsf{SFile}(s(\mathsf{SNo}_c)), \mathsf{flip}(\mathsf{SBit}_c))$$
$$\wedge\ \mathsf{SNo} = s(\mathsf{SNo}_c) \wedge \mathsf{SBit} = \mathsf{flip}(\mathsf{SBit}_c) \wedge \mathsf{ready} = \mathsf{false}) \wedge$$
$$(\mathsf{SFile}(s(\mathsf{SNo}_c)) = \bot \rightarrow \ \mathsf{RQ} = \mathsf{RQ}_c \wedge \mathsf{SNo} = \mathsf{SNo}_c \wedge \mathsf{SBit} = \mathsf{SBit}_c \wedge \mathsf{ready} = \mathsf{true})$$

$b:$ $\neg(\mathsf{ProcAck} = \mathsf{true})$ [82]

$\square$ (46, 82)

$$b:\ \mathsf{SFile}(s(\mathsf{SNo}_c)) \neq \bot \rightarrow \quad [83]$$
$$(\mathsf{RQ} = \mathsf{RQ}_c|\mathsf{msg}(\mathsf{SFile}(s(\mathsf{SNo}_c)), \mathsf{flip}(\mathsf{SBit}_c)) \wedge$$
$$\wedge\ \mathsf{SNo} = s(\mathsf{SNo}_c) \wedge \mathsf{SBit} = \mathsf{flip}(\mathsf{SBit}_c) \wedge \mathsf{ready} = \mathsf{false})$$

$$b:\ \mathsf{SFile}(s(\mathsf{SNo}_c)) = \bot \rightarrow \mathsf{RQ} = \mathsf{RQ}_c \wedge \mathsf{SNo} = \mathsf{SNo}_c \wedge \mathsf{SBit} = \mathsf{SBit}_c \wedge \mathsf{ready} = \mathsf{true} \quad [84]$$

aus [83]:

$b:$ $\neg(\mathsf{SFile}(s(\mathsf{SNo}_c)) \neq \bot)$ [85]

$\mathsf{SFile}_b(s(\mathsf{SNo}_c)) = \bot$ [85′]

aus [84]:

$b:$ $\mathsf{SFile}(s(\mathsf{SNo}_c)) = \bot)$ [90]

$\mathsf{SFile}_b(s(\mathsf{SNo}_c)) = \bot$ [90′]

$\square$ (85′, 90′)

$b:$ $\mathsf{RQ} = \mathsf{RQ}_c$ [91]

$b:$ $\mathsf{SNo} = \mathsf{SNo}_c$ [92]

$b:$ $\mathsf{SBit} = \mathsf{SBit}_c$ [93]

$b:$ $\mathsf{ready} = \mathsf{true}$ [94]

$\square$ (92, 94, 35′, 53′)

$b:$ $\mathsf{RQ} = \mathsf{RQ}_c|\mathsf{msg}(\mathsf{SFile}(s(\mathsf{SNo}_c)), \mathsf{flip}(\mathsf{SBit}_c))$ [86]

$b:$ $\mathsf{SNo} = s(\mathsf{SNo}_c)$ [87]

$b:$ $\mathsf{SBit} = \mathsf{flip}(\mathsf{SBit}_c)$ [88]

$b:$ $\mathsf{ready} = \mathsf{false}$ [89]

$\mathsf{SNo}_b = s(\mathsf{SNo}_c)$ [87′]

$\square:$ $\mathsf{SNo}_c = \mathsf{SNo}_a$ [53′]
$\mathsf{SNo}_a = s(p(n_0))$ [35′]
$\mathsf{SNo}_b \neq s(n_0)$ [77′]
$\mathsf{SNo}_b = s(\mathsf{SNo}_c)$ [87′]

$\vdots$

von [47] (S. 329):

$p : [\,0, \{\ldots\}, a, \{\mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1), \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\}, \infty]$ [47]

$\mathsf{SNo}_a = s(p(n_0))$ [35′]

Fairness bzgl. ProcAck:

$a :\ \mathsf{R}((\Box\Diamond\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true})) \to (\Diamond(\mathsf{ProcAck} = \mathsf{true})))$ [95]

auf p:

$a :\ (q)\Diamond(\neg(q\,\Diamond\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true})))$ [96]

$p : [\,0, \{\ldots\},$ [98]
$a, \{\mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1), \mathsf{SBit} = \mathsf{SBit}_a,$
$\mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\},$
$d, \{\mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1), \mathsf{SBit} = \mathsf{SBit}_a,$
$\mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true})\}, \infty]$

$d :\ \mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1)$ [99]

$d :\ \mathsf{SBit} = \mathsf{SBit}_a$ [100]

$d :\ \mathsf{SNo} = \mathsf{SNo}_a$ [101]

$d :\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [102]

$d :\ q\,\neg(\Diamond\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}))$ [103]

$\mathsf{SFile}_d(N_1) = \mathsf{SFile}_0(N_1)$ [99′]

$\mathsf{SBit}_d = \mathsf{SBit}_a$ [100′]

$\mathsf{SNo}_d = \mathsf{SNo}_a$ [101′]

$d :\ \neg(\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}))$ [104]

$d :\ (q)\Box\neg(\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}))$ [105]

$a :\ (q)\Diamond(\mathsf{ProcAck} = \mathsf{true})$ [97]

$p : [\,0, \{\ldots\},$ [122]
$a, \{\neg(\mathsf{ProcAck} = \mathsf{true})\},$
$f, \{\neg(\mathsf{ProcAck} = \mathsf{true})\}, \infty]$

$f :\ \neg(\mathsf{ProcAck} = \mathsf{true})$ [123]

$f :\ \mathsf{ProcAck} = \mathsf{true}$ [124]

$\Box(123, 124)$

$p : [\,0, \{\ldots\}, a, \{\ldots\},$ [106]
$d, \{\mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1), \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true}), \neg(\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}))\}, \infty]$

mit Theorem 3:

$d :\ \nabla SBit, SFile, SNo : \mathsf{A}\Diamond(\mathsf{RFile}(SNo) = SFile(SNo) \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', SBit))$ [107]

$d :\ \mathsf{A}\Diamond(\mathsf{RFile}(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo}_d) \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_d))$ [108]

$\hookrightarrow$ S. 334

$\vdots$

von [108] (S. 333):

$p: [0, \{\ldots\}, a, \{\ldots\},$ [106]

$d, \{\mathsf{SFile}(N_1) = \mathsf{SFile}_0(N_1), \mathsf{SBit} = \mathsf{SBit}_a, \mathsf{SNo} = \mathsf{SNo}_a, \neg(\mathsf{ProcAck} = \mathsf{true}), \neg(\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}))\}, \infty]$

$\mathsf{SBit}_d = \mathsf{SBit}_a$ [100′]

$d: \neg(\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}))$ [104]

