Ludwig-Maximilians-Universität München
Institut für Informatik
Prof. Dr. F. Kröger, M. Hammer

WS 2006/2007
Übungsblatt 9

Temporale Logik und Zustandssysteme Lösungsvorschlag

Aufgabe 9-1 **McCarthy's 91-Funktion** (keine Abgabe)

Gegeben sei die Signatur SIG mit den Sorten NAT und $PAAR$, den Konstanten $0, 1, 2, \ldots$ von der Sorte NAT, den zweistelligen Funktionszeichen $+^{(NAT\ NAT, NAT)}$, $-^{(NAT\ NAT, NAT)}$ und $\langle \_, \_ \rangle^{(NAT\ NAT, PAAR)}$ sowie den zweistelligen Prädikatszeichen $\leq^{(NAT\ NAT)}$ und $\preceq^{(PAAR\ PAAR)}$. Wir verwenden Infixschreibweise; $s > t$ steht für $\neg(t \leq s)$. In der Struktur S werde die Sorte NAT durch die Menge $\mathbb{N}$ der natürlichen Zahlen, die Sorte $PAAR$ durch die Menge $\mathbb{N} \times \mathbb{N}$ von Paaren natürlicher Zahlen, $+$, $-$ und $\leq$ wie üblich (mit $m - n = 0$, falls $n > m$) und $\langle \_, \_ \rangle$ durch die Paarfunktion interpretiert. Die Interpretation von $\preceq$ wird unten angegeben.

Wir untersuchen das rSTS $\Gamma = (X, V, Z, T, start)$ mit den Systemvariablen $X_{NAT} = \{a, d\}$, $X_{PAAR} = V = \emptyset$, der vollen Zustandsmenge Z, der Transitionsrelation T mit

$$(\eta, \eta') \in T \quad \Longleftrightarrow \quad \left\{ \begin{array}{ll} \eta'(a) = \eta(a) + 11 \text{ und } \eta'(d) = \eta(d) + 1 & \text{falls } \eta(a) \leq 100 \text{ und } \eta(d) > 0 \\ \eta'(a) = \eta(a) - 10 \text{ und } \eta'(d) = \eta(d) - 1 & \text{falls } \eta(a) > 100 \text{ und } \eta(d) > 0 \\ \eta' = \eta & \text{sonst} \end{array} \right\}$$

und der Anfangsbedingung $start \equiv d = 1$. Zu beweisen ist, dass die Formel $\Diamond(d = 0)$ Γ-gültig ist.

Für den Beweis definieren wir die Interpretation von $\prec$ auf Paaren natürlicher Zahlen wie folgt: $(m_1, n_1) \prec (m_2, n_2)$ gilt genau dann, wenn eine der folgenden Bedingungen erfüllt ist:

1. $m_2 < 91$ und $m_2 < m_1$ oder
2. $91 \leq m_1, m_2 \leq 111$ und es gilt
   (a) $n_1 = n_2 + 1$ und $m_1 \geq m_2 + 11$ oder
   (b) $m_1 \geq m_2$ und $n_1 = n_2$ oder
   (c) $n_1 < n_2 - 1$ oder
   (d) $n_1 = n_2 - 1$ und $m_1 \geq m_2 - 10$.

a) Geben Sie eine axiomatische FOLTL-Spezifikation $\mathcal{A}$ von Γ an.

Lösung: Diese Funktion ist bekannt als (John) McCarthy's 91-Funktion und liefert für alle Argumente $a \leq 101$ das Ergebnis 91. In dieser Aufgabe benutzen wir die Technik der fundierten Ordnungen zum Beweis der Terminierung der 91-Funktion.

Die Abläufe von Γ werden charakterisiert durch die folgende Axiomenmenge $\mathcal{A}$:

(data) alle S-gültigen Formeln (insbes. Arithmetik mit $+$, $-$, $\leq$, Paarbildung, Aussagen über $\preceq$)

$(F1)$ $a \leq 100 \wedge d > 0 \rightarrow a' = a + 11 \wedge d' = d + 1$

$(F2)$ $a > 100 \wedge d > 0 \rightarrow a' = a - 10 \wedge d' = d - 1$

$(F0)$ $d = 0 \rightarrow a' = a \wedge d' = d$

(root) $\mathbf{init} \rightarrow start$

b) Beweisen Sie, dass $\prec$ eine fundierte Relation auf $\mathbb{N} \times \mathbb{N}$ ist.

Lösung: Wir zeigen eine stärkere Aussage: $\preceq$ (definiert wie üblich) ist eine fundierte Ordnung, d.h., $\preceq$ ist reflexiv, antisymmetrisch und transitiv.

