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

WS 2006/2007
Übungsblatt 11

Temporale Logik und Zustandssysteme

Aufgabe 11-1 **Stapel** (8 Punkte)

In dieser Aufgabe soll ein Stapel (Stack, FILO-Buffer) natürlicher Zahlen temporallogisch modelliert werden.

Die der Modellierung zugrundeliegende Signatur SIG verfügt über die Sorten, S und NAT und $NAT^\bullet$ mit folgender Interpretation:

- NAT wird durch $\mathbb{N}$ interpretiert (Objekte, die auf den Stapel gelegt werden).
- $NAT^\bullet$ wird interpretiert durch die Menge $\mathbb{N} \cup \{\bullet\}$ (Das Symbol "$\bullet$" signalisiert einen Fehler).
- $STACK$ (der Stapel) wird interpretiert durch die Menge $\mathbb{N}^*$ der endlichen Folgen natürlicher Zahlen.

Eine endliche Folge $(n_0, n_1, \ldots, n_k)$ von natürlichen Zahlen entspricht einem Stapel, auf den die Zahlen $n_0, n_1, \ldots, n_k$ in dieser Reihenfolge abgelegt wurden.

Die Signatur enthält ferner

- die Individuenkonstante $\text{EMPTY}^{(\epsilon, STACK)}$, interpretiert durch die leere Folge.
- das Funktionssymbol $\text{APPEND}^{(NAT\ STACK, STACK)}$, interpretiert durch die Funktion $((n_0, \ldots, n_k), n) \mapsto (n_0, \ldots, n_k, n)$, die eine Zahl hinten an eine Folge anfügt.
- das Funktionssymbol $\text{LAST}^{(STACK, NAT^\bullet)}$, interpretiert durch die Funktion, die das letzte Element einer Folge zurückliefert, bzw. $\bullet$ für die leere Folge.
- das Funktionssymbol $\text{LEN}^{(STACK, NAT)}$, interpretiert durch die Funktion, die die Länge einer Folge natürlicher Zahlen bestimmt.

Wir betrachten die Aktionenmenge $Act = \{\mathsf{push}, \mathsf{pop}\}$. Ein Ausführen der Aktion push steht hier für das Ablegen einer Zahl auf dem Stapel, die Aktion pop bedeutet das Herunternehmen einer Zahl.

Beachten Sie, dass nur dann eine Zahl heruntergenommen werden kann, wenn der Stapel mindestens eine Zahl enthält.

a) Geben Sie ein markiertes Transitionssystem $(X, V, Z, T, Act, \mathcal{E})$ an, das das Verhalten des Stapels modelliert. Ihre Modellierung soll mindestens eine Systemvariable s enthalten, die den Zustand des Stapels repräsentiert.

b) Geben Sie eine Menge $\mathcal{A}$ von temporallogischen Formeln an, die das Verhalten des Stapels möglichst genau beschreiben.

c) Formulieren Sie die Eigenschaft

> "Jede Zahl, die vom Stapel genommen wurde, wurde irgendwann einmal auf den Stapel gelegt"

als temporallogische Formel F in der Sprache $\mathcal{L}^p_{\text{FOLTL}}$. *Hinweis:* Formulieren Sie zunächst die Eigenschaft "die Zahl n wurde auf den Stapel gelegt" als temporallogische Formel.

d) Geben Sie einen Ablauf $(\eta_0, \eta_1, \ldots)$ des Transitionssystems an, in dem F *nicht* gilt.

e) Formulieren Sie die Eigenschaft

> "Wenn der Stapel leer ist, so gilt von nun an die Formel F"

als temporallogische Formel G.

f) Zeigen Sie: In jedem Ablauf des Transitionssystems gilt die Formel G.

g) Zeigen Sie: $\mathcal{A} \vdash \text{LEN}(s) = n \wedge exec\mathsf{push} \rightarrow \text{LEN}(s) > n$ **unless** $exec\mathsf{pop}$ durch Angabe einer Herleitung. Die Gesetze (T1)-(T59) sowie die abgeleitete Regel

$$\begin{array}{rl} (\text{unless}_\Gamma) & exec\lambda \wedge A \rightarrow \circ C \vee \circ(B \wedge A) \quad \text{für alle } \lambda \in Act \\ & \text{nil}_\Gamma \wedge A \rightarrow B \vee C \\ & \vdash A \rightarrow B \textbf{ unless } C \end{array}$$

dürfen verwendet werden.

Aufgabe 11-2 **Warteschlange** (6 Punkte)

Gegeben seien die Sorten $QUEUE$ und NAT, die Funktionszeichen ENQ und DEQ sowie die Prädikatszeichen IN und ISEMPTY mit folgenden intuitiven Bedeutungen. Die Elemente (der Interpretation von) $QUEUE$ sind endliche Folgen von natürlichen Zahlen mit den für "Schlangen" üblichen Operationen ENQ und DEQ sowie den Prädikaten ISEMPTY und IN:

- $\text{ENQ}(q, n)$ ist die Schlange, die entsteht, wenn man die natürliche Zahl n an die Schlange q hinten anfügt.
- $\text{DEQ}(q)$ ist die Schlange, die entsteht, wenn man das vorderste Element von q entfernt, falls q nicht leer ist, und die leere Schlange sonst.
- $\text{ISEMPTY}(q)$ ist wahr genau dann, wenn q die leere Schlange ist.
- $\text{IN}(n, q)$ ist wahr genau dann, wenn n in q enthalten ist.