$d: \mathsf{A}\Diamond(\mathsf{RFile}(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo}_d) \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_d))$ [108]

Linker Zweig:

$d: \mathsf{RFile}(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo}_d) \wedge$ [109]
$\exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_d)$

wie [110] mit d anstelle e und
$d: \neg(\circ(\mathsf{ProcAck} = \mathsf{true}))$ [104]
$\mathsf{SBit}_d = \mathsf{SBit}_a$ [100′]

Rechter Zweig:

$d: (\mathsf{A})\Diamond(\mathsf{RFile}(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo}_d) \wedge$ [110]
$\exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_d))$

auf p:

$p: [0, \{\ldots\}, a, \{\ldots\},$ [111]
$d, \{\mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}))\},$
$e, \{\mathsf{SBit} = \mathsf{SBit}_a, \neg(\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}))\}, \infty]$

$e: \mathsf{SBit} = \mathsf{SBit}_a$ [112]

$e: \neg(\mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true}))$ [113]

$e: \mathsf{RFile}(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo}_d) \wedge \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_d)$ [114]

$\mathsf{SBit}_e = \mathsf{SBit}_a$ [112′]

$e: \mathsf{RFile}(\mathsf{SNo}_d) = \mathsf{SFile}_d(\mathsf{SNo}_d)$ [115]

$e: \exists D' : \mathsf{SIM} = \mathsf{msg}(D', \mathsf{SBit}_d)$ [116]

$e: \mathsf{SIM} = \mathsf{msg}(d_7', \mathsf{SBit}_d)$ [117]

$\mathsf{SIM}_e = \mathsf{msg}(d_7', \mathsf{SBit}_d)$ [117′]

aus PA1:

$e: \exists D : \mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit}) \to \mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true})$ [118]

Linker Zweig:

$e: \neg(\exists D : \mathsf{SIM} = \mathsf{msg}(D, \mathsf{SBit}))$ [119]

$e: \neg(\mathsf{SIM} = \mathsf{msg}(D_8, \mathsf{SBit}))$ [121]

$\mathsf{SIM}_e \neq \mathsf{msg}(D_8, \mathsf{SBit}_e)$ [121′]

$\square:$ $\mathsf{SIM}_e = \mathsf{msg}(d_7', \mathsf{SBit}_d)$ [117′]
$\mathsf{SBit}_e = \mathsf{SBit}_a$ [112′]
$\mathsf{SBit}_d = \mathsf{SBit}_a$ [100′]
$\square$ $\{D_8 \leftarrow d_7\}$

Rechter Zweig:

$e: \mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true})$ [120]

$\square^*$ $(113, 120)$

In diesem Beweis tritt (mit N_1) endlich einmal eine freie Variable auf, die zur Einführung von echten Präfix*funktionen* führt. Die Präfixe a, b und c sind also von der Form $\hat{a}(N_1)$, $\hat{b}(N_1)$ und $\hat{c}(N_1)$, d_3 ist ebenfalls eine Skolemfunktion $\hat{d}_3(N_1)$.

22 Theorem 5: Totale Korrektheit

Theorem 5 liefert die abschließende totale Korrektheitsaussage:

$$\begin{aligned}&(\exists M : \mathsf{SFile}(M) \neq \bot \wedge \mathsf{SFile}(s(M)) = \bot) \rightarrow \\ &\rightarrow \mathsf{A}\Diamond(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N))\end{aligned}$$

Beweis:

Sei SFile nicht leer und endlich, letzter belegter Index sei m_1. Es wird ein Pfad p angenommen, auf dem kein Zustand erreicht wird, in dem ready wahr ist und alle Daten übertragen sind. SFile bleibt während der gesamten Berechnung unverändert. Aus Theorem 4 erhält man, daß für jedes nichtleere Element $\mathsf{SFile}(N)$ ein Zustand erreicht wird, in dem dieses in RFile abgelegt ist, und entweder $\mathsf{SNo} = s(n)$ oder $\mathsf{SNo} = n \wedge \mathsf{ready} = \mathsf{true}$ ist. Insbesondere ist dies für $n = m_1$ in einem Zustand a der Fall [32]. Da m_1 das letzte Element beschreiben soll, folgt, daß in a $\mathsf{SNo}_a = m_1$ und $\mathsf{ready} = \mathsf{true}$ ist [36]. Nach der oben gemachten Annahme existiert also ein n_5 mit $\mathsf{SFile}_0(n_5) \neq \bot$ und $\mathsf{RFile}_a(n_5) \neq \mathsf{SFile}_a(n_5) = \mathsf{SFile}_0(n_5)$ [45], [46].

Aus Korollar 5 ergibt sich, daß damit in aller Zukunft $\mathsf{RFile}(n_5)$ nicht mehr verändert wird, insbesondere $\neq \mathsf{SFile}_0(n_5)$ bleibt [54]. Aus Theorem 4 – diesmal für n_5 – erhält man, daß entlang p ein Zustand erreicht wird, in dem $\mathsf{RFile}(n_5) = \mathsf{SFile}(n_5)$ ist [68].

Dieser Zustand x kann nicht als b zwischen 0 und a liegen [71], da dann aus $\mathsf{RFile}_b(n_5) = \mathsf{SFile}_b(n_5)$ mit der Persistenz aus Korollar 4 $\mathsf{RFile}_a(n_5) = \mathsf{SFile}_b(n_5)$ folgt.
$x = a$ ist ebenfalls nicht möglich, so daß $x = c$ ein späterer Zustand als a sein muß [96]. Dieses widerspricht aber der Feststellung in [54].

$$0:\ \mathsf{SNo} = 0 \quad [1]$$
$$\mathsf{SNo}_0 = 0 \quad [1']$$
$$0:\ \forall N : \mathsf{RFile}(N) = \bot \quad [2]$$
$$|$$
$$0:\ \neg((\exists M : \mathsf{SFile}(M) \neq \bot \wedge \mathsf{SFile}(s(M)) = \bot) \rightarrow \quad [3]$$
$$\mathsf{A}\Diamond(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N)))$$
$$|$$
$$0:\ \exists M : \mathsf{SFile}(M) \neq \bot \wedge \mathsf{SFile}(s(M)) = \bot \quad [4]$$
$$0:\ \neg(\mathsf{A}\Diamond(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N))) \quad [5]$$
$$|$$
$$0:\ \mathsf{SFile}(m_1) \neq \bot \quad [6]$$
$$0:\ \mathsf{SFile}(s(m_1)) = \bot \quad [7]$$
$$\mathsf{SFile}_0(m_1) \neq \bot \quad [6']$$
$$\mathsf{SFile}_0(s(m_1)) = \bot \quad [7']$$
$$|$$
$$p : [\,0, \emptyset, \infty] \quad [8]$$
$$0:\ p\,\neg(\Diamond(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N))) \quad [9]$$
$$0:\ \neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N)) \quad [10]$$
$$0:\ (p)\Box(\neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N))) \quad [11]$$
$$p : [\,0, \{\neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N))\}, \infty] \quad [12]$$
$$|$$