1. Die Reflexivität folgt unmittelbar aus der Definition.
2. Antisymmetrie: Es gelte $(m_1, n_1) \preceq (m_2, n_2)$ und $(m_2, n_2) \preceq (m_1, n_1)$, zu zeigen: $(m_1, n_1) = (m_2, n_2)$. Falls nicht, müsste eine der Bedingungen (1) oder (2a)–(2d) erfüllt sein.

- Fall: $m_2 < 91$ und $m_2 < m_1$. Ist $m_1 < 91$, so müsste $m_1 < m_2$ gelten, Widerspruch. Ist $m_1 \geq 91$, so müsste wegen der Annahme $(m_2, n_2) \preceq (m_1, n_1)$ auch $m_2 \geq 91$ gelten, Widerspruch.
- Fall: $91 \leq m_1, m_2 \leq 111$. Wir unterscheiden, ausgehend von der Annahme $(m_1, n_1) \preceq (m_2, n_2)$, die Fälle (2a)–(2d):
  - $n_1 = n_2 + 1$ und $m_1 \geq m_2 + 11$. Es folgt $n_2 = n_1 - 1$ und somit (wegen $(m_2, n_2) \preceq (m_1, n_1)$) weiter $m_2 \geq m_1 - 10$, also $m_2 + 11 \leq m_1 \leq m_2 + 10$, Widerspruch.
  - $m_1 \geq m_2$ und $n_1 = n_2$. Dann muss auch $m_2 \geq m_1$ gelten, also folgt die Behauptung.
  - $n_1 < n_2 - 1$. Dann ist $n_2 > n_1 + 1$, und daher kann nicht $(m_2, n_2) \preceq (m_1, n_1)$ gelten, Widerspruch.
  - $n_1 = n_2 - 1$ und $m_1 \geq m_2 - 10$. Symmetrisch zum ersten Teilfall.

3. Transitivität: Es gelte $(m_1, n_1) \preceq (m_2, n_2) \preceq (m_3, n_3)$, zu zeigen ist $(m_1, n_1) \preceq (m_3, n_3)$. Ist $(m_1, n_1) = (m_2, n_2)$ oder $(m_2, n_2) = (m_3, n_3)$, so ist die Behauptung trivial. Daher nehmen wir im folgenden an, dass die Bedingungen (1) oder (2) erfüllt sind und unterscheiden, ausgehend von der Annahme $(m_1, n_1) \preceq (m_2, n_2)$ die verschiedenen Fälle:
   - Fall: $m_2 < 91$. Dann ist $m_2 < m_1$. Es gilt $(m_2, n_2) \preceq (m_3, n_3)$, und hier muss $m_3 < 91$ gelten, da sonst auch $m_2 \geq 91$ folgte. Also gilt $m_3 < m_2$ und damit auch $m_3 < m_1$ bzw. $(m_1, n_1) \preceq (m_3, n_3)$.
   - Fall: $91 \leq m_1, m_2 \leq 111$. Aus $(m_2, n_2) \preceq (m_3, n_3)$ und der Definition von $\preceq$ folgt weiter $91 \leq m_3 \leq 111$. Wir unterscheiden die Teilfälle von Bedingung (2):
     - $n_1 = n_2 + 1$ und $m_1 \geq m_2 + 11$. Es folgt $91 \leq m_2 \leq 100$ und $102 \leq m_1 \leq 111$. Die Annahme $(m_2, n_2) \preceq (m_3, n_3)$ ergibt die folgenden vier Teilfälle:
       - $n_2 = n_3 + 1$ und $m_2 \geq m_3 + 11$. Dann folgte $m_2 \geq 91 + 11 = 102$, Widerspruch.
       - $n_2 = n_3$ und $m_2 \geq m_3$. Dann ist $n_1 = n_3 + 1$ und $m_1 \geq m_3 + 11$, also folgt die Behauptung.
       - $n_2 < n_3 - 1$. Dann ist $n_1 \leq n_3 - 1$ und $m_1 \geq 102 > 111 - 10 \geq m_3 - 10$, also folgt die Behauptung.
       - $n_2 = n_3 - 1$ und $m_2 \geq m_3 - 10$. Dann ist $n_1 = n_3$ und $m_1 \geq m_2 + 11 \geq m_3 - 10 + 11 \geq m_3$, also folgt die Behauptung.
     - $n_1 = n_2$ und $m_1 \geq m_2$. Wir unterscheiden dieselben Teilfälle:
       - $n_2 = n_3 + 1$ und $m_2 \geq m_3 + 11$. Dann ist $n_1 = n_3 + 1$ und $m_1 \geq m_2 \geq m_3 + 11$, also folgt die Behauptung.
       - $n_2 = n_3$ und $m_2 \geq m_3$. Dann ist $n_1 = n_3$ und $m_1 \geq m_3$, also folgt die Behauptung.
       - $n_2 < n_3 - 1$. Dann ist auch $n_1 < n_3 - 1$, also folgt die Behauptung.
       - $n_2 = n_3 - 1$ und $m_2 \geq m_3 - 10$. Dann ist $n_1 = n_3 - 1$ und $m_1 \geq m_3 - 10$, also folgt die Behauptung.
     - $n_1 = n_2$ und $m_1 \geq m_2$. Wir unterscheiden dieselben Teilfälle:
       - $n_2 = n_3 + 1$ und $m_2 \geq m_3 + 11$. Dann ist $n_1 = n_3 + 1$ und $m_1 \geq m_2 \geq m_3 + 11$, also folgt die Behauptung.
       - $n_2 = n_3$ und $m_2 \geq m_3$. Dann ist $n_1 = n_3$ und $m_1 \geq m_3$, also folgt die Behauptung.
       - $n_2 < n_3 - 1$. Dann ist auch $n_1 < n_3 - 1$, also folgt die Behauptung.
       - $n_2 = n_3 - 1$ und $m_2 \geq m_3 - 10$. Dann ist $n_1 = n_3 - 1$ und $m_1 \geq m_3 - 10$, also folgt die Behauptung.
     - $n_1 < n_2 - 1$.
       - $n_2 = n_3 + 1$ und $m_2 \geq m_3 + 11$. Wie oben folgt $91 \leq m_3 \leq 100$ und $102 \leq m_2 \leq 111$. Es gilt dann $n_1 \leq n_3 - 1$ und $m_1 \geq 91 > 100 - 10 \geq m_3 - 10$, also folgt die Behauptung.
       - $n_2 = n_3$ und $m_2 \geq m_3$. Dann ist $n_1 < n_3 - 1$.
       - $n_2 < n_3 - 1$. Dann ist $n_1 < n_3 - 1$.
       - $n_2 = n_3 - 1$ und $m_2 \geq m_3 - 10$. Dann ist $n_1 < n_3 - 1$.
     - $n_1 = n_2 - 1$ und $m_1 \geq m_2 - 10$.
       - $n_2 = n_3 + 1$ und $m_2 \geq m_3 + 11$. Dann ist $n_1 = n_3$ und $m_1 \geq m_3 + 11 - 10 \geq m_3$.
       - $n_2 = n_3$ und $m_2 \geq m_3$. Dann ist $n_1 = n_3 - 1$ und $m_1 \geq m_3 - 10$.
       - $n_2 < n_3 - 1$. Dann ist $n_1 < n_3 - 1$.
       - $n_2 = n_3 - 1$ und $m_2 \geq m_3 - 10$. Dann ist $n_1 = n_3 - 2 < n_3 - 1$.

