TLDA und Petrinetze[1]

Lars Kuhtz

20. Juli 2004

[1]Bei der Vorliegenden Arbeit handelt es sich um meine Studienarbeit im Rahmen des Diplomstudiengangs Informatik an der Humboldt Universität zu Berlin. Betreut wurde die Arbeit durch A. Alexander, wissenschaftliche Mitarbeiterin am Lehrstuhl für Theorie der Programmierung.

Inhaltsverzeichnis

1 Einleitung

Petrinetze sind ein verbreiteter graphbasierter Formalismus zur Beschreibung verteilter Systeme. Im Zusammenhang hiermit hat sich besonders die Semantik der verteilten Abläufe als nützlich erwiesen. Die noch im entstehen begriffene *Temporal Logic of Distributed Actions (TLDA)* stellt einen Formalismus dar, mit logischen Mitteln über verteilte Abläufe zu reden. Die jeweiligen Modellmengen ähneln sich dabei in der zugrundeliegenden Anschauung, wenngleich die mathematische Beschreibung deutlich verschieden ist. Diese Arbeit formuliert eine semantische Äquivalenz zwischen beiden Formalismen, und gibt eine Bildungsvorschrift an, mittels der zu einem Petrinetz eine semantisch äquivalente TLDA-Formel konstruiert werden kann. Der Äquivalenzbegriff ist dabei so stark wie möglich formuliert, so dass man sagen kann, dass die konstruierte Formel "exakt" die gleichen Abläufe wie das zugrundeliegende Petrinetz beschreibt.

Die Frage nach dem Sinn dieser Arbeit stellte sich mir zunächst nicht. Die Motivation zur Beschäftigung mit der Materie bestand darin, die Ausdruckmittel von TLDA im Umgang mit dem Formalismus und in Gegenüberstellung zu Petrinetzen besser kennenzulernen. Insbesondere der umfangreiche Beweis der Korrektheit der Bildungsvorschrift für die TLDA-Formel zu einem Petrinetz ist sehr technisch, bietet keinerlei Überraschungen und ist sicherlich in erster Linie eine Übung im Aufschreiben von Beweisen. Der Leser möge dies bedenken, bevor er sich entschließt, diesen Teil der Arbeit zu lesen.

Ein paar interessante Aspekte von TLDA und dem Verhältnis von TLDA zu Petrinetzen finden sich dann doch in dieser Arbeit.

Da ist zunächst das Prädikat *closed* und seine Problematik. Hierbei geht es im wesentlichen darum, inwieweit mittels TLDA ausgedrückt werden kann, dass eine Transition in einem verteilten Ablauf "isoliert" vorkommt.

Ein weiterer Aspekt ist die Problematik der Unterscheidung nicht einfacher (s. Definition 23) Petrinetze mittels TLDA. Hierbei ist wesentlich, dass in TLDA eine Transition nur mittels ihres Effektes auf Variablen identifiziert werden kann, während Petrinetze Transitionen über ihren Effekt auf die Menge der Plätze hinaus unterscheiden.

Schließlich beschäftigt sich auch das Kapitel über Invarianten in TLDA mit einem wichtigen bisher noch nicht ausgearbeiteten Aspekt dieser noch im Entstehen begriffenen Logik.

Im Anschluß an diese Arbeit stellen sich einige Fragen, die hier nicht behandelt werden: Diese Arbeit betrachtet nur 1-sichere Low-Level-Netze. Kann der Ansatz dieser Arbeit auch auf High-Level-Netze erweitert werden? Hier wäre zunächst die Klasse der algebraischen Netze aus [WWV+97] interessant. Dabei wäre entscheidend, nicht 1-sichere Netze handhaben zu können. Grundsätzlich scheint mir dies kein Problem zu sein. Weiterhin wäre es ggf. interessant zu untersuchen, wie sich bestimmte aus der Welt der Petrinetze bekannte Eigenschaften und Argumente (Platz-Invarianten, Leads-to-Eigenschaften, Causes-Eigenschaften, etc.) auf der Ebene der TLDA-Formeln darstellen. Ob dies tatsächlich zu neuen Einsichten führte, sei dahingestellt.

Mein herzlicher Dank gilt Adrianna Alexander für die Betreuung dieser Arbeit.

2 Schreibweisen

In dieser Arbeit werden folgende Konventionen verwendet:

- Sei R Relation. Für $(a, b) \in R$ schreibe ich auch aRb.
- Sei $R \subseteq M \times N$ eine Relation, $a \in M$ und $A \subseteq M$. $R(a) = \{b \in N \mid aRb\}$ und $R(A) = \bigcup_{a \in A} \{b \in N \mid aRb\}$.
- Sei R Relation. $aR^{-1}b \Leftrightarrow bRa$.
- In der Arbeit werden an Stelle der Terme *true* und $false$ oft sematisch äquivalente Terme (Aussagen) geschrieben.
- Die Menge der natürlichen Zahlen ($\mathbb{N}$) schließt die Null mit ein.
- Sei S eine Menge, dann bezeichnet S^+ die Menge aller nicht-leeren endlichen Sequenzen und S^ω die Menge aller nicht-leeren unendlichen Sequenzen. Weiterhin sei $S^\infty \triangleq S^\omega \cup S^+$.
- Die Funktion $l\colon S^+ \to \mathbb{N}$ weist einer endlichen Sequenz von Elementen aus S die Länge der Sequenz zu.
- Für eine Sequenz $\sigma\colon N \to S$, $N \subseteq \mathbb{N}$ über Symbolen aus S und $x \in \mathbb{N}$ bezeichnet $\sigma_{/x\to}$ die Sequenz mit $\sigma_{/x\to}(i) = \sigma(i + x)$.
- Beweisregeln werden wie folgt dargestellt:

  $$\frac{\text{Prämisse}}{\text{Konklusion}}$$

  und sind wie folgt zu lesen: Wenn die Prämisse eine gültige (im Sinne von Allgemeingültigkeit) Formel ist, so ist die Konklusion eine gültige Formel.
- $\wp(M)$ bezeichnet die Potenzmenge von M.

3 Die Logik TLDA

In diesem Kapitel werde ich eine kurze formale Beschreibung der Logik TLDA nach [Ale02] geben. Eine ausführliche Darstellung der Logik kann ebendort gefunden werden.

In dieser Arbeit werden TLDA-Formeln über dem Aussagenkalkül gebildet, d.h. Variablen werden als Aussagen verstanden und Ausdrücke werden somit über der Domain $\{true, false\}$ interpretiert. Aus diesem Grund werde ich eine auf diesen Spezialfall eingeschränkte Syntax und Sematik für TLDA angeben.

3.1 Modellmenge

Sei $Val = \{true, false\}$ und Var eine endliche oder unendliche Variablenmenge.

Definition 1 (History). Eine Abbildung $H : Var \to Val^{\infty}$ heißt *History*.

Für $x \in Var$ wird $H(x)$ als *History von* x bezeichnet. Für $H(x)$ wird auch H_x geschrieben. $H_x(i)$ bezeichnet dann das *i-te Element in der History von* x.

Oft wird nur ein kleiner Teil der (möglicherweise unendlich großen) Menge Var betrachtet. Implizit wird somit die Klasse aller Histories bezeichnet, die auf der Teilmenge der betrachteten Variablen gleich sind.

Definition 2 (Transition). Eine *Transition* ist eine Abbildung $t : V \to \mathbb{N}$, wobei $\emptyset \neq V \subseteq Var$.

$\mathcal{T}$ bezeichnet die Menge aller Transitionen.

Definition 3 (Involvierte Variablen). Zu einer Transition $t : V \to \mathbb{N}$ ist $\mathrm{Inv}(t) \triangleq V$ die Menge der *in t involvierten Variablen*.

Definition 4 (Vorgänger Relation). Die *direkter Vorgänger Relation* $\prec\cdot \subseteq \mathcal{T} \times \mathcal{T}$ is definiert durch

$$t \prec\cdot u \; gdw. \; \exists x \in \mathrm{Inv}(t) \cap \mathrm{Inv}(u) : \; t(x) = u(x) - 1.$$

$\prec$ bezeichnet die transitive Hülle, und $\preccurlyeq$ die reflexive transitive Hülle von $\prec\cdot$.

Definition 5 (Run). Sei H eine History und $T \subseteq \mathcal{T}$ eine Menge von Transitionen. $\mathcal{R} = (H, T)$ ist einen *Run* genau dann, wenn

1. für jede Variable $x \in Var$ und für alle i, $0 \leq i < l(H_x) - 1$ genau eine Transition $t \in T$ existiert mit $t(x) = i$;
2. für alle $t \in T$ und für alle $x \in \mathrm{Inv}(t)$ gilt: $0 \leq t(x) < l(H_x) - 1$;
3. $\prec_{|T \times T}$ irreflexive ist.

Definition 6 (Nebenläufige Transitionen). Sei $\mathcal{R} = (H, T)$ ein Run. Zwei Transitionen $t, u \in T, \; t \neq u$ heißen *nebenläufig* in $\mathcal{R}$ genau dann, wenn $\neg(t \prec u) \wedge \neg(u \prec t)$.

Definition 7 (Cut). Sei $\mathcal{R} = (H, T)$ ein Run. $C : Var \to \mathbb{N}$ ist ein *Cut* in $\mathcal{R}$ genau dann , wenn

$$\forall t \in T, \forall x, y \in \mathrm{Inv}(t) : \; t(x) < C(x) \Rightarrow t(y) < C(y).$$

$C_0 : Var \to \{0\}$ ist nach Definition ein Cut in $\mathcal{R}$ und wird *Anfangscut* genannt.

Definition 8 (Stattfinden einer Transition). Sei $\mathcal{R} = (H, T)$ ein Run und C ein Cut in $\mathcal{R}$. Eine Transition $t \in T$ *findet in* C *statt* (oder ist *aktiviert in* C) genau dann wenn, für alle $x \in \text{Inv}(t)$ gilt $t(x) = C(x)$

T_C ist die Menge aller Transitionen, die in C stattfinden können.

Definition 9 (Folgecut). Sei $\mathcal{R} = (H, T)$ ein Run, C ein Cut in $\mathcal{R}$ und $U \subseteq T_C$. $C'_U : Var \to \mathbb{N}$ ist definiert als:
$\forall x \in Var$:

$$C_U(x) \triangleq \begin{cases} C(x) + 1, & \text{wenn } \exists\, t \in U : x \in \text{Inv}(t) \\ C(x), & \text{sonst} \end{cases}$$

Man kann zeigen, dass C'_U ebenfalls ein Cut ist. Der Cut C'_U wird *U-Nachfolger von C* genannt.

Mit C' wird der T_C-Nachfolger von C bezeichnet.

Definition 10 (Schritt). Sei $\mathcal{R} = (H, T)$ ein Run und C ein Cut in $\mathcal{R}$. I_C ist definiert als die Menge $\{\text{Inv}(t) \mid t \in T_C\}$. $S = (C, C', I_C)$ ist ein *Schritt* in $\mathcal{R}$.

$S_0 = (C_0, C'_0, I_{C_0})$ heißt der *Anfangsschritt* von $\mathcal{R}$.

Definition 11 (Suffix eines Runs). Sei $\mathcal{R} = (H, T)$ ein Run und C ein Cut in $\mathcal{R}$. Ein *C-Suffix* $\widehat{\mathcal{R}} = (\widehat{H}, \widehat{T})$ von $\mathcal{R}$ ist definiert als

1. $\widehat{H}$ ist eine History und $\forall x \in Var : \widehat{H_x} \triangleq H_{x/C(x)\rightarrow}$
2. $\widehat{T}$ ist eine Menge von Transitionen mit $\widehat{T} \triangleq \{\widehat{t} \mid \emptyset\widehat{t}(v) = t(v) - C(x),\ t \in T,\ \forall x \in \text{Inv}(t) : t(x) \geq C(x)\}$.

Man sieht leicht, dass $\widehat{\mathcal{R}}$ ein Run ist.

Für zwei TLDA Runs $\mathcal{R}$ und $\mathcal{S}$ bezeichnet $\mathcal{R}\,\text{suff}\,\mathcal{S}$, dass $\mathcal{R}$ ein Suffix von $\mathcal{S}$ ist.

Definition 12 (t-Suffix eines Runs). Sei $\mathcal{R}$ ein Run und $t \in T_{\mathcal{R}}$ eine Transition. Ein Run $\mathcal{R}_t$ ist ein t-Suffix von $\mathcal{R}$, wenn ein Cut C existiert, so dass $\mathcal{R}_t$ ein C-Suffix von $\mathcal{R}$ ist und t in C stattfinden kann.

3.2 Syntax

Sei wiederum Var die Menge der Variablen. Seien ferner $Var' = \{x' \mid x \in Var\}$ und $\widetilde{Var} = \{\widetilde{a} \mid a \subseteq Var\}$ zwei weitere Variablenmengen. Die Logik hat also drei Sorten von Variablen, ist also getypt.

Ein *Zustandprädikat* ist eine Formel des Kalküls der Aussagenlogik, die nur Variablen aus Var enthält. Eine *Aktion* ist eine Formel des aussagenlogischen Kalküls, die sowohl Variablen aus Var, wie auch aus Var' und $\widetilde{Var}$ enthalten kann.

Eine *TLDA-Formel* ist

- enweder ein Zustandsprädikat
- oder eine Aktion.

Seien F und G TLDA-Formeln. Dann sind

- $F \wedge G$,
- $\neg F$
- $\Box F$
- und sonst nichts

TLDA-Formeln.

Weiterhin ist die Formel $\Diamond F$ eine Kurzschreibweise für $\neg\Box\neg F$.

3.3 Semantik

Eine Interpretation über $Val = \{true, false\}$ weist jedem Symbol aus Var, Var' und $\widetilde{Var}$ ein Element aus Val zu. D.h. im vorliegenden Spezialfall der Beschränkung der TLDA zugrunde liegenden Logik auf das Aussagenkalkül, haben alle drei Variablensorten den gleichen Typ.

Definition 13 (Gültigkeit einer Aktion in einem Schritt). Zu einem Schritt $S = (C, C', I_C)$, ist die Belegung β_S der Variablen wie folgt definiert.

$$\beta_S \colon Var \cup Var' \cup \widetilde{Var} \to Val$$

$$\beta_S(x) = \begin{cases} H_x(C(x)) & \text{, falls } x \in Var \\ H_x(C(x)+1) & \text{, falls } x \in Var' \\ true & \text{, falls } x \in \widetilde{Var} \text{ und ein } y \in I_C \text{ existiert, so dass } x \subseteq y \\ false & \text{, sonst} \end{cases}$$

Eine Aktion A gilt in einem Schritt S ($S \models A$) genau dann, wenn der aussagenlogische Ausdruck A unter der Belegung β_S erfüllt ist.

Da ich es später benötige definiere ich noch zu einem Cut C eine Belegung $\beta_C \colon Var \to Val$ mit $\beta_C(v) = H_v(C(v))$

Definition 14 (Gültigkeit einer Formel in einem Run). Sei $\mathcal{R} = (H, T)$ ein Run. Für eine Aktion A gilt:

$\mathcal{R} \models A$ genau dann, wenn $(C_0, C_0', I_{C_0}) \models A$.

Seien F und G TLDA-Formeln. Dann gilt:

- $\mathcal{R} \models F \wedge G$ genau dann, wenn $\mathcal{R} \models F$ und $\mathcal{R} \models G$
- $\mathcal{R} \models \neg F$ genau dann, wenn nicht $\mathcal{R} \models F$
- $\mathcal{R} \models \Box F$ genau dann, wenn $\widehat{\mathcal{R}} \models F$ für jedes Suffix $\widehat{\mathcal{R}}$ von $\mathcal{R}$.

Damit ist die Semantik vollständig beschrieben. Es ist bisweilen hilfreich, die Gültigkeit eines Zustandsprädikates in einem Cut zu betrachten. Daher gebe ich noch die folgende Definition an, die, wie man leicht sieht, mit den vorhergehenden Definitionen konsistent ist.

Definition 15 (Gültigkeit eines Zustandsprädikates in einem Cut). Sei F ein Zustandsprädikat und C ein Cut. $C \models F$ genau dann, wenn der aussagenlogische Ausdruck F unter der Belegung β_C erfüllt ist.

3.4 Spezielle Prädikate: *Enabled* und *progress*

Definition 16 (Variablen einer TLDA-Formel). Sei ϕ eine TLDA-Formel. $V(\phi) \subseteq Var$ ist definiert als die Menge aller Variablen, die in ϕ (einfach, gestrichen oder geschlängelt) vorkommen.

Es wäre möglich, das Prädikat *Enabled* mit den Mitteln von TLDA rein syntaktisch zu definieren. Der Einfachheit halber verzichte ich aber darauf und gebe eine sematische Definition dieses Prädikats an.