aus SData:

$$0:\ \forall N : \nabla SFile : \mathsf{A}\Box(\mathsf{SFile}(N) = SFile(N)) \quad [13]$$
$$0:\ \nabla SFile : \mathsf{A}\Box(\mathsf{SFile}(N_2) = SFile(N_2)) \quad [14]$$
$$0:\ \mathsf{A}\Box(\mathsf{SFile}(N_2) = \mathsf{SFile}_0(N_2)) \quad [15]$$
$$0:\ \mathsf{SFile}(N_2) = \mathsf{SFile}_0(N_2) \quad [16]$$
$$0:\ (\mathsf{A})\Box(\mathsf{SFile}(N_2) = \mathsf{SFile}_0(N_2)) \quad [17]$$
$$p : [\,0, \{\mathsf{SFile}(s(N_2)) = \mathsf{SFile}_0(N_2)\}, \infty] \quad [18]$$
$$|$$
$$p : [\,0, \{\neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N)), \mathsf{SFile}(s(N_2)) = \mathsf{SFile}_0(N_2)\}, \infty] \quad [19]$$
$$|$$

mit Theorem 4:

$$0:\ \forall N : (\mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(N) = \mathsf{SFile}(N) \wedge (\mathsf{SNo} = s(N) \vee (\mathsf{SNo} = N \wedge \mathsf{ready})))) \quad [20]$$
$$0:\ \mathsf{SFile}(N_3) \neq \bot \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(N_3) = \mathsf{SFile}(N_3) \wedge (\mathsf{SNo} = s(N_3) \vee (\mathsf{SNo} = N_3 \wedge \mathsf{ready}))) \quad [21]$$

$$0:\ \neg(\mathsf{SFile}(N_3) \neq \bot) \quad [22]$$
$$\mathsf{SFile}_0(N_3) = \bot) \quad [22']$$
$$\Box\ \{N_3 \leftarrow m_1\}(6', 22')$$

$$0:\ \mathsf{A}\Diamond(\mathsf{RFile}(m_1) = \mathsf{SFile}(m_1) \wedge (\mathsf{SNo} = s(m_1) \vee (\mathsf{SNo} = m_1 \wedge \mathsf{ready}))) \quad [23]$$

$\hookrightarrow$ S. 338

$\vdots$

von [23] (S. 337):

$p : [\,0, \{\neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N)), \mathsf{SFile}(s(N_2)) = \mathsf{SFile}_0(N_2)\}, \infty]$ [19]

$\mathsf{SFile}_0(m_1) \neq \bot$ [6′]

$\mathsf{SFile}_0(s(m_1)) = \bot$ [7′]

$0 : \ \mathsf{A}\Diamond(\mathsf{RFile}(m_1) = \mathsf{SFile}(m_1) \wedge (\mathsf{SNo} = s(m_1) \vee (\mathsf{SNo} = m_1 \wedge \mathsf{ready})))$ [23]

Linker Zweig:

$0 : \ \mathsf{RFile}(m_1) = \mathsf{SFile}(m_1) \wedge (\mathsf{SNo} = s(m_1) \vee (\mathsf{SNo} = m_1 \wedge \mathsf{ready}))$ [24]

$0 : \ \mathsf{RFile}(m_1) = \mathsf{SFile}(m_1)$ [26]

$\mathsf{RFile}_0(m_1) = \mathsf{SFile}_0(m_1)$ [26′]

$0 : \ \mathsf{SNo} = s(m_1) \vee (\mathsf{SNo} = m_1 \wedge \mathsf{ready})$ [27]

aus [2]:

$0 : \ \mathsf{RFile}(N_4) = \bot$ [28]

$\mathsf{RFile}_0(N_4) = \bot$ [28′]

$\Box :$ $\mathsf{SFile}_0(m_1) \neq \bot$ [6′]
$\mathsf{RFile}_0(m_1) = \mathsf{SFile}_0(m_1)$ [26′]
$\{N_4 \leftarrow m_1\}$

Rechter Zweig:

$0 : \ (\mathsf{A})\Diamond(\mathsf{RFile}(m_1) = \mathsf{SFile}(m_1) \wedge (\mathsf{SNo} = s(m_1) \vee (\mathsf{SNo} = m_1 \wedge \mathsf{ready})))$ [25]

auf p:

$p : [\,0, \{\neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N)), \mathsf{SFile}(s(N_2)) = \mathsf{SFile}_0(N_2)\},$ [29]
$a, \{\neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N)), \mathsf{SFile}(s(N_2)) = \mathsf{SFile}_0(N_2)\}, \infty]$

$a : \ \neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N))$ [30]

$a : \ \mathsf{SFile}(s(N_2)) = \mathsf{SFile}_0(N_2)$ [31]

$\mathsf{SFile}_a(s(N_2)) = \mathsf{SFile}_0(N_2)$ [31′]

$a : \ \mathsf{RFile}(m_1) = \mathsf{SFile}(m_1) \wedge (\mathsf{SNo} = s(m_1) \vee (\mathsf{SNo} = m_1 \wedge \mathsf{ready}))$ [32]

$a : \ \mathsf{RFile}(m_1) = \mathsf{SFile}(m_1)$ [33]

$a : \ \mathsf{SNo} = s(m_1) \vee (\mathsf{SNo} = m_1 \wedge \mathsf{ready})$ [34]

$\mathsf{RFile}_a(m_1) = \mathsf{SFile}_a(m_1)$ [33′]

$\hookrightarrow$ S. 339

$\vdots$

von [34] (S. 338):

$$p : [0, \{\neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N)), \mathsf{SFile}(s(N_2)) = \mathsf{SFile}_0(N_2)\}, \infty] \quad [19]$$

$$\mathsf{SFile}_0(s(m_1)) = \bot \quad [7']$$

$$a : \neg(\mathsf{ready} = \mathsf{true} \wedge \forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N)) \quad [30]$$

$$\mathsf{SFile}_a(s(N_2)) = \mathsf{SFile}_0(N_2) \quad [31']$$

$$\mathsf{RFile}_a(m_1) = \mathsf{SFile}_a(m_1) \quad [33']$$

$$a : \mathsf{SNo} = s(m_1) \vee (\mathsf{SNo} = m_1 \wedge \mathsf{ready}) \quad [34]$$

$$a : \mathsf{SNo} = s(m_1) \quad [35]$$

$$\mathsf{SNo}_a = s(m_1) \quad [35']$$

aus Korollar 1 in a:

$$a : \mathsf{SNo} = 0 \vee \mathsf{SFile}(\mathsf{SNo}) \neq \bot \quad [37]$$

$$a : \mathsf{SNo} = 0 \quad [38]$$

$$\mathsf{SNo}_a = 0 \quad [38']$$

$$\Box \ (\mathrm{E}6, 35', 38')$$

$$a : \mathsf{SFile}(\mathsf{SNo}) \neq \bot \quad [39]$$

$$\mathsf{SFile}_a(\mathsf{SNo}_a) \neq \bot \quad [39']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{SNo}_a = s(m_1) \quad [35'] \\ & \mathsf{SFile}_a(s(N_2)) = \mathsf{SFile}_0(N_2) \quad [31'] \\ & \mathsf{SFile}_0(s(m_1)) = \bot \quad [7'] \\ & \{N_2 \leftarrow s(m_1)\} \end{array}}$$

$$a : \mathsf{SNo} = m_1 \wedge \mathsf{ready} \quad [36]$$

$$a : \mathsf{SNo} = m_1 \quad [40]$$

$$a : \mathsf{ready} = \mathsf{true} \quad [41]$$

$$\mathsf{SNo}_a = m_1 \quad [40']$$

aus [30]:

$$a : \neg(\mathsf{ready} = \mathsf{true}) \quad [42]$$

$$\Box \ (41, 42)$$

$$a : \neg(\forall N : \mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{RFile}(N) = \mathsf{SFile}(N)) \quad [43]$$

$$a : \neg(\mathsf{SFile}(n_5) \neq \bot \rightarrow \mathsf{RFile}(n_5) = \mathsf{SFile}(n_5)) \quad [44]$$

$$a : \mathsf{SFile}(n_5) \neq \bot \quad [45]$$

$$a : \neg(\mathsf{RFile}(n_5) = \mathsf{SFile}(n_5)) \quad [46]$$

$$\mathsf{SFile}_a(n_5) \neq \bot \quad [45']$$

$$\mathsf{RFile}_a(n_5) \neq \mathsf{SFile}_a(n_5) \quad [46']$$

aus Korollar 5, Teil 3:

$$a : \mathsf{ready} = \mathsf{true} \rightarrow (\forall N : \nabla RFile : \mathsf{A}\Box(\mathsf{RFile}(N) = RFile(N))) \quad [47]$$

$$a : \neg(\mathsf{ready} = \mathsf{true}) \quad [48]$$

$$\Box \ (41, 48)$$

$$a : \forall N : \nabla RFile : \mathsf{A}\Box(\mathsf{RFile}(N) = RFile(N)) \quad [49]$$

$$a : \nabla RFile : \mathsf{A}\Box(\mathsf{RFile}(N_7) = RFile(N_7)) \quad [50]$$

$$a : \mathsf{A}\Box(\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7)) \quad [51]$$

$\hookrightarrow$ S. 340

$\vdots$

von [51] (S. 339):

$$p : [\,0, \{\ldots\}, \infty] \quad [19]$$

$$\mathsf{SFile}_a(n_5) \neq \bot \quad [45']$$

$$\mathsf{RFile}_a(n_5) \neq \mathsf{SFile}_a(n_5) \quad [46']$$

$$a : \ \mathsf{A}\Box(\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7)) \quad [51]$$

$$|$$

$$a : \ \mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7) \quad [52]$$

$$a : \ (\mathsf{A})\Box(\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7)) \quad [53]$$

auf p:

$$p : [\,0, \{\ldots\}, a, \{\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7)\}, \infty] \quad [54]$$

$$|$$

aus SData:

$$0 : \ \forall N : \nabla SFile : \mathsf{A}\Box(\mathsf{SFile}(N) = SFile(N)) \quad [55]$$

$$0 : \ \nabla SFile : \mathsf{A}\Box(\mathsf{SFile}(N_8) = SFile(N_8)) \quad [56]$$

$$0 : \ \mathsf{A}\Box(\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)) \quad [57]$$

$$0 : \ \mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8) \quad [58]$$

$$0 : \ (\mathsf{A})\Box(\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)) \quad [59]$$

auf p:

$$p : [\,0, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, a, \{\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7)\}, \infty] \quad [60]$$

$$a : \ \mathsf{A}\Box(\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)) \quad [61]$$

$$|$$

$$a : \ \mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8) \quad [62]$$

$$a : \ (\mathsf{A})\Box(\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)) \quad [63]$$

$$\mathsf{SFile}_a(N_8) = \mathsf{SFile}_0(N_8) \quad [62']$$

auf p:

$$p : [\,0, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, a, \{\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7), \mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, \infty] \quad [64]$$

$$|$$

mit Theorem 4:

$$0 : \ \forall N : (\mathsf{SFile}(N) \neq \bot \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(N) = \mathsf{SFile}(N) \wedge (\mathsf{SNo} = s(N) \vee (\mathsf{SNo} = N \wedge \mathsf{ready})))) \quad [65]$$

$$0 : \ \mathsf{SFile}(N_9) \neq \bot \rightarrow \mathsf{A}\Diamond(\mathsf{RFile}(N_9) = \mathsf{SFile}(N_9) \wedge (\mathsf{SNo} = s(N_9) \vee (\mathsf{SNo} = N_9 \wedge \mathsf{ready}))) \quad [66]$$

$$0 : \ \neg(\mathsf{SFile}(N_9) \neq \bot) \quad [67]$$

$$\mathsf{SFile}_0(N_9) = \bot \quad [67']$$

$$\boxed{\begin{array}{ll} \Box : & \mathsf{SFile}_a(n_5) \neq \bot \quad [45'] \\ & \mathsf{SFile}_a(N_8) = \mathsf{SFile}_0(N_8) \quad [62'] \\ & \{N_8 \leftarrow n_5,\ N_9 \leftarrow n_5\} \end{array}}$$

$$0 : \ \mathsf{A}\Diamond(\mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge (\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready}))) \quad [68]$$

↪ S. 341

$\vdots$

von [68] (S. 340):

$p : [\,0, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, a, \{\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7), \mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, \infty]$ [64]

$\mathsf{SFile}_a(n_5) \neq \bot$ [45′]

$\mathsf{RFile}_a(n_5) \neq \mathsf{SFile}_a(n_5)$ [46′]

$\mathsf{SFile}_a(N_8) = \mathsf{SFile}_0(N_8)$ [62′]

$0 : \ \mathsf{A}\Diamond(\mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge (\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready})))$ [68]

$0 : \ \mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge$ [69]
$(\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready}))$

wie [24] mit
$\mathsf{SFile}_a(n_5) \neq \bot$ [45′]
$\mathsf{SFile}_a(N_8) = \mathsf{SFile}_0(N_8)$ [62′]
$\{N_8 \leftarrow n_5\}$ aus [67’]