Bleibt zu zeigen: $\preceq$ ist fundiert, d.h. es gibt keine unendliche absteigende Kette $(m_1, n_1) \succ (m_2, n_2) \succ \ldots$. Angenommen, doch:

1. Für alle i ist $m_i \leq 111$. Denn für ein Paar (m_i, n_i) mit $m_i > 111$ gibt es nach Definition kein (m_{i+1}, n_{i+1}) mit $(m_i, n_i) \succ (m_{i+1}, n_{i+1})$.
2. Es gibt ein i mit $m_i \geq 91$. Denn wäre $m_i < 91$ für alle i, so folgte nach Definition von $\prec$, dass $m_i < m_{i+1} < 91$ gilt für alle i, was nicht möglich ist.
3. Es gibt i, n, so dass für alle $j \geq i$ gilt: $91 \leq m_j \leq 111$ und $n_j \leq n$. Denn nach (1) und (2) gibt es ein i mit $91 \leq m_i \leq 111$, und aus der Annahme $(m_{i+1}, n_{i+1}) \prec (m_i, n_i)$ folgt mit der Definition von $\prec$, dass $91 \leq m_{i+1} \leq 111$ gilt, also folgt dies induktiv für alle $j \geq i$. Außerdem gilt$(m_j, n_j) \prec (m_i, n_i)$ für alle $j \geq i$ wegen der Transitivität von $\prec$, und aus der Definition von $\preceq$ folgt unmittelbar $n_j \leq n_i + 1$, also kann $n =_{\text{def}} n_i + 1$ gewählt werden.
4. Widerspruch. Denn nach (3) kommen in der gegebenen unendlichen Folge nur endlich viele verschiedene Zahlenpaare vor, also enthält sie mindestens ein Paar (m, n) mehrfach, im Widerspruch zur Irreflexivität von $\prec$.

c) Zeigen Sie, dass folgende Formel aus $\mathcal{A}$ herleitbar ist:

$$a = x \wedge d = y \wedge a \leq 111 \wedge d > 0 \rightarrow \circ(a \leq 111 \wedge (d = 0 \vee \langle a, d\rangle \prec \langle x, y\rangle))$$