Definition 17 (*Enabled*-Prädikat). Sei A eine Aktion und $\mathcal{R}$ ein Run. $\mathcal{R} \models Enabled(A)$ genau dann, wenn ein Cut C (unabhängig von $\mathcal{R}$) existiert, so dass $(C_0, C, I_{C_0}) \models A$.

Definition 18 (*progress*-Prädikat). Sei A eine Aktion und $M \subseteq V(A)$. Die Formel $negP_M(A)$ ist wie folgt definiert:

$$negP_M(A) \triangleq \Diamond\Box(\bigwedge_{x \in M} \neg\widetilde{x} \wedge Enabled(A \wedge \bigwedge_{x \in V(A)\setminus M} \neg\widetilde{x}))$$

Das Prädikat $progress_M(A)$ ist nun wie folgt definiert:

$$progress_M(A) \triangleq \neg negP_M(A)$$

Ein Run $\mathcal{R}$ respektiert den Progress einer Aktion A genau dann, wenn $\mathcal{R} \models progress_{V(A)}(A)$.

3.5 Induktive Invarianten in TLDA

Ein Cut repräsentiert einen lokalen Zustand eines Systems. Insofern ist es im Allgeimeinen wünschenswert, Aussagen über alle Cuts aller Runs einer Formel machen zu können. Eine solche Aussage ist eine Invariante bzgl. des $\Box$-Operators. Es wäre also eine entsprechende Beweisregel wünschenswert, um Invarianten bzgl. des $\Box$-Operators zeigen zu können. Für die mit TLDA verwandte Logik TLA gilt eine entsprechende Beweisregel (siehe [ALM96]), der in der Verifikation von Systemen mittels TLA eine entscheidende Bedeutung zukommt:

$$\frac{P \wedge [N]_v \rightarrow P'}{P \wedge \Box[N]_v \rightarrow \Box P}\text{, wobei } P \text{ Zustandsprädikat und } N \text{ Aktion ist.}$$

Eine entsprechende Beweisregel für TLDA sollte folgende Form haben:

$$\frac{P \wedge A \rightarrow P'}{P \wedge \Box A \rightarrow \Box P}\text{, wobei } P \text{ Zustandsprädikat und } A \text{ Aktion ist.}$$

Da die Menge aller Cuts eines Runs abzählbar und halbgeordnet ist, liegt es nahe, eine Induktion über alle Cuts aller gültigen Runs zu führen, um die Gültigkeit einer Invariante zu zeigen. Um eine Induktion über alle Cuts zu führen, muß man die betreffende Eigenschaft tatsächlich für alle Y-Nachfolger für $Y \subseteq T_C$ eines Cuts C zeigen. TLDA kann aber nur über Schritte, d.h. über T_C-Nachfolger reden. Zeigt

man die Eigenschaft für den Anfagscut und für jeden von Anfangscut aus durch Schritte erreichbaren Cut, so hat man die Eigenschaft also nicht unbedingt für alle Cuts gezeigt. Wie kann nun ein Induktionsprinzip aussehen, mit dem man Aussagen über alle Cuts zeigen kann?

Zunächst könnte man fragen, ob der Ansatz, die Eigenschaft für den Anfangscut und alle Schritte zu zeigen, vielleicht aufgrund der Struktur von TLDA ausreichend ist. Dem ist nicht so, wie ein einfaches Beispiel zeigt:

Beispiel. Sei $A \triangleq \Box((a' \leftrightarrow \neg a) \wedge (b' \leftrightarrow \neg b))$ und $P \triangleq a \leftrightarrow b$. Dann gilt:

$$(P \wedge A) \rightarrow (a' \leftrightarrow b')$$

Aber es gilt nicht:

$$(P \wedge \Box A) \rightarrow \Box P$$

Obige Invariantenregel für TLDA ist im Allgeimeinen also falsch.

Weiterhin könnte man fragen, ob es möglich ist, den Induktionsanfang so zu modifizieren, dass ein Induktionsschritt über alle Schritte die Vollständigkeit der Induktion gewährleistet. Die Menge der Cuts, für die die Eigenschaft im Induktionsanfang gezeigt werden müßte, wäre dann allerdings ggf. nicht endlich. Somit ist dieser Ansatz nicht praktikabel.

Schließlich könnte man fragen, ob man für Formeln und/ oder Eigenschaften einer bestimmten syntaktischen Struktur ein entsprechendes einfaches Induktionsprinzip angegeben kann.

Dieser Ansatz scheint vielversprechend und führt mich zu folgender Vermutung:

Vermutung 1 (Invariantenregel für TLDA). *Sei P ein Zustandsprädikat und A eine umgebungsinvariante TLDA-Formel. Dann gilt:*

$$\frac{P \wedge A \rightarrow P'}{P \wedge \Box A \rightarrow \Box P}$$

Nun ist noch zu definieren, wann eine TLDA-Formel Umgebungsinvariant ist. Weiterhin ist ein syntaktisches Kriterium für Umgebungsinvarianz anzugeben:

Bei der Definition der umgebungsvarianz verwende ich den Vorschlag von Adrianna Alexander:

Definition 19 (Restriktion eines Runs). Sei $\mathcal{R} = (H_{\mathcal{R}}, T_{\mathcal{R}})$ ein Run und $V \subseteq Var$. Die *Restriktion von $\mathcal{R}$ auf V (kurz: $\mathcal{R}|_V$)* ist definiert als der Run (H, T) mit $H = H_{\mathcal{R}}|_V$ und $T = T_{\mathcal{R}}|_V$.

Definition 20 (Umgebungsinvarianz). Eine TLDA-Formel ϕ heißt *umgebungsinvariant* genau dann, wenn für jeden Run $\mathcal{R}$ mit $\mathcal{R} \models \phi$ gilt: Für alle Runs $\mathcal{S}$ gilt: wenn $\mathcal{R}|_{V(\phi)} = \mathcal{S}|_{V(\phi)}$, dann gilt $\mathcal{S} \models \phi$.

Vermutung 2 (Syntaktisches Kriterium für Umgebungsinvarianz). *Sei ϕ eine TLDA-Formel die nach folgendem Schema gebildet ist, oder die sematisch äquivalent ist zu einer Formel, die folgendes Schema erfüllt:*

$$\phi_{init} \wedge \bigwedge_{A \in V} \Box(\widetilde{A} \rightarrow \phi_A) \wedge \phi_{prog},$$

wobei

- ϕ_{init} *ein Zustandsprädikat ist,*
- $V \subseteq \wp(Var)$*,*
- *für alle in* ϕ_A *vorkommenden gestrichenen Variablen* v' *gilt:* $v \in A$*,*
- *für alle in* ϕ_A *enthaltenen geschlängelten Variablen* $\widetilde{B} \subseteq \widetilde{Var}$ *gilt:* $A \cap B \neq \emptyset$*.*

Aus Vermutung 1 kann ich nun folgende Proposition ableiten, die ich später verwenden werde:

Proposition 1 (Induktionsprinzip in TLDA für Zustandsprädikate). *Sei* $\phi \triangleq \phi_{init} \wedge \Box(\phi_{schritt})$ *eine umgebungsinvariante TLDA-Formel, wobei* ϕ_{init} *ein Zustandsprädikat und* $\phi_{schritt}$ *eine Aktion ist. Sei* $\alpha_{x_1,\ldots,x_m}$ *ein Prädikat über* $\{x_1, \ldots, x_m\} \subseteq Var$*.*
Wenn

(i) für alle Cuts C *mit* $C \models \phi_{init}$ *gilt:* $\beta_C \models \alpha_{x_1,\ldots,x_m}$*,*

(ii) für alle Schritte $S = (C, C', I_C)$ *gilt:* $\beta_C \models \alpha_{x_1,\ldots,x_m}$ *und* $S \models \phi_{schritt}$ *impliziert* $\beta_{C'} \models \alpha_{x_1,\ldots,x_m}$*,*

dann gilt $\alpha_{x_1,\ldots,x_m}$ *in jedem Cut eines Runs von* ϕ*.*

4 Netze und verteilte Abläufe

In diesem Abschnitt werde ich die Klasse von Petrinetzen formalisieren, die ich im Folgenden zugrunde lege. Wenn ich von *Netzen* spreche, beziehe ich mich auf diese Klasse. Dabei handelt es sich im wesentlichen um die Klasse der *es-Netze* aus [Rei98]. Allerdings betrachte ich in dieser Arbeit keine Fairness. Wie in [Rei98] betrachte ich nur 1-sichere Netze. Während in [Rei98] diese Eigenschaft durch eine entsprechende Schaltbedingung für Transitionen garantiert wird, fordere ich sie als Invariante, da Kausalitätsbeziehungen zwischen Transitionen aufgrund von Kontakt und Konflikten im Nachbereich nicht mittels des hier verwendeten Begriffs von verteilten Abläufen darstellbar sind. Das Beispiel eines nicht 1-sicheren Netzes in Abbildung 1 verdeutlicht dies: Angenommen, die 1-Sicherheit würde durch eine entsprechende Schaltbedingung gewährleistet. Dann ist die Transition a im Anfangszustand nicht aktiviert, da die Marke auf Platz B ein Schalten der Transition a verhindert. Das Schalten von Transition b ist also eine Voraussetzung für die Aktivierung von a. Diese kausale Abhängigkeit zwischen a und b kann jedoch nicht mittels verteilter Abläufe gemäß Definition 30 und 31 beschrieben werden. Der Grund dafür besteht darin, dass in verteilten Abläufen die Voraussetzungen für die Aktivierung einer Transition nur in Form von Marken im Vorbereich der Transition dargestellt werden. Eine Enabeling-Bedingung, die über Marken (bzw. nicht vorhandene Marken) im Nachbereich redet, kann also nicht modelliert werden.

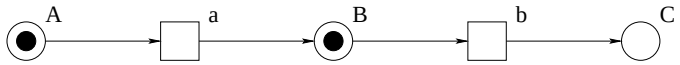

Abbildung 1: Ein nicht 1-sicheres Netz.

Definition 21 ((Anfangsmarkiertes) Petrinetz). Ein *Petrinetz* ist ein 3-Tupel $N = (P, T, F)$, wobei

- P mit $P \cap T = \emptyset$
- $F \subseteq (P \times T) \cup (T \times P)$

Die Elemente von P werden *Plätze*, die Elemnte von T *Transitionen* und die Elemente von F werden *Bögen* genannt.

Die transitive Hülle von F wird mit $<_N$ bezeichnet. (Soweit N durch den Kontext eindeutig bestimmt ist, schreibe ich auch $<$ anstatt $<_N$.)

Eine Menge $M \subseteq P$ heißt *Markierung* oder *Zustand* von N.

Ein *anfangsmarkiertes Petrinetz* ist ein 4-Tupel $N = (P, T, F, I)$, wobei (P, T, F) ein Petrinetz ist und $I \subseteq P$. I heißt *Anfangsmarkierung* von N.

Sei N ein (anfangsmarkiertes) Petrinetz. Soweit nicht anderes angegeben, gilt $N = (P_N, T_N, F_N)$ $(N = (P_N, T_N, F_N, I_N))$.

Definition 22 (Vor- / Nachbereich einer Tranisition). Sei N ein Petrinetz und $a \in P_N \cup T_N$. Der *Vorbereich von a* (${}^\bullet a$) ist definiert durch ${}^\bullet a = \{b \in P_N \cup T_N \mid bF_N a\}$. Der *Nachbereich von a* ($a^\bullet$) ist definiert durch $a^\bullet = \{b \in P_N \cup T_N \mid aF_N b\}$. Weiterhin sei ${}^\bullet a^\bullet = {}^\bullet a \cup a^\bullet$.

Definition 23 (Einfaches Petrinetz). Ein Petrinetz N heißt *einfach* genau dann, wenn für alle Transitionen $s, t \in T_N$ gilt: ${}^\bullet s = {}^\bullet t \wedge s^\bullet = t^\bullet \Rightarrow s = t$.

Definition 24 (Platzberandetes Petrinetz). Ein Petrinetz N heißt *platzberandet* genau dann, wenn für alle Transitionen $t \in T_N$ gilt: ${}^\bullet t \neq \emptyset \wedge t^\bullet \neq \emptyset$.

Die folgende Definition des Effektes einer Transition eines Petrinetzes unterscheidet sich von den sonst üblichen Definitionen des Effektes einer Transition. Dies hat technische Gründe.

Definition 25 (Effekt einer Transition eines Petrinetzes). Sei N ein Petrinetz. Der *Effekt einer Transition* $t \in T_N$ auf einen Platz $p \in {}^\bullet t^\bullet$ ist definiert als

$$\text{eff}_N : T_N \times P_N \to \{true, false\} \times \{true, false\}$$
$$\text{eff}_N(t,p) = \begin{cases} (p \in {}^\bullet t, p \in t^\bullet), \text{ für } p \in {}^\bullet t^\bullet \\ \text{nicht definiert}, \quad \text{sonst} \end{cases}$$

Der Effekt einer Transition $t \in T_N$ ist ein ${}^\bullet t^\bullet$ indizierter Vektor, der jedem Platz $p \in {}^\bullet t^\bullet$ den Effekt von t auf p zuordnet:

$$\text{eff}_N(t) = (\text{eff}(t,p))_{p \in {}^\bullet t^\bullet}$$

Definition 26 (Schritt). Sei N ein Petrinetz, und seien M, M' Markierungen von N. Eine Transition $t \in T_N$ ist *aktiviert* in M, wenn ${}^\bullet t \subseteq M$.

Das Tripel $S = (M, M', t)$ ist ein *Schritt*, wenn t in M aktiviert ist, und $M' = (M \setminus {}^\bullet t) \cup t^\bullet$.

Definition 27 (Erreichbarkeit). Sei N ein anfangsmarkiertes Petrinetz. Eine Markierung M von N heißt *erreichbar* in N genau dann, wenn Folgen $t_1, \ldots, t_n$ und $M_0, \ldots M_n$ mit $t_i \in T_N$ und $M_0, M_i \subseteq P_N$ für $1 \leq i \leq n$ exitieren, so dass (M_{i-1}, M_i, t_i) für $1 \leq i \leq n$ ein Schritt ist und $M_0 = I_N$ und $M_n = M$.

Definition 28 (1-Sicherheit). Eine anfangsmarkiertes Petrinetz N ist *1-sicher* genau dann, wenn für jede ereichbare Markierung M und jede Transition $t \in N_T$ gilt:

$${}^\bullet t \subseteq M \quad \Rightarrow \quad (t^\bullet \setminus {}^\bullet t) \cap M = \emptyset$$

Mit Hilfe dieser Definitionen kann ich nun die Klasse von Netzen definieren, auf die ich mich fortan beziehen werde:

Definition 29 (Netz). Ein *Netz* ist ein 5-Tupel $\Sigma = (P, T, F, I, Pr)$, wobei (P, T, F, I) ein platzberandetes, 1-sicheres, anfangsmarkiertes Petrinetz ist und $Pr \subseteq T$. Pr heißt *Progressprädikat*.

Sei Σ ein (anfangsmarkiertes) Petrinetz. Soweit nicht anders angegeben, gilt $\Sigma = (P_\Sigma, T_\Sigma, F_\Sigma, I_\Sigma, Pr_\Sigma)$. Soweit im jeweiligen Kontext Σ eindeutig bestimmt ist, gilt: $\Sigma = (P, T, F, I, Pr)$.

Definition 30 (Verteilter Ablauf). Ein *verteilter Ablauf* $\mathcal{C} = (P_\mathcal{C}, T_\mathcal{C}, F_\mathcal{C})$ ist ein Petrinetz mit:

(i) Für alle $p \in P_\mathcal{C}$ gilt $|{}^\bullet p| \leq 1$ und $|p^\bullet| \leq 1$.

(ii) Für alle $t \in T_\mathcal{C}$ gilt $|{}^\bullet t| \geq 1$ und $|t^\bullet| \geq 1$.

(iii) $<_\mathcal{C}$ ist irreflexiv.

(iv) Für alle $a \in P_\mathcal{C} \cup T_\mathcal{C}$ ist $\{b \mid b <_\mathcal{C} a\}$ endlich.

Zwei Elemente $a, b \in P_\mathcal{C} \cup T_\mathcal{C}$, $a \neq b$ heißen *nebenläufig* ($a \operatorname{co} b$) genau dann, wenn weder $a < b$ noch $b < a$.

Es gilt ${}^\circ\mathcal{C} = \{a \in P_\mathcal{C} \mid {}^\bullet a = \emptyset\}$ und $\mathcal{C}^\circ = \{a \in P_\mathcal{C} \mid a^\bullet = \emptyset\}$.

Sei $\mathcal{C}$ ein verteilter Ablauf. Soweit nicht anderes angegeben, gilt $\mathcal{C} = (P_\mathcal{C}, T_\mathcal{C}, F_\mathcal{C})$.