$0 : \ (\mathsf{A})\Diamond(\mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge (\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready})))$ [70]

auf p:

$p : [\,0, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\},$ [71]
$b, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, a, \{\ldots\}, \infty]$

$b : \ \mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)$ [72]

$b : \ \mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge$ [73]
$(\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready}))$
$\mathsf{SFile}_b(N_8) = \mathsf{SFile}_0(N_8)$ [72′]

$b : \ \mathsf{RFile}(n_5) = \mathsf{SFile}(n_5)$ [76]
$\mathsf{RFile}_b(n_5) = \mathsf{SFile}_b(n_5)$ [76′]

$b : \ \mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready})$ [77]

mit Korollar 4:

$b : \ \forall N : \nabla RFile : \mathsf{RFile}(N) \neq \bot \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N) = RFile(N))$ [78]

$b : \ \nabla RFile : \mathsf{RFile}(N_{11}) \neq \bot \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N_{11}) = RFile(N_{11}))$ [79]

$b : \ \mathsf{RFile}(N_{11}) \neq \bot \rightarrow \mathsf{A}\Box(\mathsf{RFile}(N_{11}) = \mathsf{RFile}_b(N_{11}))$ [80]

$\hookrightarrow$ S. 342

$p : [\,0, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\},$ [74]
$a, \{\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7),$
$\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, \infty]$

$a : \ \mathsf{A}\Diamond(\mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge$ [75]
$(\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready})))$

$\hookrightarrow$ S. 343

$\vdots$

von [80] (S. 341):

$p : [\,0, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, b, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, a, \{\ldots\}, \infty]$ [71]

$\mathsf{SFile}_a(n_5) \neq \perp$ [45′]

$\mathsf{RFile}_a(n_5) \neq \mathsf{SFile}_a(n_5)$ [46′]

$\mathsf{SFile}_a(N_8) = \mathsf{SFile}_0(N_8)$ [62′]

$\mathsf{SFile}_b(N_8) = \mathsf{SFile}_0(N_8)$ [72′]

$\mathsf{RFile}_b(n_5) = \mathsf{SFile}_b(n_5)$ [76′]

$b :\ \mathsf{RFile}(N_{11}) \neq \perp \to \mathsf{A}\Box(\mathsf{RFile}(N_{11}) = \mathsf{RFile}_b(N_{11}))$ [80]

Linker Zweig:

$b :\ \neg(\mathsf{RFile}(N_{11}) \neq \perp)$ [81]

$\mathsf{RFile}_b(N_{11}) = \perp$ [81′]

$\Box :\ \mathsf{SFile}_a(n_5) \neq \perp$ [45′]
$\mathsf{SFile}_a(N_8) = \mathsf{SFile}_0(N_8)$ [62′]
$\mathsf{SFile}_b(N_8) = \mathsf{SFile}_0(N_8)$ [72′]
$\mathsf{RFile}_b(n_5) = \mathsf{SFile}_b(n_5)$ [76′]
$\{N_8 \leftarrow n_5\}$ aus [67’]
$\{N_{11} \leftarrow n_5\}$

Rechter Zweig:

$b :\ \mathsf{A}\Box(\mathsf{RFile}(n_5) = \mathsf{RFile}_b(n_5))$ [82]

$b :\ \mathsf{RFile}(n_5) = \mathsf{RFile}_b(n_5)$ [83]

$b :\ (\mathsf{A})\Box(\mathsf{RFile}(n_5) = \mathsf{RFile}_b(n_5))$ [84]

auf p:

$p : [\,0, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\},$ [85]
$b, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8),$
$\mathsf{RFile}(n_5) = \mathsf{RFile}_b(n_5)\}$
$a, \{\ldots\}, \infty]$

$a :\ \mathsf{A}\Box(\mathsf{RFile}(n_5) = \mathsf{RFile}_b(n_5))$ [86]

$a :\ \mathsf{RFile}(n_5) = \mathsf{RFile}_b(n_5)$ [87]

$\mathsf{RFile}_a(n_5) = \mathsf{RFile}_b(n_5)$ [87′]

$a :\ (\mathsf{A})\Box(\mathsf{RFile}(n_5) = \mathsf{RFile}_b(n_5))$ [88]

$\Box :\ \mathsf{RFile}_a(n_5) = \mathsf{RFile}_b(n_5)$ [87′]
$\mathsf{RFile}_b(n_5) = \mathsf{SFile}_b(n_5)$ [76′]
$\mathsf{SFile}_b(N_8) = \mathsf{SFile}_0(N_8)$ [72′]
$\mathsf{SFile}_a(N_8) = \mathsf{SFile}_0(N_8)$ [62′]
$\mathsf{RFile}_a(n_5) \neq \mathsf{SFile}_a(n_5)$ [46′]
$\{N_8 \leftarrow n_5\}$ aus [67’]

$$\vdots$$

von [75] (S. 341):

$$p : [\,0, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, a, \{\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7), \mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, \infty] \quad [74]$$

$$\mathsf{RFile}_a(n_5) \neq \mathsf{SFile}_a(n_5) \quad [46']$$

$$\mathsf{SFile}_a(N_8) = \mathsf{SFile}_0(N_8) \quad [62']$$

$$a: \ \mathsf{A}\Diamond(\mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge (\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready}))) \quad [75]$$

$$a: \ \mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge (\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready})) \quad [89]$$

$$a: \ \mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \quad [91]$$

$$\mathsf{RFile}_a(n_5) = \mathsf{SFile}_a(n_5) \quad [91']$$

$$a: \ \mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready}) \quad [92]$$

$$\square \ (46', 91')$$

$$a: \ (\mathsf{A})\Diamond(\mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge (\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready}))) \quad [90]$$

auf p:

$$p : [\,0, \{\mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, a, \{\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7), \mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, c, \{\mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7), \mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8)\}, \infty] \quad [93]$$

$$c: \ \mathsf{RFile}(N_7) = \mathsf{RFile}_a(N_7) \quad [94]$$

$$c: \ \mathsf{SFile}(N_8) = \mathsf{SFile}_0(N_8) \quad [95]$$

$$\mathsf{RFile}_c(N_7) = \mathsf{RFile}_a(N_7) \quad [94']$$

$$\mathsf{SFile}_c(N_8) = \mathsf{SFile}_0(N_8) \quad [95']$$

$$c: \ \mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \wedge (\mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready})) \quad [96]$$

$$c: \ \mathsf{RFile}(n_5) = \mathsf{SFile}(n_5) \quad [97]$$

$$\mathsf{RFile}_c(n_5) = \mathsf{SFile}_c(n_5) \quad [97']$$

$$c: \ \mathsf{SNo} = s(n_5) \vee (\mathsf{SNo} = n_5 \wedge \mathsf{ready}) \quad [98]$$

$$\boxed{\begin{array}{ll} \square: & \{N_8 \leftarrow n_5\} \text{ aus } [67\text{'}] \\ & \mathsf{SFile}_a(N_8) = \mathsf{SFile}_0(N_8) \quad [62'] \\ & \mathsf{SFile}_c(N_8) = \mathsf{SFile}_0(N_8) \quad [95'] \\ & \mathsf{RFile}_c(n_5) = \mathsf{SFile}_c(n_5) \quad [97'] \\ & \mathsf{RFile}_c(N_7) = \mathsf{RFile}_a(N_7) \quad [94'] \\ & \mathsf{RFile}_a(n_5) \neq \mathsf{SFile}_a(n_5) \quad [46'] \\ & \{N_7 \leftarrow n_5\} \end{array}}$$