Lösung: Da die Schreibweise mit gestrichenen Variablen bequemer und leicher lesbar ist, beweisen wir die äquivalente Formel

$$a \leq 111 \wedge d > 0 \rightarrow a' \leq 111 \wedge (d' = 0 \vee \langle a', d'\rangle \prec \langle a, d\rangle)$$

(1)	$a \leq 100 \wedge d > 0 \rightarrow a' = a + 11 \wedge d' = d + 1$	(F1)
(2)	$a > 100 \wedge d > 0 \rightarrow a' = a - 10 \wedge d' = d - 1$	(F2)
(3)	$a \leq 100 \rightarrow a + 11 \leq 111$	(data)
(4)	$a < 91 \rightarrow \langle a + 11, d + 1\rangle \prec \langle a, d\rangle$	(data)
(5)	$91 \leq a \wedge a \leq 100 \rightarrow \langle a + 11, d + 1\rangle \prec \langle a, d\rangle$	(data)
(6)	$a \leq 100 \rightarrow a + 11 \leq 111 \wedge \langle a + 11, d + 1\rangle \prec \langle a, d\rangle$	(3)(4)(5)
(7)	$a \leq 100 \wedge d > 0 \rightarrow a' \leq 111 \wedge \langle a', d'\rangle \prec \langle a, d\rangle$	(1)(6)
(8)	$a > 100 \wedge a \leq 111 \wedge d > 0 \rightarrow a - 10 \leq 111 \wedge \langle a - 10, d - 1\rangle \prec \langle a, d\rangle$	(data)
(9)	$100 < a \wedge a \leq 111 \wedge d > 0 \rightarrow a' \leq 111 \wedge \langle a', d'\rangle \prec \langle a, d\rangle$	(2)(8)
(10)	$a \leq 111 \wedge d > 0 \rightarrow a' \leq 111 \wedge (d' = 0 \vee \langle a', d'\rangle \prec \langle a, d\rangle)$	(7)(9)(data)

d) Folgern Sie schließlich die Behauptung $\Diamond(d = 0)$ unter Verwendung der Regel (wfr).

Lösung: Die Idee der folgenden Herleitung ist: Ausgehend von einem Startzustand (beschrieben durch die Formel $start$) wird ein Zustand mit $d = 0$ erreicht, und ab diesem Zustand ändert sich gemäß $(F0)$ der Wert von d nicht mehr.

Für den formalen Beweis benutzen wir die Regel

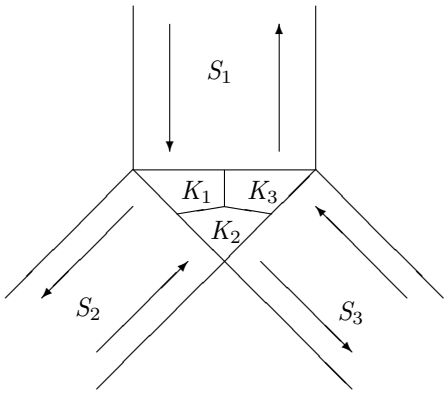
$$\text{(init)} \quad \textsf{init} \rightarrow \Box A \vdash A$$

aus Aufgabe 22 (Blatt 8), d.h. wir müssen $\textsf{init} \rightarrow \Box\Diamond(d = 0)$ beweisen. Mit Hilfe des Axioms (root) reicht es, $start \rightarrow \Box\Diamond(d = 0)$ zu beweisen. Dazu beweisen wir zunächst $start \rightarrow \Diamond(d = 0)$ und außerdem $d = 0 \rightarrow \Box(d = 0)$, was direkt aus $(F0)$ und Induktion folgt. Damit ergibt sich $start \rightarrow \Diamond\Box(d = 0)$, und die Behauptung folgt mit (T9).

Wir schreiben $A(z)$ für die Formel $\langle a, d\rangle = z \wedge a \leq 111 \wedge d > 0$.

(1)	$A(z) \rightarrow \circ(a \leq 111 \wedge (d = 0 \vee \langle a, d\rangle \prec z))$	(c)
(2)	$a \leq 111 \wedge (d = 0 \vee \langle a, d\rangle \prec z) \rightarrow d = 0 \vee \exists \bar{z}(\bar{z} \prec z \wedge A(\bar{z}))$	(pred)(data)
(3)	$A(z) \rightarrow \Diamond(d = 0 \vee \exists \bar{z}(\bar{z} \prec z \wedge A(\bar{z})))$	(1)(2)(T25)(T7)
(4)	$\exists z A(z) \rightarrow \Diamond(d = 0)$	(wfr)(3)
(5)	$a > 111 \wedge d = 1 \rightarrow d' = 0$	(F2)(data)
(6)	$a > 111 \wedge d = 1 \rightarrow \Diamond(d = 0)$	(5)(T7)
(7)	$start \rightarrow (a > 111 \wedge d = 1) \vee \exists z A(z)$	(data)
(8)	$start \rightarrow \Diamond(d = 0)$	(7)(4)(6)
(9)	$d = 0 \rightarrow \Box(d = 0)$	(F0)(pred)(ind1)
(10)	$start \rightarrow \Diamond\Box(d = 0)$	(8)(9)(T26)
(11)	$start \rightarrow \Box\Diamond(d = 0)$	(10)(T9)
(12)	$\mathbf{init} \rightarrow \Box\Diamond(d = 0)$	(11)(root)
(13)	$\Diamond(d = 0)$	(12)(init)