Definition 31 (Verteilter Ablauf eines Netzes). Sei Σ ein Netz. Ein verteilter Ablauf $\mathcal{C}$ zusammen mit einem Labeling $l\colon P_\mathcal{C} \cup T_\mathcal{C} \to P_\Sigma \cup T_\Sigma$ ist ein *Modell von* Σ (oder auch einfach: *verteilter Ablauf von* Σ) genau dann, wenn

(i) für alle $a, b \in P_\mathcal{C} \cup T_\mathcal{C}$ gilt: $a \operatorname{co} b \Rightarrow l(a) \neq l(b)$,

(ii) für alle $t \in T_\mathcal{C}$ gilt: $l(t) \in T_\Sigma$ und $l({}^\bullet t) = {}^\bullet l(t)$ und $l(t^\bullet) = l(t)^\bullet$,

(iii) $l({}^\circ\mathcal{C}) = I_\Sigma$ und

(iv) für alle $t \in Pr_\Sigma$ gilt: $l(\mathcal{C}^\circ)$ aktiviert nicht t (Man sagt: $\mathcal{C}$ *respektiert Progress von* t.)

Man schreibt: $\mathcal{C} \models_l \Sigma$, oder, wenn über l nichts weiter ausgesagt wird, einfach $\mathcal{C} \models \Sigma$.

Definition 32 (Effektes einer Transition bzgl. eines Labelings). Sei S eine Symbolmenge. Sei $\mathcal{C}$ ein verteilter Ablauf mit Labeling $l : \mathcal{C} \to \Sigma$ und $t \in T_\mathcal{C}$ eine Transition. Sei $s \in S$. Der *Effekt von* t *auf das Label* s ist definiert als

$$\operatorname{eff}^l_\mathcal{C}(t, s) = \begin{cases} (s \in l({}^\bullet t), s \in l(t^\bullet)) \text{ für } s \in l({}^\bullet t^\bullet) \\ \text{nicht definiert,} \quad \text{sonst} \end{cases}$$

Effekt von t bzgl. des Labels l ist definiert durch

$$\operatorname{eff}^l_\mathcal{C}(t) = (\operatorname{eff}^l_\mathcal{C}(t, \sigma))_{\sigma \in l({}^\bullet t^\bullet)},$$

5 Äquivalenz von Verteilten Abläufen von Netzen und TLDA-Runs

Im Folgenden rede ich von *Run*, wenn ich mich auf einen TLDA-Run beziehe und von *verteiltem Ablauf*, wenn ein verteilter Ablauf eines Netzes gemeint ist.

In diesem Kapitel definiere ich den für diese Arbeit zentralen Begriff der Äquivalenz zwischen einer TLDA-Formel und einem Netz. Ich definiere die Äquivalenz feinst möglich auf der Grundlage von Runs und verteilten Abläufen. Es handelt sich also um eine semantische Äquivalenz. Dabei sind eine Formel und ein Netz genau dann äquivalent, wenn sie "exakt" die gleichen Modelle haben. Zu klären ist, wie der Ausdruck "exakt" zu verstehen ist.

Im allgemeinen sind zwei Mengen gleich, wenn sie die gleichen Elemente enthalten. Da Runs und verteilte Abläufe von Netzen mittels verschiedener Formalismen beschrieben werden, wäre die Forderung einer (syntaktischen) Gleichheit der Elemente hier sinnlos. Vielmehr muß die Gleichheit hier durch eine möglichst feine Äquivalenz beschrieben werden. Ich definiere also zunächst, wann ein Run und ein verteilter Ablauf äquivalent sind.

Angelpunkt der Äquivalenz von Runs und verteilten Abläufen sind die Transitionen in beiden Modellen. Ich nenne einen Run und einen verteilten Ablauf äquivalent, wenn man einen Bijektion zwischen ihren Transitionen finden kann, so dass zum einen jeweils bzgl. ihres Effektes gleiche Transitionen aufeinander abgebildet werden (die Abbildung ist lokal konsistent) und zum anderen die Transtitionen in dem Run und dem verteilten Ablauf gleich angeordnet sind (die Abbildung ist global konsistent). Voraussetzung für die Betrachtung von Transitionen als elementare Einheiten des Vergleichs ist deren unmittelbare (syntaktische) Vergleichbarkeit. Dies geschieht mittels der Effekte der Transitionen. Voraussetzung hierfür ist wiederum die (ebenfalls syntaktische) Identifizierung von Variablen und Plätzen. Unmittelbare Folge des Vergleichs von Transitionen mittels ihrer Effekte ist, dass Transitionen (auf lokaler Ebene) ansonsten nicht weiter unterscheidbar sind, dass also insbesondere jegliche Labels von Transitionen keine Berücksichtigung finden. Die Konsequenzen hiervon im Bezug auf nicht einfache Netze werden weiter unten besprochen (siehe Kapitel 5.1).

Den Effekt einer Transition eines verteilten Ablaufs hatte ich bereits definiert. Im folgenden werde ich den Effekt einer Transition eines Runs so definieren, dass beide unmittelbar syntaktisch vergleichbar sind.

Definition 33 (Effekt einer Transition eines Runs). Sei $\mathcal{R} = (H_\mathcal{R}, T_\mathcal{R})$ ein Run. Der *Effekt einer Transition* $t \in T_\mathcal{R}$ auf eine Variable $x \in \mathrm{Inv}(t)$ ist definiert als

$$\mathrm{eff}_\mathcal{R} : T_\mathcal{R} \times Var \to Val \times Val$$
$$\mathrm{eff}_\mathcal{R}(t,x) = \begin{cases} (H_x(t(x)), H_x(t(x)+1)) & \text{, für } x \in \mathrm{Inv}(t) \\ \text{nicht definiert} & \text{, sonst} \end{cases}$$

Als Verallgemeinerung hiervon ist der Effekt einer Transition $t \in T_\mathcal{R}$ ein $\mathrm{Inv}(t)$-indizierter Vektor, der für jedes $x \in \mathrm{Inv}(t)$ den Effekt von t auf x beschreibt:

$$\mathrm{eff}_\mathcal{R}(t) = (\mathrm{eff}_\mathcal{R}(t,x))_{x \in \mathrm{Inv}(t)}$$

Abbildung 2 zeigt einen Run und die Effekte der Transitionen dieses Runs.

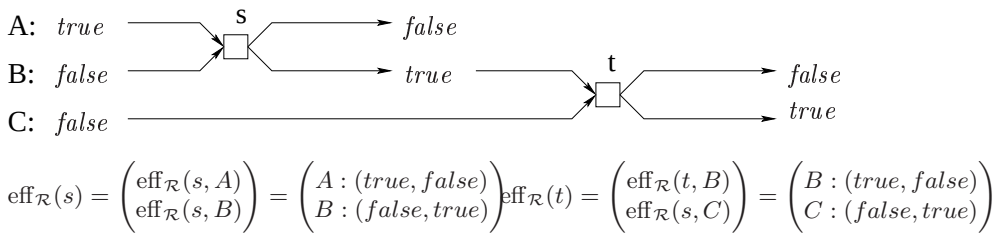

Abbildung 2: Ein Run und die Effekte der Transitionen.

Mittels des Begriffs des Effektes einer Transition formalisiere ich nun den Begriff der Äquivalenz von verteilten Abläufen und Runs wie oben beschrieben und leite daraus die Äquivalenz von TLDA-Formeln und Netzen ab. Dabei ist natürlich zu berücksichtigen, dass die Zuordnung von verteilten Abläufen zu Netzen mittels des zugehörigen Labels der Elemente des verteilten Ablaufs durch die Elemente des Netzes geschieht.

Definition 34 (Äquivalenz von verteilten Abläufen und Runs). Sei $\mathcal{C}$ ein verteilter Ablauf mit Labeling l. Sei $\mathcal{R} = (H_{\mathcal{R}}, T_{\mathcal{R}})$ ein Run. $\mathcal{C}$ und $\mathcal{R}$ sind *äquivalent bzgl. l ($\mathcal{C} \simeq_l \mathcal{R}$)* genau dann, wenn eine bijektive Abbildung $f : T_{\mathcal{R}} \to T_{\mathcal{C}}$ existiert mit:

(i) $\mathrm{eff}_{\mathcal{R}}(t) = \mathrm{eff}^l_{\mathcal{C}}(f(t))$, für alle $t \in T_{\mathcal{R}}$ (f ist lokal konsistent)

(ii) $s \prec t \Leftrightarrow f(s) <_{\mathcal{C}} f(t)$, für alle $s, t \in T_R$ (f ist global konsistent)

(iii) $^\circ\mathcal{C} = \{x \in Var \mid H_x(0)\}$

Als Beispiel zeigt Abbildung 3 einen äquivalenten verteilten Ablauf zu dem Run aus Abbildung 2.

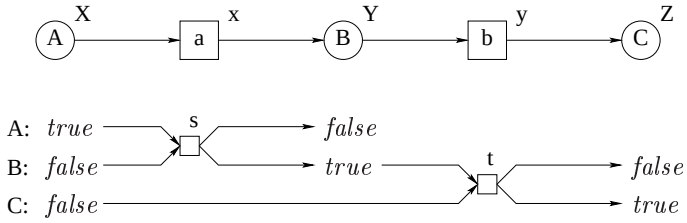

Abbildung 3: Ein gelabelter verteilter Ablauf und ein äquivalenter Run.

Schließlich kann ich nun definieren, wann ich ein Petrinetz und eine TLDA-Formel äquivalent nenne.

Definition 35 (Äquivalenz von Petrinetzen und TLDA-Formeln). Sei Σ ein Netz und Φ eine TLDA Formel über der Menge der boolschen Variablen P. Σ und Φ heißen äquivalent ($\Sigma \simeq \Phi$) genau dann, wenn zu jedem verteilten Ablauf $\mathcal{C}$ mit $\mathcal{C} \models_l \Sigma$ ein Run $\mathcal{R}$ mit $\mathcal{R} \models \Phi$ existiert, so dass $\mathcal{C} \simeq_l \mathcal{R}$, und zu jedem Run $\mathcal{R}$ mit $\mathcal{R} \models \Phi$ ein verteilter Ablauf $\mathcal{C}$ mit $\mathcal{C} \models_l \Sigma$ existiert, so dass $\mathcal{C} \simeq_l \mathcal{R}$.

Bei der vorstehenden Definition ist zu beachten, dass die Labels von $\mathcal{C}$ mit den Variablen*namen* aus $\mathcal{R}$ syntaktisch identisch sein müssen! Das heißt, dass auch die

Symbole von Σ und Φ identisch sind in dem Sinne, dass Variablen aus Φ mit Plätzen aus Σ identifiziert werden. Ggf. könnte eine schwächerere Äquivalenz formuliert werden, die Umbenennung erlaubt — dies ist aber von zweifelhaften Wert, da man genausogut Φ und Σ als kanonische Repräsentanten ihrer jeweiligen Klasse bzgl. Variabeln- bzw. Platzumbenennung betrachten könnte.

5.1 Exkurs: Äquivalenz von TLDA Formeln und *einfachen* Netzen

Die Menge der verteilten Abläufe eines Netzes bleibt beim Hinzufügen nicht einfacher Transitionen (bis auf Graphisomorphie) gleich. Jedoch betrachte ich als Modelle ausdrücklich *gelabelte* verteilte Abläufe. Da in Petrinetzen Transitionen benannt sind, ändert sich also beim Hinzufügen die Menge der gelabelten verteilten Abläufe. TLDA benennt Transitionen nicht. Daher wird für die Äquivalenz von TLDA-Formeln und Netzen eine direkte bijektive Entsprechnung nur zwischen Variablen und Platzlabels gefordert, während die Transitionsnamen keine Rolle spielen. So formuliert ist die Äquivalenz auch unter der Klasse nicht einfacher Netze stabil. Allerdings impliziert die Äquivalenz keine Bijektion zwischen den Runs der Formel und den verteilten Abläufen des Netzes, da die Injektivität von (unter Graphisomorphie gleichen) gelabelten Abläufen auf (unter Restriktion auf die relevanten Variablen gleichen) Runs nicht mehr gegeben ist.

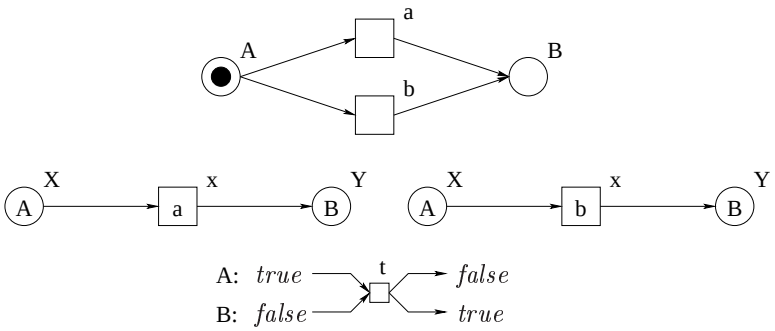

Abbildung 4: Ein nicht einfaches Netz mit zwei gelabelten verteilten Abläufen und einem äquivalenten TLDA Run

Zu jedem Run wird ein verteilter Ablauf (mit verschiedenen möglichen Labelings) konstruiert, und zu jedem gelabelten verteilten Ablauf kann genau ein Run gefunden werden. Die Abbildung von der Klasse der unter Graphisomorphie gleichen gelabelten verteilten Abläufe auf die Klasse der bis auf unrelevante Variablen gleichen Runs ist surrjektiv aber nicht injektiv. Es liegt nahe zu vermuten, dass, wenn man nur einfache Netze betrachtet, die Äquivalenz eine Bijektion zwischen den Modellmengen impliziert:

Vermutung 3. *Sei Σ ein einfaches Netz und Φ eine TLDA-Formel über der Menge der boolschen Variablen P_Σ. Wenn $\Sigma \simeq \Phi$, dann ist die Relation $\simeq \subseteq [\{\mathcal{C} \mid \mathcal{C} \models_l \Sigma\}]_{Graphisomorphie} \times \{\mathcal{R} \mid \mathcal{R} \models \Phi\}$ eine Bijektion.*

Beweisfragment zur Vermutung 3. Zeige, dass gilt: $\mathcal{C} \simeq_l \mathcal{Q} \wedge \mathcal{C} \simeq_l \mathcal{R} \Rightarrow \mathcal{Q} = \mathcal{R}$. Beachte, dass der einzige mögliche Unterschied, die Variablenmengen von $\mathcal{R}$ und $\mathcal{Q}$ sein können, das Labeling der Transitionen aber eindeutig ist. Diese ist aber gleich, da $\mathcal{Q} \models \Phi$ und $\mathcal{R} \models \Phi$ und Var in diesem Fall fest vorgegeben ist. □

Vielleicht wäre es jedoch wünschenwert, in der Frage der Φ zugrunde liegenden Variablenmenge etwas flexibler zu werden. Dazu könnten (wie oben bereits angedeutet) auf der Seite von $\mathcal{R}$ Klassen bzgl. Gleichheit auf Restriktion bzgl. relevanter Variablen betrachtet werden.

6 Die Formel Φ_Σ

6.1 Das Prädikat closed

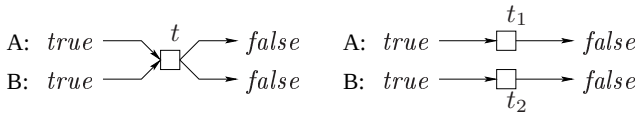

Abbildung 5: Zwei Runs, die sich durch die *Isoliertheit* der Transition voneinander Unterscheiden

Gegeben seien die Runs aus Abbildung 5. Es ist leicht zwei Netze zu konstruieren, die (bis auf Graphisomorphie) jeweils genau einen gelabelten verteilten Ablauf haben, der jeweils zu einem dieser Runs äquivalent ist. Eine äquivalente TLDA-Formel muß also jeweils genau diesen einen Run als Modell haben. Will man also zu dem jeweiligen Netz äquivalente Formelen angeben, so müssen diese Formeln zwischen den beiden Abläufen aus Abbildung 5 unterscheiden können. Insbesondere muß man also ausdrücken, dass eine Transitionen *isoliert* ist. Dazu bietet sich das Sprachmittel der Varialbenmenge $\widetilde{Var}$ an. So verlangt die Formel $\Box((\widetilde{A} \vee \widetilde{B}) \rightarrow \widetilde{AB})$, dass A und B unter allen Umständen gemeinsam von einer Transition aktualisiert werden. Ebenso verlangt die die Formel $\Box((\widetilde{A} \vee \widetilde{B}) \rightarrow \neg\widetilde{AB})$, dass A und B unter keinen Umständen durch die selbe Transition aktualisiert werden. Ganz allgemein steht man also vor dem Probelm auszudrücken, dass eine Transition isoliert ist, das heißt, nur bestimmte Variablen aktualisiert. Das läßt sich wie folgt formalisieren: Sei M die Menge der Varialben, die aktualisiert werden, so wird Folgendes gefordert:

$$\widetilde{M} \wedge \bigwedge_{v \in Var \setminus M} \neg\widetilde{M \cup \{v\}}$$

Für unendliches Var ist dies keine TLDA Formel. Tatsächlich läßt sich diese Eigenschaft nicht mittels TLDA ausdrücken, da anderenfalls über die Varialbenmenge, also über ein Element der Signatur der Sprache, quantifiziert werden müßte.