23 Abschließende Betrachtung

23.1 Erkenntnisse

Im Beweis wurden die Informationen über die verwendeten Datentypen etwas vernachlässigt. Dies betrifft vor allem den Datentyp „Bit", wo bei einigen Abschlüssen implizit verwendet wurde, daß aus $b_i \neq b_j$ $b_i = \mathsf{flip}(b_j)$ folgt. Eine in dieser Hinsicht vollständige Durchführung hätte den Aufwand weiter erhöht, ohne zu grundlegend neuen Erkenntnissen zu führen.

Die Durchführung des Beweises zeigt und motiviert den Nutzen des kombinierten Einsatzes der Gleichungsbehandlung und des ∇-Quantors zur Behandlung zustandsabhängig interpretierter Bezeichner.

Ein konsequenter Einsatz des ∇-Quantors (d.h. Bindung aller Auftreten von zustandsabhängig interpretierten Bezeichnern durch einen ∇-Quantor) macht die in [May95], Abschnitt 9.3 beschriebene Globalisierungsregel für Gleichungsatome

$$\boxed{\frac{\gamma : \mathsf{bezeichner} = wert}{\mathsf{bezeichner}_\gamma = wert}}$$

sogar überflüssig:
Wird *jedes* Auftreten eines zustandsabhängig interpretierten Bezeichners durch einen ∇-Quantor gebunden, erreicht man, daß bereits in den logischen Formeln *alle* zustandsabhängig interpretierten Bezeichner mit einem Präfix indiziert sind, womit man die übliche Globalisierungsregel

$$\boxed{\frac{\gamma : F}{\boldsymbol{K} : F} \qquad \text{falls } F = p(t_1, \ldots, t_n),\ p \in \Sigma^c(\boldsymbol{K}),\ t_i \in \mathsf{Term}\Sigma^c(\boldsymbol{K})}$$

anwenden kann.

Da dabei i.a. verschiedene Vorkommen eines Bezeichners an verschiedene Präfixe gebunden werden sollen, wie etwa in der Persistenzforderung

$$\nabla SFile^1 : \mathsf{A}\Box(\nabla SFile^2 : SFile^2 = SFile^1) \quad ,$$

muß man zusätzliche formale Mittel (hier numerische hochgestellte Indizes) zur Zuordnung einsetzen.

Das Vorgehen ist nicht auf die Namen der Regeln anzuwenden, obwohl sie ebenfalls zustandsabhängig interpretierte Bezeichner sind. Sie sind als Prädikate und nicht als Gleichungen zu verstehen und werden beim Abschluß von Zweigen nur gemeinsam mit direkten Negationen bei gleichem Präfix verwendet.

Andererseits bleibt man mit der o.g. Gleichungsregel und *ohne* den ∇-Quantor näher an der traditionellen prädikatenlogischen Syntax und Vorgehensweise. Insbesondere ist die Anwendbarkeit dieser Optimierungen auf Evolving Algebras beschränkt. In der Ausdruckskraft ergeben sich keine Unterschiede zwischen den beiden Alternativen sowie den in den einzelnen Beweisen verwendeten Zwischenformen.

Insgesamt ergibt sich – mit ∇-Quantor – die folgende überarbeitete Axiomatisierung von $\mathcal{ABP}$, mit der man den Beweis idealerweise durchführen sollte:

Datenstrukturaxiome

DSB: $\nabla SB : \mathsf{Bit}(SB) = \mathsf{true}$

DRB: $\nabla RB : \mathsf{Bit}(RB) = \mathsf{true}$

B1: $\forall B : \mathsf{Bit}(B) = \mathsf{true} \leftrightarrow \mathsf{Bit}(\mathsf{flip}(B)) = \mathsf{true}$

B2: $\forall B, B' : (\mathsf{Bit}(B) = \mathsf{true} \wedge \mathsf{Bit}(B') = \mathsf{true}) \to (B = B' \vee B = \mathsf{flip}(B'))$

B3: $\forall B : \mathsf{Bit}(B) = \mathsf{true} \to B = \mathsf{flip}(\mathsf{flip}(B))$

B4: $\forall B : \mathsf{Bit}(B) = \mathsf{true} \to B \neq \mathsf{flip}(B)$

B5: $\forall B, B' : (\mathsf{Bit}(B) = \mathsf{true} \wedge \mathsf{Bit}(B') = \mathsf{true} \wedge \mathsf{flip}(B) = \mathsf{flip}(B')) \to B = B'$

DSN: $\nabla SNo : \mathsf{Integer}(SNo) = \mathsf{true}$

DRN: $\nabla RNo : \mathsf{Integer}(RNo) = \mathsf{true}$

N1: $\forall N : \mathsf{Integer}(N) = \mathsf{true} \leftrightarrow (N = 0 \vee \exists N' : \mathsf{Integer}(N') = \mathsf{true} \wedge N = s(N'))$

N2: $\forall N : \mathsf{Integer}(N) = \mathsf{true} \to p(s(N)) = N$

N3: $\forall N : \mathsf{Integer}(N) = \mathsf{true} \to s(N) \neq N$

N4: $\forall N, N' : (\mathsf{Integer}(N) = \mathsf{true} \wedge \mathsf{Integer}(N') = \mathsf{true} \wedge s(N) = s(N')) \to N = N'$

N5: $\forall N, N' : (\mathsf{Integer}(N) = \mathsf{true} \wedge \mathsf{Integer}(N') = \mathsf{true} \wedge p(N) = p(N')) \to N = N'$

DSM: $\nabla SIM : \mathsf{Message}(SIM) = \mathsf{true}$

DRM: $\nabla RIM : \mathsf{Message}(RIM) = \mathsf{true}$

M1: $\forall M : \mathsf{Message}(M) = \mathsf{true} \leftrightarrow$
$(M = \bot \vee \exists D, B : \mathsf{Bit}(B) = \mathsf{true} \wedge \mathsf{Data}(D) = \mathsf{true} \wedge M = \mathsf{msg}(D, B))$

