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

WS 2006/2007
Übungsblatt 9

Temporale Logik und Zustandssysteme

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.

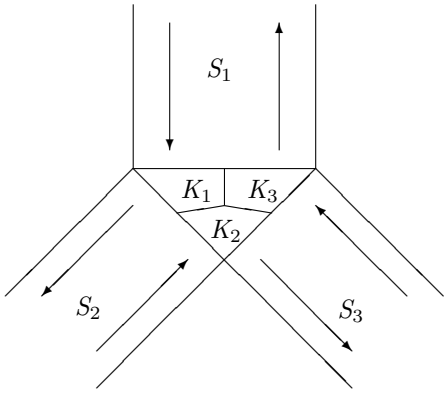
b) Beweisen Sie, dass $\prec$ eine fundierte Relation auf $\mathbb{N} \times \mathbb{N}$ ist.

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

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

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

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.

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.

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.

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 $\mathsf{S}_\Gamma^{(\eta_k)}(\mathrm{enabled}_\lambda) = \mathsf{ff}$ 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 $\mathsf{S}_\Gamma^{(\eta_i)}(\mathrm{enabled}_\lambda) = \mathsf{tt}$.

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

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.

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

Abgabe: Mittwoch, den 20.12.2006, vor der Übung.