Weiter seien N eine Individuenkonstante und x eine Variable der Sorte NAT.

Sei Π das folgende PAR-Programm (mit durch vorstehende Angaben informell beschriebener Signatur SIG_Π und Struktur S_Π):

$\Pi \equiv$ **var** $q : QUEUE; n : NAT$
start $\text{ISEMPTY}(q) \wedge n > N$
cobegin loop $\alpha_0 : q := \text{ENQ}(q, n);$
$\alpha_1 : n := n + 1$
endloop
$\|$
loop β : **await** $\neg\text{ISEMPTY}(q)$ **then** $q := \text{DEQ}(q)$
endloop
coend

a) Beweisen Sie durch Angabe einer Herleitung: $\mathcal{A}_\Pi \vdash \Box(n > N)$.

b) Beweisen Sie durch Angabe einer Herleitung: $\mathcal{A}_\Pi \vdash \Box(\text{IN}(x, q) \rightarrow x > N)$.

c) Geben Sie eine Formel aus $\mathcal{L}_{\text{TL}\Pi}$ an, die besagt, dass jedes Element, das in der Schlange enthalten ist, irgendwann „ganz vorne steht".

Hinweis: Für die Herleitungen sind insbesondere folgende (data)-Axiome nützlich:

(H1) $\text{ISEMPTY}(q) \rightarrow \neg\text{IN}(x, q)$.

(H2) $\text{IN}(x, \text{ENQ}(n, q)) \leftrightarrow x = n \vee \text{IN}(x, q)$.

(H3) $\text{IN}(x, \text{DEQ}(q)) \rightarrow \text{IN}(x, q)$.

Aufgabe 11-3 **Mengen** (keine Abgabe)

Das folgende PAR-Programm vertauscht Elemente der endlichen Mengen S und T von natürlichen Zahlen.

$\Pi \equiv$ **var** $min, max, min_0, max_0 : NAT^\infty$;
$S, T : NATS$
start $max_0 > \max(T) \wedge min_0 < \min(S) \wedge min = min_0 \wedge max = max_0$
cobegin loop $\alpha_0 : min := \min(S)$;
α_1 : **await** $min < max \wedge max < max_0$ **then** $max_0 := max$;
$\alpha_2 : S := (S \setminus \{min\}) \cup \{max_0\}$
endloop
$\|$
loop $\beta_0 : max := \max(T)$;
β_1 : **await** $max > min \wedge min > min_0$ **then** $min_0 := min$;
$\beta_2 : T := (T \setminus \{max\}) \cup \{min_0\}$
endloop
coend

Die informellen Bedeutungen der Sorten NAT^∞ und $NATS$ sind: (die Interpretation von) NAT^∞ enthält alle natürlichen Zahlen sowie die Pseudowerte ∞ und $-\infty$; die Relationen $<$, $>$, usw. sind wie üblich erweitert auf NAT^∞, d.h. für alle natürlichen Zahlen n gilt $-\infty < n$ und $n < \infty$.
Die Sorte $NATS$ besteht aus allen endlichen Mengen von natürlichen Zahlen. Die Interpretationen von $\cup$, $\setminus$ sind wie üblich, $\min(U)$ bzw. $\max(U)$ bezeichen das kleinste bzw. größte Element einer Menge U, falls diese nicht leer ist, und sonst die Pseudowerte $-\infty$ bzw. ∞. Insbesondere gelten also u.a. folgende Daten-Axiome:

$$x \in U \rightarrow x \geq \min(U),$$
$$x \in U \rightarrow x \leq \max(U),$$
$$\min(U) = k \wedge x \geq k \rightarrow \min((U \setminus \{k\}) \cup \{x\}) \geq k.$$

a) Beweisen Sie $\mathcal{A}_\Pi \vdash start_\Pi \rightarrow \Box I$ für

$$\begin{aligned} I \equiv\ & \wedge (max_0 \geq max) \wedge (min_0 \leq min) \\ & \wedge (min \leq \min(S)) \wedge (at\{\alpha_1, \alpha_2\} \rightarrow min = \min(S)) \\ & \wedge (max \geq \max(T)) \wedge (at\{\beta_1, \beta_2\} \rightarrow max = \max(T)) \\ & \wedge (at\,\alpha_2 \rightarrow min \leq \max_0) \wedge (at\,\beta_2 \rightarrow min_0 \leq max), \end{aligned}$$

wobei $at\,M$ für eine endliche Menge M von Marken die Formel $\bigvee_{\alpha \in M} at\,\alpha$ bezeichnet.
Sie dürfen ohne Beweis voraussetzen, dass $\mathcal{A}_\Pi \vdash I$ **invof** $\{\beta_0, \beta_1, \beta_2\}$ gilt.

b) Beweisen Sie $\mathcal{A}_\Pi \vdash \Box(\exists x \exists y(x \in S \wedge y \in T \wedge x < y) \rightarrow min < max)$.

Abgabe: Mittwoch, den 17.1.2007, vor der Übung.