Aufgabe 9-2 **Straßenkreuzung** (8 Punkte)



Es soll ein rlSTS Γ zur kollisionsfreien Verkehrsführung auf der schematisch abgebildeten Straßenkreuzung durch temporallogische Formeln beschrieben werden. Als mögliche Aktionen sollen betrachtet werden ($1 \leq i \leq 3$, $\oplus$ bezeichne die Addition modulo 3):

- Ein Rechtsabbieger aus Straße S_i kommend fährt in Abschnitt K_i,
- ein Rechtsabbieger verlässt Abschnitt K_i,
- ein Linksabbieger aus Straße S_i kommend fährt in Abschnitt K_i,
- ein Linksabbieger fährt von K_i nach $K_{i\oplus 1}$,
- ein Linksabbieger verlässt $K_{i\oplus 1}$.

Γ muss gewährleisten, dass sich immer nur ein Fahrzeug in jedem Abschnitt befindet. Zu Beginn sei die Kreuzung leer.

a) Geben Sie für $\Gamma = (X, V, Z, T, start, Act, \mathcal{E})$ die Signatur SIG, die Struktur S, die Mengen X, V, Act und die Formel $start$ an.

Lösung: Eine Spezifikation des Systems braucht keine Prädikatenlogik, wir können also SIG und S beliebig wählen (zustandsendliche Systeme können immer ohne Prädikatenlogik spezifiziert werden, hier ist es lediglich eine Frage der Bequemlichkeit).

- $X = \{\}$
- $Act_\Gamma = \bigcup_{1 \leq i \leq 3} \{\rho_i^1, \rho_i^2, \lambda_i^1, \lambda_i^2, \lambda_i^3\}$

- $V = \left(\bigcup_{1 \leq i \leq 3} \{r_i, k_i, l_i^i, l_i^{i \oplus 1}\}\right) \cup \{exec\lambda \mid \lambda \in Act_\Gamma\}$
- $start_\Gamma \equiv \neg(k_1 \vee k_2 \vee k_3)$

Informelle Bedeutung der Aktionen: ρ_i^1 - ein Rechtsabbieger fährt auf Feld i, ρ_i^2 - ein Rechtsabbieger verlässt Feld i, λ_i^a - ein Linksabbieger (aus Strasse i kommend) fährt auf Feld i ($a = 1$), fährt weiter nach $i \oplus 1$ ($a = 2$) und verlässt Feld $i \oplus 1$ ($a = 3$).

Informelle Bedeutung der Variablen: r_i - Rechtsabbieger auf Feld K_i, l_j^i - Linksabbieger aus Straße j kommend auf Feld K_i, k_i - Feld K_i besetzt (eine Abkürzung für $r_i \vee l_i^i \vee l_{i \oplus 2}^i$).

b) Beschreiben Sie die möglichen Zustände und Transitionen durch Formeln aus $\mathcal{L}_{\mathrm{TL}\Gamma}$. Geben Sie eine kurze Begründung dafür, dass Ihre Spezifikation nie mehr als ein Fahrzeug auf jedem Kreuzungsabschnitt K_i zulässt.

Lösung: Die möglichen Zustände sind bereits weitestgehend durch die möglichen Variablenbelegungen gegeben (beispielsweise könnten wir einen Auffahrunfall gar nicht als Zustand darstellen). Es muß allerdings als eine "Invariante" die Abhängigkeit von k_i festgehalten werden:

- $k_i \leftrightarrow r_i \vee l_i^i \vee l_{i \oplus 2}^i$

Zusätzlich könnte man verlangen, daß verschiedene Abbiegertypen nicht auf einem Feld sein dürfen. Dies sollte man jedoch der Transitionsmodellierung überlassen - ein Unfall sollte durch geeignetes Ziehen verhindert werden, nicht durch Ausschliessen eines entsprechenden Zustandes. Generell ist es sinnvoll, bis auf Invarianzeigenschaften der Modellierung keine Annahmen an den Zustand zu machen.

Die Transitionen müssen sich wiederum mit der Frame-Eigenschaft befassen. Wir definieren $N(x_1, \ldots x_n) \equiv \bigwedge_{i=1}^n (\circ x_i \leftrightarrow x_i)$ und $I \equiv \{1, 2, 3\}$.