M2: $\forall D, D', B, B' : (\mathsf{Message}(\mathsf{msg}(D, B)) = \mathsf{true} \wedge \mathsf{Message}(\mathsf{msg}(D', B')) = \mathsf{true}$
$\mathsf{msg}(D, B) = \mathsf{msg}(D', B')) \to$
$\to D = D' \wedge B = B'$

DSQ: $\nabla SQ : \mathsf{Queue}(SQ) = \mathsf{true}$

DRQ: $\nabla RQ : \mathsf{Queue}(RQ) = \mathsf{true}$

Q1: $\forall Q : \mathsf{Queue}(Q) = \mathsf{true} \leftrightarrow$
$Q = \varepsilon \vee ((\exists M, Q' : (Q = M|Q' \wedge \mathsf{Queue}(Q') = \mathsf{true} \wedge \mathsf{Message}(M) = \mathsf{true}) \wedge$
$(\exists M, Q' : (Q = Q'|M \wedge \mathsf{Queue}(Q') = \mathsf{true} \wedge \mathsf{Message}(M) = \mathsf{true})))$

Q2: $\forall M, M', Q, Q' : (\mathsf{Queue}(M|Q) = \mathsf{true} \wedge \mathsf{Queue}(M'|Q') = \mathsf{true} \wedge$
$\mathsf{Message}(M) = \mathsf{true} \wedge \mathsf{Message}(M) = \mathsf{true} \wedge M|Q = M'|Q') \to$
$\to M = M' \wedge Q = Q'$

Q3: $\forall M, M', Q, Q' : (\mathsf{Queue}(Q|M) = \mathsf{true} \wedge \mathsf{Queue}(Q'|M') = \mathsf{true} \wedge$
$\mathsf{Message}(M) = \mathsf{true} \wedge \mathsf{Message}(M) = \mathsf{true} \wedge Q|M = Q'|M') \to$
$\to M = M' \wedge Q = Q'$

Bool: $\mathsf{ready} = \mathsf{true} \vee \mathsf{ready} = \mathsf{false}$

DSF: $\nabla SFile : \forall N : \mathsf{Integer}(N) = \mathsf{true} \to \mathsf{Data}(SFile(N)) = \mathsf{true}$

DRF: $\nabla RFile : \forall N : \mathsf{Integer}(N) = \mathsf{true} \to \mathsf{Data}(RFile(N)) = \mathsf{true}$

Startzustand:

$$\mathsf{SNo}_0 = 0 \wedge \mathsf{RNo}_0 = 0 \wedge \mathsf{SIM}_0 = \perp \wedge \mathsf{RIM}_0 = \perp \wedge SQ_0 = \varepsilon \wedge \mathsf{RQ}_0 = \varepsilon \wedge$$
$$\forall N : \mathsf{SFile}_0(N) = \perp \rightarrow \mathsf{SFile}_0(s(N)) = \perp \wedge \exists N : \mathsf{SFile}_0 = \perp$$

Anwendbarkeit:

SC1:	$(\nabla SIM, SQ : SIM = \perp \wedge \exists D, B, Q : SQ = \mathsf{msg}(D,B)\vert Q) \leftrightarrow \mathsf{E}\circ(\mathsf{SendCom} = \mathsf{true})$
RC1:	$(\nabla RIM, RQ : RIM = \perp \wedge \exists D, B, Q : RQ = \mathsf{msg}(D,B)\vert Q) \leftrightarrow \mathsf{E}\circ(\mathsf{RecCom} = \mathsf{true})$
SL1:	$(\nabla SQ : SQ \neq \varepsilon) \leftrightarrow \mathsf{E}\circ(\mathsf{SLose} = \mathsf{true})$
RL1:	$(\nabla RQ : RQ \neq \varepsilon) \leftrightarrow \mathsf{E}\circ(\mathsf{RLose} = \mathsf{true})$
RT1:	$\mathsf{E}\circ(\mathsf{ReTrans} = \mathsf{true})$
PA1:	$(\nabla SBit, SIM : \exists D : SIM = \mathsf{msg}(D, SBit)) \leftrightarrow \mathsf{E}\circ(\mathsf{ProcAck} = \mathsf{true})$
CM1:	$(\nabla SIM : \exists D, B : SIM = \mathsf{msg}(D, B)) \leftrightarrow \mathsf{E}\circ(\mathsf{ClMsg} = \mathsf{true})$
AD1:	$(\nabla RBit, RIM : \exists D : RIM = \mathsf{msg}(D, RBit)) \leftrightarrow \mathsf{E}\circ(\mathsf{AccDat} = \mathsf{true})$
AM1:	$(\nabla RBit, RIM : \exists D : RIM = \mathsf{msg}(D, \mathsf{flip}(RBit))) \leftrightarrow \mathsf{E}\circ(\mathsf{AckMsg} = \mathsf{true})$

Invarianzaxiome:

SIM:	$\nabla SIM^1 : \mathsf{A}(\nabla SIM^2 : SIM^2 = SIM^1 \ \mathsf{unless}^+ \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{ClMsg} = \mathsf{true})$
RIM:	$\nabla RIM^1 : \mathsf{A}(\nabla RIM^2 : RIM^2 = RIM^1 \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$
SQ:	$\nabla SQ^1 : \mathsf{A}(\nabla SQ^2 : SQ^2 = SQ^1 \ \mathsf{unless}^+ \ \mathsf{SendCom} = \mathsf{true} \vee \mathsf{SLose} = \mathsf{true} \vee \mathsf{AckMsg} = \mathsf{true})$
RQ:	$\nabla RQ^1 : \mathsf{A}(\nabla RQ^2 : RQ^2 = RQ^1 \ \mathsf{unless}^+ \ \mathsf{RecCom} = \mathsf{true} \vee \mathsf{RLose} = \mathsf{true} \vee \mathsf{ReTrans} = \mathsf{true} \vee \mathsf{ProcAck} = \mathsf{true})$
SBit:	$\nabla SBit^1 : \mathsf{A}(\nabla SBit^2 : SBit^2 = SBit^1 \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true})$
RBit:	$\nabla RBit^1 : \mathsf{A}(\nabla RBit^2 : RBit^2 = RBit^1 \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true})$
SFile:	$\nabla SFile^1 : \mathsf{A}\Box(\nabla SFile^2 : SFile^2 = SFile^1)$
RFile:	$\nabla RFile^1 : \mathsf{A}(\nabla RFile^2 : RFile^2 = RFile^1 \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true})$
SNo:	$\nabla SNo^1 : \mathsf{A}(\nabla SNo^2 : SNo^2 = SNo^1 \ \mathsf{unless}^+ \ \mathsf{ProcAck} = \mathsf{true})$
RNo:	$\nabla RNo^1 : \mathsf{A}(\nabla RNo^2 : RNo^2 = RNo^1 \ \mathsf{unless}^+ \ \mathsf{AccDat} = \mathsf{true})$