Um dieses Problem zu umgehen, definiere ich ein zweistelligen Prädikat *closed*. Das erste Argument ist eine Variable aus $\widetilde{Var}$, das zweite Argument ist eine *endliche* Teilmenge von Var und beschränkt die Menge der Variablen, über die etwas ausgesagt wird.

Definition 36 (Prädikat closed**).** Sei $\widetilde{x} \in \widetilde{Var}$ und $A \subseteq Var$ endlich. Das Prädikat closed $\subseteq \widetilde{Var} \times Var$ ist definiert durch:

$$\text{closed}(\widetilde{x}, A) \;\equiv\; \widetilde{x} \wedge \bigwedge_{\substack{v \in A \\ v \notin x}} \neg\widetilde{x \cup \{v\}}$$

Es fragt sich ganz allgemein, wie bei der Konstruktion einer Formel zu einer gegebenen Menge von Runs mit dem Umstand umzugehen ist, dass nur über einen endlichen Variablenraum geredet werden kann, während es Runs gibt, die nicht endlich darstellbar sind. Eine Möglichkeit wäre, diesem Umstand bereits in der Formulierung der Äquivalenz zwischen Runs und verteilten Abläufen Rechnung zu tragen, indem man die Äquivalenz bezüglich der Restriktion des Runs auf die *relevanten*, d.h. im Wertebereich des Labelings des verteilten Ablaufs vorkommenden Variablen

definiert. Ich habe es mir hier etwas einfacher gemacht, indem ich das Problem bei der Definition des Äquivalenzbegriffs ganz außer Acht gelassen habe und stattdessen im Folgenden die Varialbenmenge Var immer auf die (endliche) Platzmenge des zugrundeliegenden Netzes beschränke.

6.2 Definition von Φ_Σ

Definition 37. Sei Σ ein Netz. Dann ist die TLDA-Formel Φ_Σ wie folgt über der Variablenmenge $Var = P_\Sigma$ definiert:

$$\phi_{init} \triangleq \left(\bigwedge_{p \in I_\Sigma} p \right) \wedge \left(\bigwedge_{p \notin I_\Sigma} \neg p \right)$$

$$\phi_t \triangleq \left(\bigwedge_{p \in {}^\bullet t} p \right) \wedge \left(\bigwedge_{p \in {}^\bullet t \setminus t^\bullet} \neg p' \right) \wedge \left(\bigwedge_{p \in t^\bullet} p' \right) \wedge \text{closed}(\widetilde{{}^\bullet t^\bullet}, P_\Sigma) \quad \text{, für alle } t \in T_\Sigma$$

$$\phi_p \triangleq \left(\widetilde{p} \rightarrow \bigvee_{t \in ({}^\bullet p^\bullet)} \phi_t \right) \quad \text{, für alle } p \in P_\Sigma$$

$$\phi_{prog} \triangleq \bigwedge_{t \in Pr_\Sigma} \text{progress}_{{}^\bullet t^\bullet}(\phi_t)$$

$$\Phi_\Sigma \triangleq \phi_{init} \wedge \bigwedge_{p \in P_\Sigma} \Box \phi_p \wedge \phi_{prog}$$

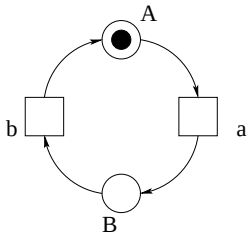

Abbildung 6: Ein Beispielnetz

Als Beispiel diene das Netz aus Abbildung 6. Die Formel Φ_{Abb6} stellt sich dann wie folgt dar:

$$\Phi_{Abb6} \triangleq \underbrace{(A \wedge \neg B)}_{\phi_{init}}$$
$$\wedge \Box \underbrace{\left(\widetilde{A} \rightarrow \vee \begin{array}{l} \underbrace{A \wedge \neg A' \wedge B' \wedge closed(\widetilde{AB}, AB)}_{\phi_a} \\ \underbrace{B \wedge \neg B' \wedge A' \wedge closed(\widetilde{AB}, AB)}_{\phi_b} \end{array} \right)}_{\phi_A}$$
$$\wedge \Box \underbrace{\left(\widetilde{B} \rightarrow \vee \begin{array}{l} \underbrace{A \wedge \neg A' \wedge B' \wedge closed(\widetilde{AB}, AB)}_{\phi_a} \\ \underbrace{B \wedge \neg B' \wedge A' \wedge closed(\widetilde{AB}, AB)}_{\phi_b} \end{array} \right)}_{\phi_B}$$
$$\wedge \underbrace{\left(\wedge \begin{array}{l} \text{progress}_{\{A,B\}}(\underbrace{A \wedge \neg A' \wedge B' \wedge closed(\widetilde{AB}, AB)}_{\phi_a}) \\ \text{progress}_{\{A,B\}}(\underbrace{B \wedge \neg B' \wedge A' \wedge closed(\widetilde{AB}, AB)}_{\phi_b}) \end{array} \right)}_{\phi_{prog}}$$

6.3 Satz über die Korrektheit von Φ_Σ

Die zentrale Aussage dieser Arbeit ist nun der folgende Satz:

Satz 2. *Sei Σ ein Netz. Wenn Vermutung 1 stimmt, so gilt: $\Sigma \simeq \Phi_\Sigma$.*

Der Rest dieser Arbeit widment sich dem Beweis des vorstehenden Satzes.

7 Beweis des Satzes über die Korrektheit von Φ_Σ

In diesem Kapitel wird der Satz 2 bewiesen.

Sei Σ ein Netz und Φ_Σ wie in Definition 37. Zu zeigen ist:

1. **Teil:** Für alle Runs $\mathcal{R}$ mit $\mathcal{R} \models \Phi_\Sigma$ existiert ein verteilter Ablauf $\mathcal{C}$ mit $\mathcal{C} \models \Sigma$ und $\mathcal{C} \simeq \mathcal{R}$.
2. **Teil:** Für alle verteilten Abläufe $\mathcal{C}$ mit $\mathcal{C} \models \Sigma$ existiert ein Run $\mathcal{R}$ mit $\mathcal{R} \models \Phi_\Sigma$ und $\mathcal{R} \simeq \Sigma$.

Technische Lemmata für den Beweis von Satz 2

Das folgende Lemma stellt einen unmittelbaren Zusammenhang zwischen den erreichbaren Markierungen eines Netzes Σ und den Cuts eines Runs von Φ_Σ her. Es ermöglicht damit, Aussagen über Invarianten von Σ auf Φ_Σ zu übertragen.

Lemma 3. *Sei Σ ein Netz. Jede gültige Belegung der Variablen in einem Cut C eines Runs von Φ_Σ entspricht einer erreichbaren Markierung M von Σ, in dem Sinne, dass gilt:*

$$\{p \in Var \mid H_p(C(p))\} = M$$

Beweis von Lemma 3. Zu zeigen ist eine Invariante bzgl. des $\Box$-Opertors. Die Behauptung folgt unmittelbar aus Proposition 1. Um Proposition 1 anwenden zu können, muß Φ_Σ umgebungsinvariant sein. Da $Var = V(\Phi_\Sigma)$, ist Φ_Σ trivialerweise umgebungsinvariant. Es genügt also die Voraussetzungen von Proposition 1 zu zeigen.

Sei C ein Cut mit $C \models \phi_{init}$. Daraus folgt umittelbar

$$\{p \in Var \mid H_p(C_0(p))\} = \{p \in P_\Sigma \mid p \in I_\Sigma\} = I_\Sigma$$

Damit ist Voraussetzung (i) von Proposition 1 gezeigt.

Sei $\phi_{schritt} \triangleq \bigwedge_{p \in P_\Sigma} \phi_p$. Sei $S = (C, C', I_C)$ ein Schritt mit $S \models \phi_{schritt}$ und $M = \{p \in Var \mid H_p(C(p))\}$ ist eine erreichbare Markierung von Σ.

Ich zeige: $M' = \{p \in Var \mid H_p(C'(p))\}$ ist eine erreichbare Markierung von Σ.

Wegen $Var = P_\Sigma$ gilt natürlich $M' = \{p \in P_\Sigma \mid H_p(C'(p))\}$.

Sei $T_S = \{t \in T_\Sigma \mid S \models \phi_t\}$.

Wegen $\phi_t \rightarrow \widetilde{{}^\bullet t^\bullet}$ für alle $t \in T_\Sigma$ gilt (nach [Ale02]), dass für $t \in T_S$ die Mengen ${}^\bullet t^\bullet$ paarweise disjunkt sind.

Nun gilt:

$$\begin{aligned}
& C \models \bigwedge_{p \in {}^\bullet t} p \\
\curvearrowright \quad & \forall t \in T_S \forall p \in {}^\bullet t \colon H_p(C(p)) \\
\curvearrowright \quad & \bigcup_{t \in T_S} {}^\bullet t \subseteq \{p \in Var \mid H_p(C(p))\} = M \\
\curvearrowright \quad & \forall t \in T_S \colon t \text{ ist aktiviert in } M
\end{aligned}$$

Da die Mengen ${}^\bullet t^\bullet$ für $t \in T_S$ paarweise disjunkt sind, gilt für einen Schritt $(M, M^{(t)}, t)$ in Σ, dass alle $t' \in T_S \setminus \{t\}$ in der Markierung $M^{(t)} = (M \setminus {}^\bullet t) \cup t^\bullet$ aktiviert sind. Durch Induktion über T_S folgt, dass $M^{(T_S)} = (M \setminus \bigcup_{t \in T_S} {}^\bullet t) \cup \bigcup_{t \in T_S} t^\bullet$ eine ereichbare Markierung in Σ ist.

Ich zeige nun, dass $M^{(T_S)} = M'$.

Aus $S \models \Phi_\Sigma$ folgt $S \models \widetilde{p} \rightarrow \bigvee_{t \in ({}^\bullet p^\bullet)} \phi_t$, für alle $p \in P_\Sigma$. Daraus folgt unmittelbar $I_C = \bigcup_{t \in T_S} {}^\bullet t^\bullet$. Für alle $p \in (P_\Sigma \setminus \bigcup_{t \in T_S} {}^\bullet t^\bullet)$ gilt folglich $C(p) = C'(p)$ und somit $H_p(C(p)) \Leftrightarrow H_p(C'(p))$. Das heißt:

$$\{p \in (P_\Sigma \setminus \bigcup_{t \in T_S} {}^\bullet t^\bullet) \mid H_p(C'(p))\} = \{p \in (P_\Sigma \setminus \bigcup_{t \in T_S} {}^\bullet t^\bullet) \mid H_p(C(p))\}$$

und

$$M' \cap (P_\Sigma \setminus \bigcup_{t \in T_S} {}^\bullet t^\bullet) = M \cap (P_\Sigma \setminus \bigcup_{t \in T_S} {}^\bullet t^\bullet)$$

Wegen $S \models \bigwedge_{t \in T_S} \phi_t$ gilt weiterhin

$$\begin{aligned}
& C' \models \bigwedge_{t \in T_S} \bigwedge_{p \in {}^\bullet t \setminus t^\bullet} \neg p \wedge \bigwedge_{t \in T_S} \bigwedge_{p \in t^\bullet} p \\
\curvearrowright \quad & \forall t \in T_S \forall p \in {}^\bullet t^\bullet : \ \big(\neg H_p(C'(p)) \Leftrightarrow p \in {}^\bullet t \wedge H_p(C'(p)) \Leftrightarrow p \in t^\bullet\big) \\
\curvearrowright \quad & \{p \in \bigcup_{t \in T_S} {}^\bullet t^\bullet \mid H_p(C'(p))\} = \bigcup_{t \in T_S} t^\bullet \\
\curvearrowright \quad & M' \cap \bigcup_{t \in T_S} {}^\bullet t^\bullet = \bigcup_{t \in T_S} t^\bullet
\end{aligned}$$

Einfache Umformungen im Mengenverband ergeben schließlich:

$$\begin{aligned}
M' &= M' \cap P_\Sigma = M' \cap ((P_\Sigma \setminus \bigcup_{t \in T_S} {}^\bullet t^\bullet) \cup \bigcup_{t \in T_S} {}^\bullet t^\bullet) \\
&= (M' \cap (P_\Sigma \setminus \bigcup_{t \in T_S} {}^\bullet t^\bullet)) \cup (M' \cap \bigcup_{t \in T_S} {}^\bullet t^\bullet) \\
&= (M \cap (P_\Sigma \setminus \bigcup_{t \in T_S} {}^\bullet t^\bullet)) \cup \bigcup_{t \in T_S} t^\bullet \\
&= (M \setminus \bigcup_{t \in T_S} {}^\bullet t^\bullet) \cup \bigcup_{t \in T_S} t^\bullet \\
&= (M \setminus \bigcup_{t \in T_S} {}^\bullet t) \cup \bigcup_{t \in T_S} t^\bullet \\
&= M^{(T_S)}
\end{aligned}$$

M' ist also eine ereichbare Markierung in Σ. Damit ist auch Voraussetzung (ii) von Proposition 1 gezeigt. □

Das folgende Lemma stellt die Anwendung der Eigenschaft der 1-Sicherheit eines Netzes Σ auf die Formel Φ_Σ dar und liefert die Begründung dafür, dass weiter unten im Lemma 7 zu einer Transition $t \in T_\Sigma$ der Effekt einer entsprechenden Transition in $T_\mathcal{R}$ unmittelbar aus der Formel ϕ_t abgelesen werden kann. Im Folgenden setze ich dieses Lemma oft stillschweigend voraus, wenn ich mit Φ_Σ argumentiere.

Lemma 4 (Äquivalente Formulierung für ϕ_t). *Sei Σ ein Netz. Es gilt:*

$$\Phi_\Sigma \rightarrow \Box \left(\bigwedge_{p \in {}^\bullet t} p \rightarrow \bigwedge_{p \in t^\bullet \setminus {}^\bullet t} \neg p \right)$$

Beweis von Lemma 4. Dies folgt unmittelbar aus Lemma 3 und der 1-Sicherheit von Σ: Sei $\mathcal{R}$ ein Run mit $R \models \Phi_\Sigma$ und $\mathcal{R}'$ ein Suffix von $\mathcal{R}$. Nach Lemma 3 gilt für $\mathcal{R}'$, dass $M = \{p \in Var \mid H_p(0)\}$ eine ereichbare Markierung von Σ ist. Sei nun $t \in T_\Sigma$. Wenn $\mathcal{R}' \models \bigwedge_{p \in {}^\bullet t} p$ gilt, dann ist für alle $p \in {}^\bullet t$ $H_p(0)$ erfüllt. Also gilt ${}^\bullet t \subseteq M$. Folglich ist t in M aktiviert und aufgrund der 1-Sicherheit von Σ gilt $(t^\bullet \setminus {}^\bullet t) \cap M = \emptyset$. Das heißt, dass für alle $p \in t^\bullet \setminus {}^\bullet t$ $H_p(0)$ nicht erfüllt ist. Folglich gilt $\mathcal{R}' \models \bigwedge_{p \in t^\bullet \setminus {}^\bullet t} \neg p$ für alle Suffixe $\mathcal{R}'$ von allen Runs $\mathcal{R}$ von Φ_Σ. □

Lemma 5. *Sei Σ ein Netz. Es gilt:*

$$\Phi_\Sigma \rightarrow \Box \left(\mathit{Enabled}_{{}^\bullet t^\bullet}(\phi_t) \Leftrightarrow \bigwedge_{p \in {}^\bullet t} p \right)$$

Beweis von Lemma 5.

$$\begin{aligned}
&\mathit{Enabled}_{{}^\bullet t^\bullet}(\phi_t) \\
&\equiv \exists c_p, p \in {}^\bullet t^\bullet \exists b \exists b_p, p \in P_\Sigma \setminus {}^\bullet t^\bullet : \\
&\quad \phi[c_p/p', p \in {}^\bullet t^\bullet, b/\widetilde{{}^\bullet t^\bullet}, b_p/\widetilde{{}^\bullet t^\bullet \cup p}, p \in P_\Sigma \setminus {}^\bullet t^\bullet] \\
&\equiv \exists c_p, p \in {}^\bullet t \setminus t^\bullet \exists c_q, q \in t^\bullet \exists b \exists b_p, p \in P_\Sigma \setminus {}^\bullet t^\bullet : \\
&\quad \bigwedge_{p \in {}^\bullet t} p \wedge \bigwedge_{p \in {}^\bullet t \setminus t^\bullet} \neg c_p \wedge \bigwedge_{q \in t^\bullet} c_q \wedge b \wedge \bigwedge_{p \in P_\Sigma \setminus {}^\bullet t^\bullet} \neg b_p \\
&\equiv \bigwedge_{p \in {}^\bullet t} p \wedge \exists c_p, p \in {}^\bullet t \setminus t^\bullet \exists c_q, q \in t^\bullet \exists b \exists b_p, p \in P_\Sigma \setminus {}^\bullet t^\bullet : \\
&\quad \bigwedge_{p \in {}^\bullet t \setminus t^\bullet} \neg c_p \wedge \bigwedge_{q \in t^\bullet} c_q \wedge b \wedge \bigwedge_{p \in P_\Sigma \setminus {}^\bullet t^\bullet} \neg b_p \\
&\equiv \bigwedge_{p \in {}^\bullet t} p
\end{aligned}$$