- $exec\rho_i^1 \rightarrow \neg k_i \wedge \circ r_i \wedge N(r_{i \oplus 1}, r_{i \oplus 2}) \wedge \bigwedge_{j \in I} N(l_j^j, l_j^{j \oplus 1})$
- $exec\rho_i^2 \rightarrow r_i \wedge \neg\circ k_i \wedge N(r_{i \oplus 1}, r_{i \oplus 2}) \wedge \bigwedge_{j \in I} N(l_j^j, l_j^{j \oplus 1})$
- $exec\lambda_i^1 \rightarrow \neg k_i \wedge \circ l_i^i \wedge \bigwedge_{j \in I} N(r_j) \wedge \bigwedge_{j \in I \setminus \{i\}} N(l_j^j, l_j^{j \oplus 1}) \wedge N(l_i^{i \oplus 1})$
- $exec\lambda_i^2 \rightarrow \neg k_{i \oplus 1} \wedge l_i^i \wedge \circ l_i^{i \oplus i} \wedge \neg\circ k_i \wedge \bigwedge_{j \in I} N(r_j) \wedge \bigwedge_{j \in I \setminus \{i\}} N(l_j^j, l_j^{j \oplus 1})$
- $exec\lambda_i^3 \rightarrow l_i^{i \oplus 1} \wedge \neg\circ k_{i \oplus 1} \wedge \bigwedge_{j \in I} N(r_j) \wedge \bigwedge_{j \in I \setminus \{i\}} N(l_j^j, l_j^{j \oplus 1}) \wedge N(l_i^i)$

Wie wir leicht sehen können, ist gewährleistet, daß nur dann k_i gesetzt wird, wenn vorher $\neg k_i$ galt (jeweils die erste Konjunktion der Aktionen ρ_i^1, λ_i^1 sowie λ_i^2). Dabei ist auch wichtig, daß die Frameeigenschaft garantiert wird und keine Autos "auf die Kreuzung fallen".

Zusätzlich müssen wir jedoch noch festhalten, daß nur eine Aktion gleichzeitig stattfinden kann (sogenanntes „Interleaving"):

- $exec\alpha \rightarrow \neg exec\beta \qquad$ für alle $\alpha, \beta \in Act, \alpha \neq \beta$

c) Nun kann immer noch folgende Verklemmungssituation entstehen: Auf jedem Kreuzungsabschnitt wartet ein Linksabbieger. Dies soll nun noch berücksichtigt werden. Ändern Sie Γ und die temporallogische Beschreibung entsprechend. Geben Sie eine Formel B an, die besagt, dass oben beschriebener Verklemmungszustand nicht eintreten kann.

Lösung: Die Verklemmung würde auftreten, wenn Linksabbieger einfahren und dann nicht auf den für sie nächsten Abschnitt $K_{i \oplus 1}$ fahren. Daher benötigen wir für $exec\lambda_i^1$ eine Prüfung, ob der Abbiegevorgang verklemmungsfrei abgeschlossen werden kann:

$$exec\lambda_i^1 \rightarrow \neg k_i \wedge \neg \mathbf{l}_{\mathbf{i \oplus 1}}^{\mathbf{i \oplus 1}} \circ l_i^i \wedge \bigwedge_{j \in I} N(r_j) \wedge \bigwedge_{j \in I \setminus \{i\}} N(l_j^j, l_j^{j \oplus 1}) \wedge N(l_i^{i \oplus 1})$$

Wir geben die Formel für Verklemmungsfreiheit B also an als:

$$B \equiv \Box(\neg l_1^1 \vee \neg l_2^2 \vee \neg l_3^3)$$

Lösung: Wir können allerdings ebensogut auf eine prädikatenlogische Modellierung ausweichen, wobei gewissermaßen die "Fakten" der aussagenlogischen Modellierung in geeignete "Makros" übersetzt werden.

1. Setze $SIG = (\mathbf{S}, \mathbf{F}, \mathbf{P})$ mit $\mathbf{S} = \{CSS\}, \mathbf{F} = \{\mathsf{free}, \mathsf{car_r}, \mathsf{car_l^1}, \mathsf{car_l^2}\}$ und $\mathbf{P} = \emptyset$. Sei S eine Struktur für SIG mit

   - $|CSS|_\mathsf{S} = \{free, car_r, car_l^1, car_l^2\}$
   - $|\mathsf{free}|_\mathsf{S} = free$, $|\mathsf{car_r}|_\mathsf{S} = car_r$, $|\mathsf{car_l^1}|_\mathsf{S} = car_l^1$, $|\mathsf{car_l^2}|_\mathsf{S} = car_l^2$

   Für $\Gamma = (X, V, Z, T, start, Act, \mathcal{E})$ ist

   - $X = X_{CSS} = \{K_1, K_2, K_3\}$
   - $V = \{exec\lambda \mid \lambda \in Act\}$
   - $Act = \bigcup_{i=1}^{3} \{\rho_i^1, \rho_i^2, \lambda_i^1, \lambda_i^2, \lambda_i^3\}$
   - $start \equiv \bigwedge_{i=1}^{3} K_i = \mathsf{free}$

   Dabei sind die Wirkungen der Aktionen aus Act wie oben beschrieben.