Auswirkungen der Regeln:

SC2: $\forall D, B, Q: \ (\nabla SQ : SQ = \mathsf{msg}(D,B)|Q) \rightarrow$
$\quad \mathsf{A}\circ(\mathsf{SendCom} = \mathsf{true} \rightarrow \nabla SQ, SIM : SQ = Q \wedge SIM = \mathsf{msg}(D,B))$

RC2: $\forall D, B, Q: \ (\nabla RQ : RQ = \mathsf{msg}(D,B)|Q) \rightarrow$
$\quad \mathsf{A}\circ(\mathsf{RecCom} = \mathsf{true} \rightarrow \nabla RQ, RIM : RQ = Q \wedge RIM = \mathsf{msg}(D,B))$

SL2: $\forall Q: \ (\nabla SQ : SQ = Q) \rightarrow$
$\quad \mathsf{A}\circ(\mathsf{SLose} = \mathsf{true} \rightarrow (\nabla SQ : \exists Q^0, D, B, Q^1 : Q = Q^0|\mathsf{msg}(D,B)|Q^1 \wedge SQ = Q^0|Q^1))$

RL2: $\forall Q: \ (\nabla RQ : RQ = Q) \rightarrow$
$\quad \mathsf{A}\circ(\mathsf{RLose} = \mathsf{true} \rightarrow (\nabla RQ : \exists Q^0, D, B, Q^1 : Q = Q^0|\mathsf{msg}(D,B)|Q^1 \wedge RQ = Q^0|Q^1))$

RT2: $\nabla RQ^1 : \ \mathsf{A}\circ(\mathsf{ReTrans} = \mathsf{true} \rightarrow$
$\quad \nabla RQ^2, SFile, SNo, SBit : RQ = RQ^1|\mathsf{msg}(SFile(SNo), SBit))$

PA2: $\nabla RQ^1, SBit^1, SIM^1, SNo^1 : \forall D :$
$SIM = \mathsf{msg}(D, SBit) \rightarrow$
$\mathsf{A}\circ(\mathsf{ProcAck} = \mathsf{true} \rightarrow$
$(\nabla SFile, RQ^2, SNo^2, SBit^2, ready :$
$SFile(s(SNo^1)) \neq \bot \rightarrow \ RQ^2 = RQ^1|\mathsf{msg}(SFile(SNo^2), SBit^2)$
$\wedge\, SNo^2 = s(SNo^1) \wedge SBit^2 = \mathsf{flip}(SBit^1)$
$\wedge\, ready = \mathsf{false})$
$\wedge\, (\nabla SFile, RQ^2, SNo^2, SBit^2, ready :$
$SFile(s(SNo^1)) = \bot \rightarrow \ RQ^2 = RQ^1 \wedge SNo^2 = SNo^1 \wedge SBit^2 = SBit^1$
$\wedge\, ready = \mathsf{true}))$

CM2: $\mathsf{ClMsg} = \mathsf{true} \rightarrow (\nabla SIM : SIM = \bot)$

AD2: $\nabla RIM : \forall D, B :$
$(RIM = \mathsf{msg}(D,B) \rightarrow$
$\mathsf{A}\circ(\mathsf{AccDat} = \mathsf{true} \rightarrow$
$\nabla RFile, RNo^2, RBit : RFile(RNo^1) = D \wedge RNo^2 = s(RNo^1) \wedge RBit = \mathsf{flip}(B)))$

AM2: $\nabla SQ^1, RIM^1 : \forall D, B :$
$(RIM^1 = \mathsf{msg}(D,B) \rightarrow$
$\mathsf{A}\circ(\mathsf{AckMsg} = \mathsf{true} \rightarrow \nabla SQ^2, RIM^2 : SQ^2 = SQ^1|\mathsf{msg}(\lambda, B) \wedge RIM^2 = \bot))$

23.2 Fazit

Neben den Erkenntnissen des vorhergehenden Abschnittes zeigt der vorliegende Beweis, *daß* es möglich ist, Protokolle mit dem vorgestellten Kalkül formal zu verifizieren, womit die Fallstudie die beiden eingangs erwähnten Zielsetzungen erfüllt hat.

Die Verwendung der speziell auf die Beschreibung von Evolving Algebras abgestimmten Optimierungen (Globalisierung von Gleichungen und ∇-Quantor) ab Lemma 7 brachte folgende Ergebnisse:

- Verkürzung der Beweise um 10-15% gegenüber der nicht optimierten Vorgehensweise.
- Verbesserte Lesbarkeit der Beweise, da die Bezeichner nicht mehr einfach b_{17} heißen, sondern als SBit_σ aussagekräftiger sind. Dies ist insbesondere für eine interaktive Beweisführung von Vorteil.

Eine Implementierung als interaktives Beweissystem sollte eine konsequente Anwendung des ∇-Quantors sowie der Universen unterstützen.

Weiterhin zeigt sich, daß der größte Teil aus reinen Induktionsbeweisen über die Zustandsfolge besteht. Diese stellen geringe modallogische Anforderungen (sie sind prinzipiell sogar prädikatenlogisch codierbar), dafür erfordern sie eine komplizierte Gleichheitsbehandlung, da i.a. viele Fallunterscheidungen notwendig sind. Im übrigen ist dieser Teil – da er keine Fairness verwendet – auch in CTL formulierbar, so daß man dafür eventuell einfachere Beweisverfahren heranziehen kann.

Bei den modallogischen Beweisen unter Einbeziehung von Fairness (ab Lemma 7) zeigt sich, daß ein zielgerichtetes Vorgehen (insbesondere in der Verwendung der Fairnessregeln) absolut notwendig ist.

Abschließend hoffe ich, daß sich so wenig Fehler wie möglich eingeschlichen haben.

Literatur

[Gu88] Y. Gurevich: *Logic and the Challenge of Computer Science.* Trends in Theoretical Computer Science (E. Börger, ed.), Computer Science Press, 1988, S. 1-57.

[Gu91] Y. Gurevich: *Evolving Algebras. A Tutorial Introduction.* EATCS Bull. Feb. 1991.

[Gu92] Y. Gurevich: *Evolving Algebras: An Attempt to Discover Semantics.* Current Trends in Theoretical Computer Science, World Scientific, 1993, S. 266-292.

[Hu94a] J. K. Huggins: *An Evolving Algebra Interpreter.* Tech. Rept., Univ. of Michigan, Ann Arbor.

[Hu94b] J. K. Huggins: *Kermit: Specification and Verification.* Tech. Rept., Univ. of Michigan, Ann Arbor.

[May95] W. May: *Protokollverifikation in Temporallogik: Evolving Algebras und ein Tableaukalkül.* Diplomarbeit, ILKD, Universität Karlsruhe, 1995.