□

Lemma 6. *Sei Σ ein Netz und $t \in Pr_\Sigma$. Für eine Run $\mathcal{R}$ gilt:*

$$\mathcal{R} \models \mathit{progress}_{{}^\bullet t^\bullet}(\phi_t) \text{ gdw. } \exists p \in {}^\bullet t \, \forall i \in \mathbb{N} \, \exists r \in T_\mathcal{R} \colon H_p(i) \rightarrow r(p) = i$$

Beweis von Lemma 6.

$$\mathcal{R} \models progress_{\bullet t \bullet}(\phi_t)$$

$$\curvearrowright \quad \mathcal{R} \models \neg negP_{\bullet t \bullet}(\phi_t)$$

$$\curvearrowright \quad \mathcal{R} \models \neg\Diamond\Box(\bigwedge_{p \in \bullet t \bullet} \neg\widetilde{p} \wedge Enabled(\phi_t))$$

$$\curvearrowright \quad \mathcal{R} \models \Box\Diamond(\bigvee_{p \in \bullet t \bullet} \widetilde{p} \vee \neg \bigwedge_{p \bullet t} p) \qquad \text{(Lemma 3)}$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\, \exists T, T \text{ suff } S\colon$$
$$(\exists p \in {}^\bullet t^\bullet\colon T \models \widetilde{p}) \vee (\exists p \in {}^\bullet t\colon T \models \neg p))$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\, \exists T, T \text{ suff } S\colon$$
$$(\exists p \in {}^\bullet t\colon T \models \widetilde{p} \vee \neg p) \vee (\exists p \in t^\bullet \setminus {}^\bullet t\colon T \models \widetilde{p}))$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\, \exists T, T \text{ suff } S\colon$$
$$(\exists p \in {}^\bullet t \exists s \in T_T\colon s(p) = 0 \vee \neg H_p^{(T)}(0))$$
$$\vee (\exists p \in t^\bullet \setminus {}^\bullet t\colon T \models \bigvee_{s \in {}^\bullet p^\bullet} \phi_s)$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\, \exists T, T \text{ suff } S\colon$$
$$(\exists p \in {}^\bullet t \exists s \in T_T\colon H_p^{(T)}(0) \to s(p) = 0)$$
$$\vee (\exists p \in t^\bullet \setminus {}^\bullet t\colon (\exists s \in p^\bullet\colon T \models \phi_s) \vee (\exists s \in {}^\bullet p \setminus p^\bullet\colon T \models \phi_s))$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\, \exists T, T \text{ suff } S\colon$$
$$(\exists p \in {}^\bullet t \exists s \in T_T\colon H_p^{(T)}(0) \to s(p) = 0)$$
$$\vee (\exists p \in t^\bullet \setminus {}^\bullet t\colon (\exists s \in p^\bullet\colon T \models p) \vee (\exists s \in {}^\bullet p \setminus p^\bullet\colon T \models p')$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\, \exists T, T \text{ suff } S\colon$$
$$(\exists p \in {}^\bullet t \exists s \in T_T\colon H_p^{(T)}(0) \to s(p) = 0)$$
$$\vee (\exists p \in t^\bullet \setminus {}^\bullet t\colon (T \models p) \vee (T' \text{ (Nachfolger von T)} \models p)$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\colon$$
$$(\exists T, T \text{ suff } S \exists p \in {}^\bullet t \exists s \in T_T\colon H_p^{(T)}(0) \to s(p) = 0)$$
$$\vee (\exists T, T \text{ suff } S \exists p \in t^\bullet \setminus {}^\bullet t\colon T \models p) \vee (\exists T, T \text{ suff } S \exists p \in t^\bullet \setminus {}^\bullet t\colon T \models p)$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\colon \qquad \text{(Korollar 4)}$$
$$(\exists p \in {}^\bullet t \exists i \in \mathbb{N} \exists s \in T_S\colon H_p^{(S)}(i) \to s(p) = i)$$
$$\vee (\exists T, T \text{ suff } S \exists p \in {}^\bullet t\colon T \models \neg p)$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\colon$$
$$(\exists p \in {}^\bullet t \exists i \in \mathbb{N} \exists s \in T_S\colon H_p^{(S)}(i) \to s(p) = i)$$
$$\vee (\exists p \in {}^\bullet t \exists i \in \mathbb{N} s \in T_S\colon \neg H_p^{(S)}(i))$$

$$\curvearrowright \quad \forall S, S \text{ suff } \mathcal{R}\colon$$
$$(\exists p \in {}^\bullet t \exists i \in \mathbb{N} \exists s \in T_S\colon H_p^{(S)}(i) \to s(p) = i)$$

Induktiv folgt, dass es unendlich viele Suffixe von $\mathcal{R}$ gibt. Nun kann ein Schubfachargument angwandt werden: Unendlich viele Schritte involvieren endlich viele

Variablen. Also existiert eine Variable die unendlich oft involviert ist:

$$\exists p \in {}^\bullet t \, \forall i \in \mathbb{N} \, \exists s \in T_{\mathcal{R}} \colon H_p^{(\mathcal{R})}(i) \to s(p) = i$$

Die Rückrichtung kann ähnlich gezeigt werden:

$$\begin{aligned}
& \exists p \in {}^\bullet t \, \forall i \in \mathbb{N} \, \exists s \in T_R \colon H_p^{(R)}(i) \to s(p) = i \\
\curvearrowright \quad & \forall S, S \text{ suff } \mathcal{R} \exists p \in {}^\bullet t \exists i \in \mathbb{N} \exists s \in T_S \colon H_p^{(S)}(i) \to s(p) = i \\
\curvearrowright \quad & \forall S, S \text{ suff } \mathcal{R} \, \exists T, T \text{ suff } S \exists p \in {}^\bullet t \exists s \in T_T \colon H_p^{(T)}(0) \to s(p) = 0) \\
\curvearrowright \quad & \forall S, S \text{ suff } \mathcal{R} \, \exists T, T \text{ suff } S \exists p \in {}^\bullet t \exists s \in T_T \colon \neg H_p^{(T)}(0) \vee s(p) = 0) \\
\curvearrowright \quad & \forall S, S \text{ suff } \mathcal{R} \, \exists T, T \text{ suff } S \exists p \in {}^\bullet t \colon \widetilde{p} \vee \neg p) \\
\curvearrowright \quad & \forall S, S \text{ suff } \mathcal{R} \, \exists T, T \text{ suff } S \colon (\exists p \in {}^\bullet t^\bullet \colon T \models \widetilde{p}) \vee (\exists p \in {}^\bullet t \colon T \models \neg p)) \\
\curvearrowright \quad & \mathcal{R} \models \Box\Diamond(\bigvee_{p \in {}^\bullet t^\bullet} \widetilde{p} \vee \neg \bigwedge_{p^\bullet t} p) && \text{(Lemma 3)} \\
\curvearrowright \quad & \mathcal{R} \models \neg\Diamond\Box(\bigwedge_{p \in {}^\bullet t^\bullet} \neg\widetilde{p} \wedge \mathit{Enabled}(\phi_t)) \\
\curvearrowright \quad & \mathcal{R} \models \neg \mathit{negP}_{{}^\bullet t^\bullet}(\phi_t) \\
\curvearrowright \quad & \mathcal{R} \models \mathit{progress}_{{}^\bullet t^\bullet}(\phi_t)
\end{aligned}$$

□

Lemma 7. *Sei Σ ein Netz und $\mathcal{R}$ ein Run mit $\mathcal{R} \models \Phi_\Sigma$. Sei ferner $r \in T_{\mathcal{R}}$, dann exitiert ein $t \in T_\Sigma$, so dass $\mathrm{eff}_\Sigma(t) = \mathrm{eff}_{\mathcal{R}}(r)$. Wenn Σ einfach ist, dann ist t eindeutig bestimmt.*

Beweis von Lemma 7. Sei $\mathcal{R}_r$ ein r-Suffix von $\mathcal{R}$.

$$\curvearrowright \quad \mathcal{R}_r \models \widetilde{\mathrm{Inv}(r)} \qquad \text{(Def. } r\text{-Suffix)}$$

Wegen $\mathcal{R} \models \Phi_\Sigma$ folgt $\mathcal{R}_r \models \bigwedge_{p \in P_\Sigma} (\widetilde{p} \to \bigvee_{t \in {}^\bullet p^\bullet} \phi_t)$. Somit ergibt sich:

$$\begin{aligned}
& \forall x \in \mathrm{Inv}(r) \colon \mathcal{R}_r \models \bigvee_{t \in {}^\bullet x^\bullet} \phi_t \\
\curvearrowright \quad & \forall x \in \mathrm{Inv}(r) \, \exists t \in {}^\bullet x^\bullet \colon \mathcal{R}_r \models \phi_t && (*) \\
\curvearrowright \quad & \forall x \in \mathrm{Inv}(r) \, \exists t \in {}^\bullet x^\bullet \colon \mathcal{R}_r \models \mathrm{closed}(\widetilde{V(\phi_t)}, P_\Sigma) && \text{(Def. } \phi_t) \\
\curvearrowright \quad & \forall x \in \mathrm{Inv}(r) \, \exists t \in {}^\bullet x^\bullet \, \exists s \in T_R \colon && \text{(Def. von closed)} \\
& \quad \mathcal{R}_r \text{ ist } s\text{-Suffix von } R \ \wedge \mathrm{Inv}(s) = V(\phi_t) \\
\curvearrowright \quad & \forall x \in \mathrm{Inv}(r) \, \exists t \in {}^\bullet x^\bullet \, \exists s \in T_R \colon && \text{(da } x \in V(\phi_t)) \\
& \quad \mathcal{R}_r \text{ ist } s\text{-Suffix von } R \ \wedge \mathrm{Inv}(s) = V(\phi_t) \\
& \quad \wedge \mathrm{Inv}(s) \cap \mathrm{Inv}(r) \neq \emptyset
\end{aligned}$$

Aus $\mathrm{Inv}(r) \cap \mathrm{Inv}(s) \neq \emptyset$ und R_r ist s-Suffix und r-Suffix von R folgt $r = s$ und man erhält:

$$\begin{aligned}
& \forall x \in \mathrm{Inv}(r)\ \exists t \in {}^\bullet x^\bullet\ \exists s \in T_R\colon \\
& \quad \mathcal{R}_r \text{ ist } s\text{-Suffix von } R\ \wedge \mathrm{Inv}(s) = V(\phi_t) = \mathrm{Inv}(r) \\
\curvearrowright\ & \forall x \in \mathrm{Inv}(r)\ \exists t \in {}^\bullet x^\bullet\colon V(\phi_t) = \mathrm{Inv}(r) \wedge R_r \models \phi_t \qquad \text{(wegen } (*)\text{)} \\
\curvearrowright\ & \exists t \in T_\Sigma\colon V(\phi_t) = \mathrm{Inv}(r) \wedge R_r \models \phi_t
\end{aligned}$$

Wenn nur einfache Netze betrachtet werden, gilt nach Konstruktion von Φ_Σ $V(\phi_t) = V(\phi_u) \Rightarrow (u = t \vee \phi_u \rightarrow \neg\phi_t)$. Somit ist t eindeutig bestimmt:

$$\exists! t \in T_\Sigma\colon V(\phi_t) = \mathrm{Inv}(r) \wedge R_r \models \phi_t$$

Da es nach Korollar 4 genau eine Belegung der Variablen in $\mathrm{Inv}(r)$ gibt, die ϕ_t erfüllt, somit der Wert aller Variablen eindeutig bestimmt ist, folgt schließlich (nach Def. eff und Def. Φ_Σ)

$$\exists t \in T_\Sigma\ \mathrm{eff}_R(r) = \mathrm{eff}_\Sigma(t)$$

bzw.

$$\exists! t \in T_\Sigma\ \mathrm{eff}_R(r) = \mathrm{eff}_\Sigma(t) \quad \text{, falls } \Sigma \text{ einfach ist.}$$

□

Proposition 8. *Sei Σ ein Netz und $\mathcal{C}$ ein verteilter Ablauf mit $\mathcal{C} \models_l \Sigma$. Sei $s, t \in T_\mathcal{C}$ und $x \in P_\Sigma$. Es gilt:*

$$x \in {}^\bullet l(t)^\bullet \wedge x \in {}^\bullet l(s)^\bullet \quad \Rightarrow \quad s < t \vee t < s \vee t = s$$

Beweis von Proposition 8. Sei $x \in {}^\bullet l(t)^\bullet \wedge x \in {}^\bullet l(s)^\bullet$. Es existieren also $p \in {}^\bullet t^\bullet$ und $q \in {}^\bullet s^\bullet$ mit $l(p) = x = l(q)$. Da (nach Def. verteilter Ablauf) gleich gelabelte Element nicht nebenläufig sind, folgt

$$p < q \vee q < p \vee p = q$$

Im folgenden nehme ich an, dass $p < q \vee p = q$. Nach der Definition von verteiltem Ablauf exitierten nun genau ein u mit $p \in {}^\bullet u$ und genau ein v mit $q \in v^\bullet$. Wenn $p = q$, dann gilt $v < p = q < u$ und $s = u \vee s = v$ und $t = u \vee t = v$, woraus die Behauptung unmittelbar folgt. Bleibt also $p < q$. Hieraus folgt $u \leq v$.

1. Fall: $p \in t^\bullet \quad \curvearrowright \quad t < p < u \leq v.$

2. Fall: $p \in {}^\bullet t \quad \curvearrowright \quad p < t = u \leq v.$

Es gilt somit $t \leq v$.

1. Fall: $q \in s^\bullet \quad \curvearrowright \quad t \leq v = s.$

2. Fall: $q \in {}^\bullet s \quad \curvearrowright \quad t \leq v < s.$

Für $q < p \vee p = q$ erhält man ganz analog $s < t \vee s = t$, so dass insgesamt gilt $s < t \vee t < s \vee t = s$. □

Proposition 9. *Sei Σ ein Netz und $\mathcal{C}$ ein verteilter Ablauf mit $\mathcal{C} \models_l \Sigma$. Sei $s, t \in T_\mathcal{C}$ und $x \in P_\Sigma$. Es gilt:*

(i) $x \in {}^\bullet l(s)^\bullet \wedge x \in {}^\bullet l(t) \wedge s < t \wedge (\nexists u \in T_\mathcal{C} \colon s < u < t \wedge x \in {}^\bullet l(u)^\bullet) \quad \Rightarrow \quad x \in l(s)^\bullet$

(ii) $x \in l(s)^\bullet \wedge x \in {}^\bullet l(t)^\bullet \wedge s < t \wedge (\nexists u \in T_\mathcal{C} \colon s < u < t \wedge x \in {}^\bullet l(u)^\bullet) \quad \Rightarrow \quad x \in {}^\bullet l(t)$

Beweis von Proposition 9. Um i. zu zeigen, sei $x \in {}^\bullet l(s)^\bullet$ und $x \in {}^\bullet l(t)$ und $s < t$ und $\nexists u \in T_\mathcal{C} \colon s < u < t \wedge x \in {}^\bullet l(u)^\bullet$.

1. Fall: $x \in {}^\bullet l(s)$. Dann existieren $p, q \in P_\mathcal{C}$ mit

$$l(p) = x = l(q) \wedge p \in {}^\bullet s \wedge q \in {}^\bullet t$$

Da gleich gelabelte Elemente nicht nebenläufig sind, gilt $(p < q \vee q < p \vee p = q)$ und insgesamt gilt:

$$(p < q \vee q < p \vee p = q) \wedge s < t \wedge pF_\mathcal{C} s \wedge qF_\mathcal{C} t$$

Da s einzige Transition im Nachbreich von p ist, folgt

$$pF_\mathcal{C} s < qF_\mathcal{C} t$$

und wegen $\nexists u \in T_\mathcal{C} \colon s < u < t \wedge x \in {}^\bullet l(u)^\bullet$ und $l(q) = x$ folgt $pF_\mathcal{C} sF_\mathcal{C} qF_\mathcal{C} t$. Also gilt $q \in s^\bullet$ und man erhält $x \in l(s)^\bullet$.