2. In unserer Modellierung haben wir nun eine totale Zustandsmenge, abgesehen von der Interleaving-Einschränkung:

   - $exec\alpha \rightarrow \neg exec\beta$ für alle $\alpha, \beta \in Act, \alpha \neq \beta$

   Die Zustandsübergänge sind gegeben für jedes $i \in \{1, \ldots, 3\}$, wobei $N(x_1, \ldots, x_n) \equiv \bigwedge_{i=1}^{n} x_i' = x_i$ abkürzt:

   - $exec\rho_i \rightarrow K_i = \mathsf{free} \wedge K_i' = \mathsf{car}_r \wedge N(K_{i\oplus 1}, K_{i\oplus 2})$
   - $exec\rho_i \rightarrow K_i = \mathsf{car}_r \wedge K_i' = \mathsf{free} \wedge N(K_{i\oplus 1}, K_{i\oplus 2})$
   - $exec\lambda_i^1 \rightarrow K_i = \mathsf{free} \wedge K_i' = \mathsf{car}_l^1 \wedge N(K_{i\oplus 1}, K_{i\oplus 2})$
   - $exec\lambda_i^2 \rightarrow K_i = \mathsf{car}_l^1 \wedge K_{i\oplus 1} = \mathsf{free} \wedge K_i' = \mathsf{car}_l^1 \wedge K_{i\oplus 1}' = \mathsf{car}_l^2 \wedge N(K_{i\oplus 2})$
   - $exec\lambda_i^3 \rightarrow K_{i\oplus 1} = \mathsf{car}_l^2 \wedge K_{i\oplus 1}' = \mathsf{free} \wedge N(K_{i\oplus 2}, K_i)$

   Da sich diese Modellierung genau wie die propositionale Modellierung verhält, überzeugen wir uns leicht, daß sie ebenso die Sicherheitseigenschaft erfüllt.

3. Erneut verschärfen wir die Bedingung für das Einfahren für Linksabbieger:

   - $exec\lambda_i^1 \rightarrow K_i = \mathsf{free} \wedge K_{i\oplus 1} \neq \mathsf{car}_l^1 \wedge K_i' = \mathsf{car}_l^1 \wedge N(K_{i\oplus 1}, K_{i\oplus 2})$

   Die Formel D für das Ausbleiben von Verklemmung ist demnach

$$D \equiv \bigvee_{i=1}^{3} K_i \neq \mathsf{car}_l^1$$

Insgesamt nimmt uns hier die Prädikatenlogik also nur die Verwendung verschiedener Variablen für die Beschreibung eines Kreuzungsabschnitts sowie die damit verbundenen Invarianten ab.

Aufgabe 9-3 **Fairness** (5 Punkte)

Betrachten Sie folgenden weiteren Fairnessbegriff für (r)lSTS $\Gamma = (X, V, Z, T, Act, (start))$:

schwache Fairness (weak fairness) Ein Ablauf $\mathsf{W} = (\eta_0, \eta_1, \ldots)$ von Γ ist schwach fair, wenn für alle $\lambda \in Act$ gilt: Falls $\mathsf{S}_\Gamma^{(\eta_k)}(\text{enabled}_\lambda) = \mathsf{ff}$ für höchstens endlich viele $k \geq 0$, dann ist $\mathsf{S}_\Gamma^{(\eta_k)}(exec\lambda) = \mathsf{tt}$ für unendlich viele $k \geq 0$.

Wie bei dem Fairnessbegriff der Vorlesung gelte für alle $\lambda \in Act$ und $i \in \mathbb{N}$: Falls $\mathsf{S}_\Gamma^{(\eta_i)}(exec\lambda) = \mathsf{tt}$, so ist auch $\mathsf{S}_\Gamma^{(\eta_i)}(\text{enabled}_\lambda) = \mathsf{tt}$.

a) Zeigen Sie: Jeder faire Ablauf von Γ im Sinne der Vorlesung ist auch schwach fair.

Lösung: Der Fairnessbegriff aus der Vorlesung ist in der Literatur als "starke Fairness" bekannt. Daneben gibt es eine Vielzahl anderer Fairnessbegriffe; zwei davon sollen hier stellvertretend untersucht werden.

Sei W ein fairer Ablauf von Γ (im Sinne der Vorlesung) und $\mathsf{K} = (\mathsf{S}, \mathsf{W})$. Ist $\mathsf{S}^{(\eta_k)}(\text{enabled}_\lambda) = \mathsf{ff}$ für höchstens endlich viele $k \geq 0$, so folgt insbesondere $\mathsf{S}^{(\eta_k)}(\text{enabled}_\lambda) = \mathsf{tt}$ für unendlich viele $k \geq 0$. Aus der Fairnessbedingung der Vorlesung folgt dann, dass $\mathsf{S}^{(\eta_k)}(exec\,\lambda) = \mathsf{tt}$ gilt für unendlich viele $k \geq 0$.

b) Geben Sie ein Transitionssystem Γ und einen Ablauf von Γ an, der schwach fair, aber nicht fair im Sinne des Fairnessbegriffs der Vorlesung ist.

Lösung: *Idee:* Wir brauchen eine Aktion, die unendlich oft, aber nicht persistent ausführbar ist. Das kann man durch einen *Konflikt* erreichen, d.h. einen Zustand, in dem zwei Aktionen ausführbar sind, so dass nach Ausführung einer Aktion die andere nicht mehr ausführbar ist. Ein typisches Beispiel dafür ist eine Semaphorlösung zum gegenseitigen Ausschluss zweier Prozesse:

semaphore s := 1;

loop			**loop**	
ncrit_1:	/* nicht-kritischer Abschnitt */		ncrit_2:	/* nicht-kritischer Abschnitt */
try_1:	P(s);	$\parallel$	try_2:	P(s);
crit_1:	/* kritischer Abschnitt */		crit_2:	/* kritischer Abschnitt */
exit_1:	V(s);		exit_2:	V(s);
endloop			**endloop**	

Die formale Modellierung durch ein Transitionssystem sei als Übung überlassen. Dabei gilt insbesondere $\text{enabled}_{\text{try}_i} \equiv s = 1 \wedge at\,\text{try}_i$, wobei $at\,\text{try}_i$ die Zustände beschreibe, in denen Prozess i vor der Anweisung try_i steht.

Ein Ablauf, bei dem Prozess 1 an der P-Anweisung (try_1) stehen bleibt, während Prozess 2 immer wieder den kritischen Abschnitt betritt und verlässt, erfüllt die schwache Fairnessbedingung, weil die Ausführbarkeitsbedingung $\text{enabled}_{\text{try}_1}$ unendlich oft nicht erfüllt ist.

Dagegen erfüllt dieser Ablauf nicht die (starke) Fairnessbedingung der Vorlesung, weil $\text{enabled}_{\text{try}_1}$ unendlich oft erfüllt ist (nämlich immer dann, wenn der zweite Prozess bei ncrit_2 oder try_2 steht), die Anweisung try_1 aber nur endlich oft ausgeführt wird.

c) Geben Sie ein Axiom (wfair_Γ) analog zum Axiom (fair_Γ) an, welches den schwachen Fairnessbegriff charakterisiert.

Lösung: Charakterisierung der Fairnessbegriffe durch temporallogische Axiome:

$$(\text{wfair}_\Gamma) \quad \Box\text{enabled}_\lambda \rightarrow \Diamond exec\,\lambda$$

Gleichmächtig zu (wfair_Γ) sind die Formulierungen

$$\Diamond\Box\text{enabled}_\lambda \rightarrow \Diamond exec\,\lambda \qquad \text{bzw.} \qquad \Diamond\Box\text{enabled}_\lambda \rightarrow \Box\Diamond exec\,\lambda$$

Das Axiom (progress) ist aus (wfair_Γ) immer noch ableitbar:

(1)	$\text{nil}_\Gamma \wedge \text{enabled}_\lambda \rightarrow \bigcirc(\text{nil}_\Gamma \wedge \text{enabled}_\lambda)$	(prop)(nil)
(2)	$\text{nil}_\Gamma \wedge \text{enabled}_\lambda \rightarrow \Box(\text{nil}_\Gamma \wedge \text{enabled}_\lambda)$	(ind1)(1)
(3)	$\Box(\text{nil}_\Gamma \wedge \text{enabled}_\lambda) \rightarrow \Box\text{nil}_\Gamma \wedge \Box\text{enabled}_\lambda$	(T17)(prop)
(4)	$\text{nil}_\Gamma \wedge \text{enabled}_\lambda \rightarrow \Box\text{nil}_\Gamma \wedge \Diamond exec\,\lambda$	(2)(3)(wfair)
(5)	$\Box\text{nil}_\Gamma \wedge \Diamond exec\,\lambda \rightarrow \Diamond(\text{nil}_\Gamma \wedge exec\,\lambda)$	(T29)(prop)
(6)	$\neg(\text{nil}_\Gamma \wedge exec\,\lambda)$	(taut)
(7)	$\Box\neg(\text{nil}_\Gamma \wedge exec\,\lambda)$	(6)(alw)
(8)	$\text{enabled}_\lambda \rightarrow \neg\text{nil}_\Gamma$	(prop)(4)(5)(7)

Abgabe: Mittwoch, den 20.12.2006, vor der Übung.