2. Fall: $x \in l(s)^\bullet$. In diesem Fall ist nichts weiter zu zeigen.

Der Beweis von ii. geht analog. □

Proposition 10. *Sei Σ ein Netz und $\mathcal{C}$ ein verteilter Ablauf mit $\mathcal{C} \models_l \Sigma$. Sei $x \in P_\Sigma$ und $p \in P_\mathcal{C}$ mit $l(p) = x$. Sei ferner $t \in T_\mathcal{C}$.*

(i) Wenn $p < t$ und kein $s \in T_\mathcal{C}$ mit $x \in {}^\bullet l(s)^\bullet$ und $p < s < t$ exitiert, dann ist $x \in {}^\bullet l(t)$.

(ii) Wenn $t < p$ und kein $s \in T_\mathcal{C}$ mit $x \in {}^\bullet l(s)^\bullet$ und $t < s < p$ exitiert, dann ist $x \in l(t)^\bullet$.

Beweis von Proposition 10. Beweis von i: Wegen $p < t$ gilt, dass eine Transition u im Nachbreich von p existiert, die (nach Definition von verteiltem Ablauf) eindeutig bestimmt ist. Es gilt also: $pF_\mathcal{C} u \leq t$. Wegen $x \in {}^\bullet l(u)^\bullet$ kann nach Voraussetzung nicht gelten $u < t$, also folgt $u = t$. Somit ist $x \in {}^\bullet l(t)$.

Beweis von ii: Analog zum Beweis von i erhält man: $t \leq uF_\mathcal{C} p$ und mit dem gleichen Argument folgt: $u = t$ und $x \in l(t)^\bullet$. □

Erster Teil des Beweises von Satz 2

Sei $\mathcal{R} = (H_\mathcal{R}, T_\mathcal{R})$ ein Run mit $\mathcal{R} \models \Phi_\Sigma$. Zu zeigen ist:

$$\exists \mathcal{C} \colon \mathcal{C} \models \Sigma \wedge \mathcal{C} \simeq \mathcal{R}$$

Schritte:

1. Konstruiere $\mathcal{C}$, und
2. zeige: $\mathcal{C} \simeq \mathcal{R}$.
3. Zeige: $\mathcal{C} \models \Sigma$.

1. Schritt

Konstruktion von $\mathcal{C}$, so dass $\mathcal{C} \simeq \mathcal{R}$:

Sei $\mathcal{C}$ ein Petrinetz mit

$$\begin{aligned} T_{\mathcal{C}} =& T_{\mathcal{R}} \\ P_{\mathcal{C}} =& \{(x,i) \mid x \in Var \wedge H_x(i), i \in \mathbb{N}\} \\ F_{\mathcal{C}} =& \{\big((x,i),t\big) \mid (x,i) \in P_{\mathcal{C}} \wedge t \in T_{\mathcal{C}} \wedge x \in \mathrm{Inv}(t) \wedge t(x) = i\} \cup \\ & \{\big(t,(x,i)\big) \mid (x,i) \in P_{\mathcal{C}} \wedge t \in T_{\mathcal{C}} \wedge x \in \mathrm{Inv}(t) \wedge t(x)+1 = i\} \end{aligned}$$

Aus der Definition eines Runs folgt unmittelbar, dass zu jedem $(x,i) \in P_{\mathcal{C}}$ maximal ein $t \in T_{\mathcal{C}}$ existiert mit $(x,i)F_{\mathcal{C}}t$ und maximal ein $t \in T_{\mathcal{C}}$ existiert mit $tF_{\mathcal{C}}(x,i)$. Ebenso ist klar, dass zu jedem $t \in T_{\mathcal{C}}$ mindestens ein $(x,i) \in P_{\mathcal{C}}$ existiert mit $(x,i)F_{\mathcal{C}}t$ und mindestens ein $(x,i) \in P_{\mathcal{C}}$ existiert mit $tF_{\mathcal{C}}(x,i)$. Offensichtlich ist auch $\{a \mid a <_{\mathcal{C}} b\}$ endlich für alle $a \in P_{\mathcal{C}} \cup T_{\mathcal{C}}$. Da $\prec_{\mathcal{R}}$ irreflexiv ist, folgt zusammen mit folgender Proposition, dass $\mathcal{C}$ ein verteilter Ablauf ist.

Proposition 11. *Für alle $s,t \in T_{\mathcal{C}}$ gilt: $s <_{\mathcal{C}} t \Leftrightarrow s \prec_{\mathcal{R}} t$.*

Beweis von Proposition 11. "$\Rightarrow$": Sei $s <_{\mathcal{C}} t$.

$$\begin{aligned} \curvearrowright\ & \exists n \in \mathbb{N}\ \exists u_1,\dots,u_n \in T_{\mathcal{C}}, p_1,\dots,p_{n-1} \in P_{\mathcal{C}} \colon s = u_1 \ \wedge\ t = u_n \quad (\text{Def. } <_{\mathcal{C}}) \\ & \qquad \wedge\ (\forall 1 \le i \le n-1 \colon u_i F_{\mathcal{C}} p_i \ \wedge\ p_i F_{\mathcal{C}} u_{i+1}) \end{aligned}$$

$$\begin{aligned} \curvearrowright\ & \exists n \in \mathbb{N}\ \exists u_1,\dots,u_n \in T_{\mathcal{C}}, p_1,\dots,p_{n-1} \in P_{\mathcal{C}} \colon s = u_1 \ \wedge\ t = u_n \quad (\text{Def. } F_{\mathcal{C}}) \\ & \quad \wedge\ \Big(\forall 1 \le i \le n-1 \colon u_i(p_i^1) = p_i^2 - 1 \ \wedge\ u_{i+1}(p_i^1) = p_i^2\Big), \\ & \text{mit}\quad u_i \in T_{\mathcal{R}}, \\ & \qquad p_i^1 \text{ ist 1. Element des Tupels } p_i, \\ & \qquad p_i^2 \text{ ist 2. Element des Tupels } p_i, \\ & \qquad p_i^1 \in \mathrm{Inv}(u_i),\ p_i^1 \in \mathrm{Inv}(u_{i+1}),\ p_i^2 \in \mathbb{N} \end{aligned}$$

$$\begin{aligned} \curvearrowright\ & \exists n \in \mathbb{N}\ \exists u_1,\dots,u_n \in T_{\mathcal{C}}, p_1,\dots,p_{n-1} \in P_{\mathcal{C}} \colon s = u_1 \ \wedge\ t = u_n \quad (\text{Def. } \prec_{\mathcal{R}}) \\ & \qquad \wedge\ (\forall 1 \le i \le n-1 \colon u_i \prec_{\mathcal{R}} u_{i+1}), \\ \curvearrowright\ & \exists n \in \mathbb{N}\ \exists u_1,\dots,u_n \in T_{\mathcal{C}}, p_1,\dots,p_{n-1} \in P_{\mathcal{C}} \colon s = u_1 \ \wedge\ t = u_n \quad (\text{Def. } \prec_{\mathcal{R}}) \\ & \qquad \wedge\ (\forall 1 \le i \le n-1 \colon u_1 \prec_{\mathcal{R}} u_n), \\ \curvearrowright\ & s \prec t \end{aligned}$$

"$\Leftarrow$": Die Rückrichtung ergibt sich, indem der vorstehende Beweis zeilenweise von unten nach oben gelesen wird. □

Die folgenden Propositionen werden später noch verwendet. Sie folgen unmittelbar aus der Definition von $\mathcal{C}$.

Proposition 12.

(i) $\exists i \in \mathbb{N}\colon \big((x,i),t\big) \in F_{\mathcal{C}} \Leftrightarrow \big((x,t(x)),t\big) \in F_{\mathcal{C}} \Leftrightarrow x \in \mathrm{Inv}(t) \wedge H_x(t(x))$.

(ii) $\exists i \in \mathbb{N}\colon \big(t,(x,i)\big) \in F_{\mathcal{C}} \Leftrightarrow \big(t,(x,t(x)+1)\big) \in F_{\mathcal{C}} \Leftrightarrow x \in \mathrm{Inv}(t) \wedge H_x(t(x)+1)$.

Proposition 13. *Es gilt:*

$$^\circ\mathcal{C} = \{x \in Var \mid H_x(0)\}$$

Das Labeling l von $\mathcal{C}$ mit Σ ist wie folgt definiert:

$$\begin{array}{ll} l\colon \mathcal{C} \to \Sigma \quad \text{mit} & \\ l\big((x,i)\big) = x & \text{für } (x,i) \in P_\mathcal{C} \\ l(r) = t, \quad \text{mit } \mathrm{eff}_\Sigma(t) = \mathrm{eff}_\mathcal{R}(r) & \text{für } r \in T_\mathcal{C} (= T_\mathcal{R}) \end{array}$$

Wegen Lemma 7 ist l wohldefiniert. Man beachte aber, dass t in der Definition von l nur dann eindeutig bestimmt ist, wenn Σ einfach ist.

2. Schritt

Zu zeigen ist $\mathcal{C} \simeq \mathcal{R}$.
Sei $f\colon T_\mathcal{R} \to T_\mathcal{C}$ mit $f = id$.

1. Proposition 11 besagt, dass für alle $s,t \in T_\mathcal{C}$ gilt: $s <_\mathcal{C} t \Leftrightarrow s \prec_\mathcal{R} t$.

2. Zu zeigen ist: $\forall t \in T_\mathcal{R}\colon \mathrm{eff}_\mathcal{R}(t) = \mathrm{eff}^l_\mathcal{C}(f(t))$.

Ich zeige zunächst komponentenweise Gleichheit:

Sei $x \in \mathrm{Inv}(t)$. Dann gilt

$$\begin{array}{rll} \mathrm{eff}^l_\mathcal{C}(f(t),x) &= \big(x \in l({}^\bullet f(t)), x \in l(f(t)^\bullet)\big) & \text{(Def. } \mathrm{eff}^l_\mathcal{C}\text{)} \\ &= \big(\exists i \in \mathbb{N}\colon (x,i) F_\mathcal{C} f(t), \exists j \in \mathbb{N}\colon f(t) F_\mathcal{C} (x,j)\big) & \text{(Def. } l, F_\mathcal{C}, {}^\bullet t, t^\bullet\text{)} \\ &= \big(H_x(t(x)), H_x(t(x)+1)\big) & \text{(Proposition 12)} \\ &= \mathrm{eff}_\mathcal{R}(t,x) & \text{(Def. } \mathrm{eff}_\mathcal{R}\text{)} \end{array}$$

Bleibt zu zeigen, dass die Definitionsbereiche der Effekte gleich sind, d.h.:

$$x \in \mathrm{Inv}(t) \quad \Leftrightarrow \quad \exists i \in \mathbb{N}\colon (x,i) \in {}^\bullet f(t)^\bullet$$

"$\Rightarrow$": Sei $x \in \mathrm{Inv}(t)$. Sei $S = (C, C', I_C)$ ein Schritt in $\mathcal{R}$ mit $t \in T_C$. Somit gilt $S \models \Phi_\Sigma$ und es folgt:

$$\begin{array}{lll} & S \models \widetilde{x} & \text{(Def. } I_C\text{)} \\ \curvearrowright & S \models \bigvee\limits_{s \in {}^\bullet x^\bullet} \phi_s & \text{(Def. } \mathcal{R}, \Phi_\Sigma\text{)} \\ \curvearrowright & \exists s \in {}^\bullet x^\bullet\colon S \models \phi_s & \\ \curvearrowright & \exists s\colon (x \in s^\bullet \vee x \in {}^\bullet s) \wedge S \models \phi_s & \text{(Def. } {}^\bullet\text{)} \\ \curvearrowright & \exists s\colon S \models x \vee x' & \text{(Def. } \phi_s\text{)} \\ \curvearrowright & S \models x \vee x' & \\ \curvearrowright & H_x(t(x)) \vee H_x(t(x)+1) & \text{(da nach Voraussetzung } x \in \mathrm{Inv}(t)\text{)} \\ \curvearrowright & \exists i \in \mathbb{N}\colon \big((x,i), f(t)\big) \in F_\mathcal{C} \vee \exists i \in \mathbb{N}\colon \big(f(t), (x,i)\big) \in F_\mathcal{C} & \text{(Proposition 12 und Voraussetzung)} \\ \curvearrowright & \exists i \in \mathbb{N}\colon (x,i) \in {}^\bullet f(t)^\bullet & \end{array}$$

"$\Leftarrow$": Sei $(x,i) \in {}^\bullet f(t)^\bullet$.

$$\curvearrowright \quad f(t)F_{\mathcal{C}}(x,i) \vee (x,i)F_C f(t) \qquad \text{(Def. } {}^\bullet\text{)}$$
$$\curvearrowright \quad x \in \mathrm{Inv}(t) \qquad \text{(Def. } F_{\mathcal{C}}\text{)}$$

3. Proposition 13 besagt, dass ${}^\circ\mathcal{C} = \{x \in Var \mid H_x(0)\}$.

Somit ist $f = id$ die gesuchte Bijektion von $T_{\mathcal{R}}$ auf $T_{\mathcal{C}}$ und es gilt: $\mathcal{C} \simeq \mathcal{R}$.

3. Schritt

Zu zeigen ist: $\mathcal{C} \models_l \Sigma$

1. Labeling l erfüllt:
   (a) Nebenläufige Elemente sind unterschiedlich gelabelt
   (b) Für $t \in T_{\mathcal{C}}$ gilt: $l({}^\bullet t) = {}^\bullet l(t)$ und $l(t^\bullet) = l(t)^\bullet$
2. $I_\Sigma = {}^\circ\mathcal{C}$
3. $\mathcal{C}$ respektiert den Progress aller Transitionen.

zu 1a: Seien $d, e \in T_{\mathcal{C}}$ nebenläufig in $\mathcal{C}$. Es folgt unmittelbar $d \neq e$. Weiterhin sei $s = l(d)$ und $t = l(e)$. Da $\mathcal{C} \simeq \mathcal{R}$ sind $f^{-1}(d)$ und $f^{-1}(e)$ dann auch nebenläufig in $\mathcal{R}$ und somit gilt (nach einer Proposition aus [Ale02]) $\mathrm{Inv}(d) \cap \mathrm{Inv}(e) = \emptyset$. Wir haben also

$$s = l(d) \ \wedge \ t = l(e) \ \wedge \ \mathrm{Inv}(f^{-1}(d)) \cap \mathrm{Inv}(f^{-1}(e)) = \emptyset$$

Mit der Definition von l folgt:

$$\mathrm{eff}_\Sigma(s) = \mathrm{eff}_{\mathcal{R}}(f^{-1}(d)) \wedge \mathrm{eff}_\Sigma(t) = \mathrm{eff}_{\mathcal{R}}(f^{-1}(e)) \wedge \mathrm{Inv}(f^{-1}(d)) \cap \mathrm{Inv}(f^{-1}(e)) = \emptyset$$

und aufgrund der Definition des Effektes und von ϕ_s und ϕ_t gilt

$$V(\phi_s) = \mathrm{Inv}(f^{-1}(d)) \ \wedge \ V(\phi_t) = \mathrm{Inv}(f^{-1}(e)) \ \wedge \ \mathrm{Inv}(f^{-1}(d)) \cap \mathrm{Inv}(f^{-1}(e)) = \emptyset$$

Daraus folgt unmittelbar

$$V(\phi_s) \cap V(\phi_t) = \emptyset$$

und man erhält schließlich $s \neq t$.

Seien nun $(p,i), (q,j) \in P_{\mathcal{C}}$ nebenläufig. Dann gilt, dass $(p,i)^\bullet$ und $(q,j)^\bullet$ nebenläufig oder gleich sind. Wegen $\mathcal{C} \simeq \mathcal{R}$ sind $f^{-1}((p,i)^\bullet)$ und $f^{-1}((q,j)^\bullet)$ in $\mathcal{R}$ ebenfalls nebenläufig oder gleich. Im zweiten Falle müßte gelten: $f^{-1}((p,i)^\bullet)(p) = i$ und $f^{-1}((p,i)^\bullet)(q) = j$. Dies impliziert $p \neq q$ oder $(p,i) = (q,j)$, wobei letztere Alternative nach Voraussetzung falsch ist. Bleibt noch der Fall zu betrachten, dass $f^{-1}((p,i)^\bullet)$ und $f^{-1}((q,j)^\bullet)$ in $\mathcal{R}$ nebenläufig sind. Dann gilt (nach einer Proposition aus [Ale02]) $f^{-1}((p,i)^\bullet) \cap f^{-1}((q,j)^\bullet) = \emptyset$ und, da $p \in \mathrm{Inv}(f^{-1}((p,i)^\bullet))$ und $q \in \mathrm{Inv}(f^{-1}((q,j)^\bullet))$, folgt $p \neq q$. Nach Definition von l gilt somit $l((p,i)) \neq l((q,j))$. Damit ist 1a gezeigt.

zu 1b: Zu zeigen ist: Für $t \in T_{\mathcal{C}}$ gilt: $l({}^\bullet t) = {}^\bullet l(t)$ und $l(t^\bullet) = l(t)^\bullet$.

$$
\begin{aligned}
l({}^\bullet t) =& l(\{(p,i) \mid (p,i) F_{\mathcal{C}} t\}) \\
=& \{l((p,i)) \mid (p,i) F_{\mathcal{C}} t\} \\
=& \{p \mid \exists i \in \mathbb{N} \colon (p,i) F_{\mathcal{C}} t\} && \text{(Def. } l\text{)} \\
=& \{p \mid p \in \mathrm{Inv}(f^{-1}(t)) \wedge H_p(f^{-1}(t)(p))\} && \text{(Prop. 12)} \\
=& \{p \mid \mathrm{eff}_{\mathcal{R}}(f^{-1}(t), p) = (true, *), * \in \{true, false\}\} && \text{(Def. eff}_{\mathcal{R}}\text{)} \\
=& \{p \mid \mathrm{eff}_{\Sigma}(l(t), p) = (true, *), * \in \{true, false\}\} && \text{(Def. } l\text{)} \\
=& \{p \mid p \in {}^\bullet l(t)\} = {}^\bullet l(t) && \text{(Def. eff}_{\Sigma}\text{)}
\end{aligned}
$$

$$
\begin{aligned}
l(t^\bullet) =& l(\{(p,i) \mid t F_{\mathcal{C}} (p,i)\}) && \text{(siehe oben)} \\
=& \{p \mid \exists i \colon t F_{\mathcal{C}} (p,i)\} \\
=& \{p \mid p \in \mathrm{Inv}(f^{-1}(t)) \wedge H_p(f^{-1}(t)(p) + 1)\} \\
=& \{p \mid \mathrm{eff}_{\mathcal{R}}(f^{-1}(t), p) = (*, true), * \in \{true, false\}\} \\
=& \{p \mid \mathrm{eff}_{\Sigma}(l(t), p) = (*, true), * \in \{true, false\}\} \\
=& \{p \mid p \in l(t)^\bullet\} = l(t)^\bullet
\end{aligned}
$$

zu 2:

$$
\begin{aligned}
{}^\circ\mathcal{C} =& \{x \in Var \mid H_0(x)\} && \text{(Prop. 13)} \\
=& \{x \in Var \mid \Phi_\Sigma \rightarrow x\} && \text{(Sematik von TLDA)} \\
=& \{x \in Var \mid \phi_{init} \rightarrow x\} && \text{(Konstruktion von } \Phi_\Sigma\text{)} \\
=& \{x \in Var \mid x \in I_\Sigma\} && \text{(Konstruktion von } \phi_{init}\text{)} \\
=& I_\Sigma
\end{aligned}
$$

zu 3: Zu zeigen ist: Für alle $t \in Pr_\Sigma$ gilt: $l(\mathcal{C}^\circ)$ aktiviert nicht t.

Sei $t \in Pr_\Sigma$. Es gilt:

$$
\begin{aligned}
& \mathcal{R} \models progress_{\bullet t \bullet}(\phi_t) \\
\curvearrowright\ & \exists p \in {}^\bullet t \forall i \in \mathbb{N} \exists r \in T_{\mathcal{R}} \colon H_p(i) \rightarrow r(p) = i && \text{(Lemma 6)} \\
\curvearrowright\ & \exists p \in {}^\bullet t \forall i \in \mathbb{N} \exists s \in T_R \colon (p,i) \in P_{\mathcal{C}} \rightarrow s(p) = i \\
\curvearrowright\ & \exists p \in {}^\bullet t \forall a \in l^{-1}(p) \exists s \in T_{\mathcal{C}} \colon a F_{\mathcal{C}} s \\
\curvearrowright\ & \exists p \in {}^\bullet t \forall a \in l^{-1}(p) \exists s \in T_{\mathcal{C}} \colon s \in a^\bullet \\
\curvearrowright\ & \exists p \in {}^\bullet t \forall a \in l^{-1}(p) \colon a^\bullet \neq \emptyset \\
\curvearrowright\ & \exists p \in {}^\bullet t \forall a \colon l(a) = p \rightarrow a^\bullet \neq \emptyset \\
\curvearrowright\ & \exists p \in {}^\bullet t \neg \exists a \colon l(a) = p \wedge a^\bullet \neq \emptyset \\
\curvearrowright\ & \exists p \in {}^\bullet t \colon \neg p \in \{l(a) \mid a \in P_{\mathcal{C}} \wedge a^\bullet \neq \emptyset\} \\
\curvearrowright\ & \exists p \in {}^\bullet t \colon \neg p \in l(\{a \mid a \in P_{\mathcal{C}} \wedge a^\bullet \neq \emptyset\}) \\
\curvearrowright\ & \exists p \in {}^\bullet t \colon p \notin l(\mathcal{C}^\circ) \\
\curvearrowright\ & {}^\bullet t \not\subseteq l(\mathcal{C}^\circ) \\
\curvearrowright\ & l(\mathcal{C}^\circ) \text{ aktiviert nicht } t
\end{aligned}
$$

Zweiter Teil des Beweises von Satz 2

Sei $\mathcal{C}$ ein verteilter Ablauf mit $\mathcal{C} \models_l \Sigma$. Zu zeigen ist:

$$\exists \mathcal{R}\colon \mathcal{R} \models \Phi_\Sigma \wedge \mathcal{R} \simeq \Sigma$$

Schritte:

1. Konstruiere $\mathcal{R}$, und
2. zeige: $\mathcal{R} \simeq \mathcal{C}$.
3. Zeige: $\mathcal{R} \models \Phi_\Sigma$.

1. Schritt

Sei $g\colon T_\mathcal{C} \to \mathrm{Abb}(D, \mathbb{N})$, $D \subseteq P_\Sigma$ eine Abbildung von $T_\mathcal{C}$ in die Menge der Abbildungen von Teilmengen von P_Σ nach $\mathbb{N}$ mit:

$$g(t)\colon {}^\bullet l(t)^\bullet \to \mathbb{N}$$
$$g(t)(x) = \min\{i \in \mathbb{N} \mid \forall s < t, x \in {}^\bullet l(s)^\bullet\colon g(s)(x) < i\}$$

Die folgenden Propositionen werden später verwendet.

Proposition 14. *Für alle $t \in T_\mathcal{C}$ ist $g(t) \neq \emptyset$.*

Beweis von Propostion 14. Für alle $t \in T_\mathcal{C}$ ist ${}^\bullet t^\bullet \neq \emptyset$ □

Proposition 15. *Seien $s, t \in T_\mathcal{C}$ und $p \in P_\Sigma$. Es gilt*

$$x \in \mathrm{Inv}(g(s)) \wedge x \in \mathrm{Inv}(g(t)) \quad \Rightarrow \quad (s = t) \vee (s < t) \vee (t < s)$$

Beweis von Proposition 15. Die Aussage folgt als Korollar unmittelbar aus Proposition 8. □

Proposition 16. *Seien $s, t \in T_\mathcal{C}$ und $p \in P_\Sigma$. Es gilt*

(i) $g(s)(p) + 1 = g(t)(p) \wedge p \in {}^\bullet l(t) \quad \Rightarrow \quad p \in l(s)^\bullet$

(ii) $g(s)(p) + 1 = g(t)(p) \wedge p \in l(s)^\bullet \quad \Rightarrow \quad p \in {}^\bullet l(t)$

Beweis von Proposition 16. Seien $s, t \in T_\mathcal{C}$ und $p \in P_\Sigma$. Um i. zu zeigen, sei $g(s)(p) + 1 = g(t)(p)$ und $p \in {}^\bullet l(t)$. Nach Definition von g folgt $p \in {}^\bullet l(s)^\bullet$. Da nach Voraussetzung $p \in {}^\bullet l(t)^\bullet$ gilt nach Proposition 8 $s < t \vee t < s \vee s = t$. Zusammen mit $g(s)(p) < g(t)(p)$ folgt $s < t$.

Wegen $g(s)(p) + 1 = \min\{i \in \mathbb{N} \mid \forall u < t, p \in {}^\bullet l(u)^\bullet\colon g(u)(p) < i\}$ erhält man insgesamt:

$$p \in {}^\bullet l(s)^\bullet \wedge p \in {}^\bullet l(t) \wedge s < t \wedge (\nexists u \in T_\mathcal{C}\colon s < u < t \wedge p \in {}^\bullet l(u)^\bullet)$$

Mit Proposition 9 folgt $p \in l(s)^\bullet$.

Der Beweis von ii. geht analog. □

Proposition 17. *Seien $s,t \in T_{\mathcal{C}}$ und $p \in P_\Sigma$. Es gilt*

$$g(s)(p) = g(t)(p) \quad \Rightarrow \quad s = t$$

Beweis von Proposition 17. Seien $s,t \in T_{\mathcal{C}}$ und $p \in P_\Sigma$ und $g(s)(p) = g(t)(p)$. Nach Defintion von g gilt:

$$\begin{aligned} p \in {}^\bullet l(s)^\bullet \wedge p \in {}^\bullet l(t)^\bullet \wedge \min\{i \in \mathbb{N} \mid \forall u < s, p \in {}^\bullet l(u)^\bullet \colon g(u)(p) < i\} \\ = \min\{i \in \mathbb{N} \mid \forall u < t, p \in {}^\bullet l(u)^\bullet \colon g(u)(p) < i\} \end{aligned}$$

Hieraus folgt unmittelbar

$$p \in {}^\bullet l(s)^\bullet \wedge p \in {}^\bullet l(t)^\bullet \wedge (\neg t < s \wedge \neg s < t)$$

Wegen Propostion 8 folgt

$$(s < t \vee t < s \vee s = t) \wedge (\neg t < s \wedge \neg s < t)$$

Somit gilt $s = t$. □

Proposition 18. *g ist injektiv.*

Beweis von Proposition 18. Sei $s,t \in T_{\mathcal{C}}$ und $g(s) = g(t)$. Wegen Proposition 14 existiert ein $p \in P_\Sigma$ mit $g(s)(p) = g(t)(p)$. Mit Proposition 17 folgt $s = t$. □

Im Folgenden definiere ich Histories zu den Plätzen von Σ.

Sei $(H_x)_{x \in P_\Sigma}$ eine P_Σ-induzierte Familie von Folgen von Wahrheitswerten, d.h. $(H_x)_{x \in P_\Sigma}$ sind einstellige Prädikate über "Präfixen" von $\mathbb{N}$. Die jeweilige Länge dieser (ggf. unendlichen) "Präfixe" wird mit $l(H_x)$ bezeichnet. Dabei sei

$$l(H_x) = \max\{i \in \mathbb{N} \mid \exists t \in T_{\mathcal{C}} \colon g(t)(x) = i - 2\} \cup \{1\}$$

$$H_x(i) \text{ gdw. } \begin{cases} x \in I_\Sigma & \text{, für } i = 0 \\ \exists t \in T_{\mathcal{C}} \colon g(t)(x) = i \wedge x \in {}^\bullet l(t) \\ \vee \; \exists t \in T_{\mathcal{C}} \colon g(t)(x) + 1 = i \wedge x \in l(t)^\bullet & \text{, für } 0 < i < l(H_x) \\ \text{nicht definiert} & \text{, sonst} \end{cases}$$

(Die zweite Alternative im Fall $0 < i < l(H_x)$ wird für Plätze mit leerem Nachbreich benötigt.)

Ich setze $Var = P_\Sigma$, $T_{\mathcal{R}} = g(T_{\mathcal{C}})$ und $\mathcal{R} = (H, T_{\mathcal{R}})$ und werde zeigen:

Proposition 19. *$\mathcal{R}$ ist ein Run über der Variablenmenge Var.*

Um Proposition 19 zu beweisen zeige ich zunächst:

Proposition 20. *Sei $s,t \in T_{\mathcal{C}}$. Es gilt*

$$s < t \text{ gdw. } g(s) \prec g(t)$$

Beweis von Propostione 20. Seien $q,r \in T_{\mathcal{R}}$. Aufgrund der Injektivität von g genügt zu zeigen, dass $q \prec r$ genau dann gilt, wenn $g^{-1}(q) < g^{-1}(r)$.

Sei nun $g^{-1}(q) < g^{-1}(r)$. Dann existieren Plätze $p_0, \ldots, p_n \in P_{\mathcal{C}}$ und Transitionen $t_1, \ldots, t_n \in T_{\mathcal{C}}$, so dass gilt

$$g^{-1}(q) F_{\mathcal{C}} p_0 F_{\mathcal{C}} t_1 F_{\mathcal{C}} p_1 F_{\mathcal{C}} t_2 F_{\mathcal{C}} \ \ldots \ t_n F_{\mathcal{C}} p_n F_{\mathcal{C}} g^{-1}(r)$$

daraus folgt

$$\begin{aligned} & p_0 \in g^{-1}(q)^\bullet \wedge p_0 \in {}^\bullet t_1 \\ \wedge\ & p_1 \in t_1^\bullet \wedge p_1 \in {}^\bullet t_2 \\ & \vdots \\ \wedge\ & p_n \in t_n^\bullet \wedge p_n \in {}^\bullet g^{-1}(r) \end{aligned}$$

und weiter nach Defintion von g

$$q(p_0) + 1 = g(t_1)(p_0) \ \wedge\ g(t_1)(p_1) + 1 = g(t_2)(p_1) \ \wedge\ \ldots \ \wedge\ g(t_n)(p_n) + 1 = r(p_n)$$

nach Definition von $\prec$ gilt

$$q \prec g(t_1) \prec g(t_2) \prec \ldots \prec g(t_n) \prec r$$

und somit erhält man

$$q \prec r$$

Die Rückrichtung ergibt sich, indem man den Beweis zeilenweise von unten nach oben ließt. □

Beweis von Proposition 19. Zu zeigen ist:

1. Für alle $x \in Var$ mit $0 \leq i < l(H_x) - 1$ existiert genau ein $t \in T_\mathcal{R}$, so dass $t(x) = i$.
2. Für alle $t \in Var$ und $x \in \mathrm{Inv}(t)$ ist $0 \leq t(x) < l(H_x) - 1$.
3. $\prec |_{T_\mathcal{R} \times T_\mathcal{R}}$ ist irreflexiv.

zu 1: Sei $x \in Var$ mit $0 \leq i < l(H_x)-1$. Es gilt also $x \in l(P_\mathcal{C})$ und $l(H_x) \geq i+2 \geq 2$. Nach Definition von $l(H_x)$ existiert also ein $t \in T_\mathcal{C}$ mit $g(t)(x) \geq i$ und nach Defintion von g muß dann auch ein $t \in T_\mathcal{C}$ existieren mit $g(t)(x) = i$. Sei nun $r \in T_\mathcal{R}$ mit $r = g(t)$, dann ist $r(x) = i$. Damit ist die Existenzaussage gezeigt. Die Eindeutigkeit folgt nun unmittelbar aus Proposition 17.

zu 2: Nach Definition von $l(H_x)$ ist

$$l(H_x) = \max\{i \in \mathbb{N} \mid \exists t \in T_\mathcal{C} \colon g(t)(x) = i - 2\} \cup \{1\}$$

Sei nun $t \in T_\mathcal{C}$ so gewählt, dass $g(t)(x)$ maximal. Dann maximiert $g(t) \in T_\mathcal{R}$ den Wert von x für alle $r \in T_\mathcal{R}$ und es gilt $l(H_x) \geq g(t)(x)+2$ und somit $t(x) < l(H_x)-1$.

zu 3: Da $<_\mathcal{C}$ nach Definition azyklisch ist, ist nach Proposition 19 $\prec_\mathcal{R}$ ebenfalls azyklisch.

Somit ist gezeigt, dass $\mathcal{R}$ ein Run ist. □

2. Schritt

Zu zeigen ist $\mathcal{R} \simeq \mathcal{C}$, d.h., dass eine Bijektion $f\colon T_{\mathcal{R}} \to T_{\mathcal{C}}$ existiert, mit

1. $\mathrm{eff}_{\mathcal{R}}(t) = \mathrm{eff}^{l}_{\mathcal{C}}(f(t))$, für alle $t \in T_{\mathcal{R}}$ und
2. $s \prec_{\mathcal{R}} t \Leftrightarrow f(s) <_{\mathcal{C}} f(t)$, für alle $s, t \in T_{\mathcal{R}}$.
3. $C_0(\mathcal{R}) = \{p \in Var \mid H_p(0)\}$

Im Folgenden sei $f = (g|_{T_{\mathcal{C}}})^{-1}$. Aus der Injetivität von g folgt unmittelbar die Bijektivität von f.

zu 1: Da ich das folgende Argument später noch einmal benötigen werde, formuliere ich zunächst folgende Proposition:

Proposition 21. *Sei $r \in T_{\mathcal{R}}$ und $x \in Var$. Es gilt*

(i) $H_x(r(x)) \quad \Leftrightarrow \quad x \in {}^\bullet l(f(r))$

(ii) $H_x(r(x)+1) \quad \Leftrightarrow \quad x \in l(f(r))^\bullet$

Beweis von Proposition 21. Sei $r \in T_{\mathcal{R}}$ und $x \in Var$. Im Falle $r(x) = 0$ gilt $H_x(r(x)) \Leftrightarrow x \in I_\Sigma$. Nach Definition von I_Σ gilt dies genau dann, wenn ein $p \in P_{\mathcal{C}}$ existiert mit

$$l(p) = x \wedge {}^\bullet p = \emptyset \qquad (*)$$

Weiterhin existiert wegen $x \in {}^\bullet l(f(r))^\bullet$ (da $r(x)$) ein $q \in P_{\mathcal{C}}$ mit $l(q) = x \wedge q \in {}^\bullet f(r)^\bullet$. Aus $l(p) = x = l(q)$ folgt $(p < q) \vee (q < p) \vee (p = q)$ und wegen $(*)$ folgt $p \leq q$. Wenn $p = q$ gilt wegen $(*)$, dass $p \in {}^\bullet f(r)$ und somit $x \in {}^\bullet l(f(r))$. Wenn $p < q$ folgt $p < f(r)$, da im Vorbreich von q genau eine Transition existiert. Da $r(x) = 0$, existiert keine Transition $s \in T_{\mathcal{C}}$ mit $x \in {}^\bullet l(s)^\bullet$ und $p < s < f(r)$. Nach Proposition 10 folgt $x \in {}^\bullet l(f(r))$. Umgekehrt gilt: Aus $x \in {}^\bullet f(r)$ und $r(x) = 0$ folgt, dass ein $p \in P_{\mathcal{C}}$ mit leerem Vorbereich existiert, mit $l(p) = x$. Somit gilt $H_p(r(x))$. $r(x) + 1 = 0$ kann für den Fall $r(x) = 0$ nicht eintreten.

Im Falle $r(x) > 0$ gilt:

$$\begin{aligned}
&H_x(r(x)) \\
&\quad\Leftrightarrow \quad \vee \begin{array}{l} \exists t \in T_{\mathcal{C}}\colon g(t)(x) = r(x) \wedge x \in {}^\bullet l(t) \\ \exists t \in T_{\mathcal{C}}\colon g(t)(x) + 1 = r(x) \wedge x \in l(t)^\bullet \end{array} \\
&\quad\curvearrowright \quad \vee \begin{array}{l} \exists t \in T_{\mathcal{C}}\colon g(t) = r \wedge x \in {}^\bullet l(t) \\ \exists t \in T_{\mathcal{C}}\colon g(t)(x) + 1 = g(f(r))(x) \wedge x \in l(t)^\bullet \end{array} && \text{(Prop. 17, Def. } g, f\text{)} \\
&\quad\curvearrowright \quad x \in {}^\bullet l(f(r)) && \text{(Def. } g, f\text{, Prop. 16)} \\
&\quad\curvearrowright \quad \exists t \in T_{\mathcal{C}}\colon g(t) = r \wedge x \in {}^\bullet l(t) \\
&\quad\curvearrowright \quad \exists t \in T_{\mathcal{C}}\colon g(t)(x) = r(x) \wedge x \in {}^\bullet l(t) \\
&\quad\curvearrowright \quad H_x(r(x))
\end{aligned}$$

Somit gilt:

$$H_x(r(x)) \quad \Leftrightarrow \quad x \in {}^\bullet l(f(r))$$

Ebenso gilt:

$$
\begin{aligned}
& H_x(r(x)+1) \\
& \quad \Leftrightarrow \quad \vee \begin{array}{l} \exists t \in T_{\mathcal{C}} \colon g(t)(x) = r(x)+1 \wedge x \in {}^\bullet l(t) \\ \exists t \in T_{\mathcal{C}} \colon g(t)(x)+1 = r(x)+1 \wedge x \in l(t)^\bullet \end{array} \\
& \quad \curvearrowright \quad \vee \begin{array}{l} \exists t \in T_{\mathcal{C}} \colon g(t)(x) = g(f(r))(x)+1 \wedge x \in {}^\bullet l(t) \\ \exists t \in T_{\mathcal{C}} \colon g(t) = r \wedge x \in l(t)^\bullet \end{array} && \text{(Def. } g, f\text{, Prop. 17)} \\
& \quad \curvearrowright \quad x \in l(f(r))^\bullet && \text{(Prop. 16, Def. } g, f\text{)} \\
& \quad \curvearrowright \quad \exists t \in T_{\mathcal{C}} \colon g(t) = r \wedge x \in l(t)^\bullet \\
& \quad \curvearrowright \quad \exists t \in T_{\mathcal{C}} \colon g(t)(x)+1 = r(x)+1 \wedge x \in l(t)^\bullet \\
& \quad \curvearrowright \quad H_x(r(x))
\end{aligned}
$$

Somit gilt:

$$H_x(r(x)+1) \quad \Leftrightarrow \quad x \in l(f(r))^\bullet$$

□

Mithilfe dieser Proposition ist die Behauptung nun leicht zu zeigen:

$$\mathrm{eff}_{\mathcal{R}}(r,x) = \begin{cases} \big(H_x(r(x)), H_x(r(x)+1)\big) & \text{, falls } x \in \mathrm{Inv}(r) \\ \text{nicht definiert} & \text{, sonst} \end{cases}$$

Da $x \in \mathrm{Inv}(r) \Leftrightarrow x \in {}^\bullet f(r)^\bullet$, gilt nach Proposition 21:

$$\begin{aligned} \mathrm{eff}_{\mathcal{R}}(r,x) &= \begin{cases} \big(x \in {}^\bullet l(f(r)), x \in l(f(r))^\bullet\big) & \text{, falls } x \in {}^\bullet f(r)^\bullet \\ \text{nicht definiert} & \text{, sonst} \end{cases} \\ &= \mathrm{eff}_{\mathcal{C}}(f(r),x) \end{aligned}$$

Es folgt: $\mathrm{eff}_{\mathcal{R}}(r) = \mathrm{eff}^l_{\mathcal{C}}(f(r))$.

zu 2: Wurde bereits mit Proposition 20 gezeigt.

zu 3: Folgt unmittelbar aus der Definition von $\mathcal{R}$.

3. Schritt

Sei f wie im 2. Schritt definiert.

Zu zeigen ist $\mathcal{R} \models \Phi_\Sigma$. Nach Definition von Φ_Σ ist zu zeigen:

1. $\mathcal{R} \models \phi_{init}$
2. $\mathcal{R} \models \bigwedge_{p \in P_\Sigma} \Box \phi_p$
3. $\mathcal{R} \models \phi_{prog}$

zu 1: Zu zeigen ist

$$(C_0(\mathcal{R}), C_0'(\mathcal{R}), I_{C_0(\mathcal{R})}) \models \bigwedge_{p \in I_\Sigma} p \wedge \bigwedge_{p \notin I_\Sigma} \neg p \qquad (*)$$

Der Wert einer ungestrichenen Variable p wird in $(C_0(\mathcal{R}), C_0'(\mathcal{R}), I_{C_0(\mathcal{R})})$ zu $wahr$ evaluiert genau dann, wenn $H_p(C_0(\mathcal{R}))$ gilt. Nach Definition von C_0 ist $wert_{C_0(\mathcal{R})}(p) = wahr \Leftrightarrow H_p(0)$. Nach Definition von H gilt:

$$wert_{C_0(\mathcal{R})}(p) = wahr \quad \Leftrightarrow \quad p \in I_\Sigma$$

Somit gilt $(*)$.

zu 2: Sei $p \in P_\Sigma$. Zu zeigen ist für jedes Suffix $\mathcal{R}'$ von $\mathcal{R}$:

$$S \models \Box(\widetilde{p} \rightarrow \bigvee_{t \in {}^\bullet p^\bullet} \phi_t), \quad \text{wobei } S = (C, C', I_C) \text{ Anfangsschritt von } \mathcal{R}' \text{ ist.}$$

Sei $wert_S(\widetilde{p}) = wahr$. Dann ist $\{p\} \in I_C$. Also existiert ein $r \in T_C$ mit $p \in \mathrm{Inv}(r)$. Nach Definition von $\mathcal{R}$ und f folgt $p \in {}^\bullet l(f(r))^\bullet$. Es genügt also zu zeigen, dass $wert_S(\phi_{l(f(r))}) = wahr$, d.h.

$$S \models \left(\bigwedge_{p \in {}^\bullet l(f(r))} p \right) \wedge \left(\bigwedge_{p \in {}^\bullet l(f(r)) \setminus l(f(r))^\bullet} \neg p' \right) \wedge \left(\bigwedge_{p \in l(f(r))^\bullet} p' \right) \wedge \text{closed} \left(\widetilde{{}^\bullet l(f(r))^\bullet}, P_\Sigma \right)$$

Dies kann leicht für die einzelnen Elemente der Konjuktion gezeigt werden:

Für $p \in Var$ gilt:

$$\begin{array}{lll} & wert_S(p) = wahr & \\ \Leftrightarrow & H_p(C(p)) & \\ \Leftrightarrow & H_p(r(p)) & (\text{da } r \text{ nach [Ale02] eindeutig bestimmt ist}) \\ \Leftrightarrow & p \in {}^\bullet l(f(r)) & (\text{Prop. 21}) \end{array}$$

Für $p' \in Var'$ gilt:

$$\begin{array}{lll} & wert_S(p') = wahr & \\ \Leftrightarrow & H_p(C'(p)) & \\ \Leftrightarrow & H_p(r(p)+1) & (\text{da } r \text{ nach [Ale02] eindeutig bestimmt ist}) \\ \Leftrightarrow & p \in l(f(r))^\bullet & (\text{Prop. 21}) \end{array}$$

und es gilt weiterhin

$$\begin{array}{lll} & wert_S(p') = false & \\ \Leftrightarrow & nicht\ wert_S(p') = wahr & \\ \Leftrightarrow & p \notin l(f(r))^\bullet & \\ \Leftrightarrow & p \in {}^\bullet l(f(r)) \setminus l(f(r))^\bullet & (\text{da } p \in {}^\bullet l(f(r))^\bullet) \end{array}$$

Wegen $\mathrm{Inv}(r) = {}^\bullet l(f(r))^\bullet$ exitiert keine echte Übermenge von ${}^\bullet l(f(r))^\bullet$ in I_C. Somit gilt schließlich auch $\text{closed} \left(\widetilde{{}^\bullet l(f(r))^\bullet}, P_\Sigma \right)$.

zu 3: Sei $t \in Pr_\Sigma$. Es folgt:

$$
\begin{aligned}
& l(\mathcal{C}^\circ) \text{ aktiviert nicht } t \\
\curvearrowright\ & {}^\bullet t \not\subseteq l(\mathcal{C}^\circ) \\
\curvearrowright\ & \exists p \in {}^\bullet t\colon p \notin l(\mathcal{C}^\circ) \\
\curvearrowright\ & \exists p \in {}^\bullet t \neg \exists a \in P_\mathcal{C}\colon l(a) = p \wedge a \in \mathcal{C}^\circ \\
\curvearrowright\ & \exists p \in {}^\bullet t \forall a \in l^{-1}(p)\colon a \notin \mathcal{C}^\circ \\
\curvearrowright\ & \exists p \in {}^\bullet t \forall a \in l^{-1}(p) \exists c \in T_\mathcal{C}\colon a \in {}^\bullet c
\end{aligned}
$$

Sei nun $p \in {}^\bullet t$ mit

$$\forall a \in l^{-1}(p) \exists c \in T_\mathcal{C}\colon a \in {}^\bullet c \qquad (*)$$

Sei $i \in \mathbb{N}$, so dass $H_p(i)$. Dann gilt nach Definition von H einer der drei folgenden Fälle:

(i) $i = 0 \wedge p \in I_\Sigma$

(ii) $0 < i < l(H_p) \wedge \exists d \in T_\mathcal{C}\colon g(d)(p) = i \wedge p \in {}^\bullet l(d)$

(iii) $0 < i < l(H_p) \wedge \exists d \in T_\mathcal{C}\colon g(d)(p) = i + 1 \wedge p \in l(d)^\bullet$

zu i:

$$
\begin{aligned}
& i = 0 \wedge p \in I_\Sigma \\
\curvearrowright\ & \exists a \in P_\mathcal{C}\colon l(a) = p \wedge a \in {}^\circ\mathcal{C} \\
\curvearrowright\ & \exists a \in l^{-1}(p) \exists c \in T_\mathcal{C}\colon a \in {}^\circ\mathcal{C} \wedge a \in {}^\bullet c && \text{(wegen } (*)\text{)} \\
\curvearrowright\ & \exists a \in l^{-1}(p) \exists c \in T_\mathcal{C}\colon {}^\bullet a = \emptyset \wedge p \in {}^\bullet l(c)^\bullet \\
\curvearrowright\ & \exists c \in T_\mathcal{C} \neg \exists e \in T_\mathcal{C}\colon e < c \wedge p \in {}^\bullet l(c)^\bullet \\
\curvearrowright\ & \exists c \in T_\mathcal{C}\colon g(c)(p) = 0 && \text{(Def. von } g\text{)} \\
\curvearrowright\ & \exists r \in T_\mathcal{R}\colon r(p) = i
\end{aligned}
$$

zu ii:

$$
\begin{aligned}
& \exists d \in T_\mathcal{C}\colon g(d)(p) = i \wedge p \in {}^\bullet l(d) \\
\curvearrowright\ & \exists r \in T_\mathcal{R}\colon r(p) = i
\end{aligned}
$$

zu iii:

$$
\begin{aligned}
& \exists d \in T_{\mathcal{C}} \colon g(d)(p) = i + 1 \wedge p \in l(d)^\bullet \\
\curvearrowright\ & \exists d \in T_{\mathcal{C}} \colon g(d)(p) = i + 1 \wedge (\exists a \in P_{\mathcal{C}} \colon l(a) = p \wedge a \in d^\bullet) \\
\curvearrowright\ & \exists a \in l^{-1}(p) \exists d \in T_{\mathcal{C}} \exists c \in T_{\mathcal{C}} \colon g(d)(p) = i + 1 \wedge a \in d^\bullet \wedge a \in {}^\bullet c && \text{(wegen } (*)\text{)} \\
\curvearrowright\ & \exists a \in l^{-1}(p) \exists c, d \in T_{\mathcal{C}} \colon g(d)(p) = i + 1 \wedge p \in {}^\bullet l(c) \\
& \qquad \wedge (\neg \exists e \in T_{\mathcal{C}} \colon d < e < c \wedge a \in {}^\bullet e^\bullet) && \text{(da Vor- und Nachbereich von } a \text{ eindeutig)} \\
\curvearrowright\ & \exists a \in l^{-1}(p) \exists c, d \in T_{\mathcal{C}} \colon g(d)(p) = i + 1 \wedge p \in {}^\bullet l(c)^\bullet \\
& \qquad \wedge (\neg \exists e \in T_{\mathcal{C}} \colon d < e < c \wedge p \in {}^\bullet l(e)^\bullet) && \text{(da nebenläufige Elemente unterschiedlich gelabelt)} \\
\curvearrowright\ & \exists c, d \in T_{\mathcal{C}} \colon g(d)(p) = i + 1 \wedge g(c)(p) = i && \text{(Def. von } g\text{)} \\
\curvearrowright\ & \exists c \in T_{\mathcal{C}} \colon g(c)(p) = i \\
\curvearrowright\ & \exists r \in T_{\mathcal{R}} \colon r(p) = i
\end{aligned}
$$

Zusammenfassend gilt also

$$\exists p \in {}^\bullet t \forall i \in \mathbb{N} \exists r \in T_{\mathcal{R}} \colon H_p(i) \rightarrow r(p) = i$$

Nach Lemma 6 folgt $\mathcal{R} \models \mathit{progress}_{\bullet t \bullet}(\phi_t)$.

Damit ist Satz 2 bewiesen.

Literatur

[Ale02] Adrianna Alexander. The temporal logic of distributed actions. Working draft zu TLDA, 2002.

[ALM96] M. Abadi, L. Lamport, and S. Merz. A TLA Solution to the RPC-Memory specification problem. In M. Broy, S. Merz, and K. Spies, editors, *Formal System Specification: The RPC-Memory specification case study*, volume 1169, pages 21–66. Springer-Verlag, Berlin, 1996.

[Rei98] Wolfgang Reisig. *Elements of Distributed Algorithms. Modeling and Analysis with Petri Nets.* Springer, 1998.

[WWV+97] Michael Weber, Rolf Walter, Hagen Völzer, Tobias Vesper, Wolfgang Reisig, Sibylle Peuker, Ekkart Kindler, Jörn Freiheit, and Jörg Desel. Dawn. petrinetzmodelle zur verifikation verteilter algorithmen. Informatik-Berichte 88, Humboldt-Universität zu Berlin, Berlin, 1997.