Ludwig-Maximilians-Universität München WS 2006/2007
Institut für Informatik Übungsblatt 8
Prof. Dr. F. Kröger, M. Hammer

Temporale Logik und Zustandssysteme Lösungsvorschlag

Aufgabe 8-1 **Allgemeingültigkeit in FOLTL** (4 Punkte)

Sei $TSIG = (SIG, \mathbf{X}, \mathbf{V})$ eine temporale Signatur. Welche der folgenden Formeln von $\mathcal{L}_{\mathrm{FOLTL}}(TSIG)$ sind allgemeingültig? (Dabei sind $x, y \in \mathcal{X}$ und $a \in \mathbf{X}$.) Beweisen Sie Ihre Antworten.

a) $\exists x(a \neq x \wedge a' = x) \rightarrow (a' \neq a)$.

Lösung: Diese Formel ist allgemeingültig. Sei $\mathsf{K} = (\mathsf{S}, \mathsf{W})$ eine beliebige temporale Struktur für $TSIG$, sei $i \in \mathbb{N}$ beliebig und sei ξ eine beliebige Variablenbelegung. Dann gilt Folgendes:

$$
\begin{aligned}
& \mathsf{K}_i^{(\xi)}(\exists x(a \neq x \wedge a' = x)) = \mathsf{tt} \\
\Longrightarrow\ & \mathsf{K}_i^{(\xi')}(a \neq x \wedge a' = x) = \mathsf{tt} \text{ für ein } \xi' \sim_x \xi \\
\Longrightarrow\ & \eta_i(a) \neq \xi'(x) \text{ und } \eta_{i+1}(a) = \xi'(x) \text{ für ein } \xi' \sim_x \xi \\
\Longrightarrow\ & \eta_i(a) \neq \eta_{i+1}(a) \\
\Longrightarrow\ & \mathsf{K}_i^{(\xi)}(a' \neq a) = \mathsf{tt}
\end{aligned}
$$

Daraus folgt $\mathsf{K}_i^{(\xi)}(\exists x(a \neq x \wedge a' = x) \rightarrow (a' \neq a)) = \mathsf{tt}$. Nachdem K, ξ und $i \in \mathbb{N}$ beliebig waren, folgt die Behauptung.

b) $\Box\Diamond(a' \neq a) \rightarrow \forall x \Diamond\Box(a \neq x)$.

Lösung: Diese Formel ist nicht allgemeingültig.

Sei $\mathsf{K} = (\mathsf{S}, \mathsf{W})$ eine temporale Struktur für $TSIG$ mit $|N|_{\mathsf{S}} = \mathbb{N}$, $\eta_{2i}(a) = i$ und $\eta_{2i+1}(a) = 0$. Sei ξ eine beliebige Variablenbelegung bezüglich S und sein $i \in \mathbb{N}$ beliebig.

$$
\begin{aligned}
& \mathsf{K}_0^{(\xi)}(\Box\Diamond(a' \neq a)) = \mathsf{tt} \\
\text{gdw. } & \text{für alle } i \geq 0 \text{ gibt es } j \geq i \text{ mit } \mathsf{K}_{j+1}^{(\xi)}(a) \neq \mathsf{K}_j^{(\xi)}(a) \\
\text{gdw. } & \text{für alle } i \geq 0 \text{ gibt es } j \geq i \text{ mit } \eta_{j+1}(a) \neq \eta_j(a)
\end{aligned}
$$

Setzt man $j = 2i + 1$, so gilt für ein beliebiges $i \in \mathbb{N}$, so gilt wegen $j + 1 = 2i + 2$ offenbar $\eta_{j+1}(a) = i + 1$ und $\eta_j(a) = 0$, insbesondere also $\eta_{j+1}(a) \neq \eta_j(a)$ und damit nach den obigen Ausführungen $\mathsf{K}_0^{(\xi)}(\Box\Diamond(a' = a)) = \mathsf{tt}$.

Jetzt zeigen wir, dass $\mathsf{K}_0^{(\xi)}(\forall x \Diamond\Box(a \neq x)) = \mathsf{ff}$ gilt. Sei ξ' gegeben durch $\xi'(x) = 0$ und $\xi'(y) = \xi(y)$ für $y \neq x$. Nach der Definition von K gilt $\mathsf{K}_{2i+1}^{(\xi')}(a) = 0$ für alle $i \in \mathbb{N}$. Außerdem gilt nach der Definition von ξ' auch $\mathsf{K}_{2i+1}^{(\xi')}(x) = \xi'(x) = 0$. Also gibt es für jedes $i \in \mathbb{N}$ ein $j \geq i$ (nämlich $j = 2i + 1$) mit $\mathsf{K}_j^{(\xi')}(a = x) = \mathsf{tt}$. Da $\xi' \sim_x \xi$, folgt damit $\mathsf{K}_0^{(\xi)}(\exists x \neg\Diamond\Box(a \neq x)) = \mathsf{tt}$, also $\mathsf{K}_0^{(\xi)}(\forall x \Diamond\Box(a \neq x)) = \mathsf{ff}$.

Aufgabe 8-2 **Zähler** (3 Punkte)

Gegeben sei die Signatur SIG mit der Sorte NAT, den Konstanten $0, 1, 2, \ldots$ der Sorte NAT, den Funktionszeichen $+^{(NAT\ NAT, NAT)}$ und $-^{(NAT\ NAT, NAT)}$ sowie dem Prädikatszeichen $<^{(NAT\ NAT)}$.

Sei $a \in \mathbf{X}_{NAT}$ und $x \in \mathcal{X}_{NAT}$. Sei $\mathcal{F}$ die Menge aller Formeln von $\mathcal{L}_{\mathrm{FOL}}(SIG^+)$, die im Standardmodell der natürlichen Zahlen gelten. Beweisen Sie in dem formalen System $\Sigma_{\mathrm{FOLTL}}^{\mathrm{w}}$, wobei WF die Sorte NAT mit $<$ als $\prec$ ist:

a) $\mathcal{F} \vdash a < x \wedge z = x - a \wedge \Box(a' = a + 1) \to \circ(a \leq x)$. (keine Abgabe)

Lösung: Setze $A \equiv a < x \wedge z = x - a \wedge \Box(a' = a + 1)$.

(1)	$a < x \wedge y = a + 1 \to y \leq x$	Annahme
(2)	$y \leq x \to \circ(y \leq x)$	(ltl6)
(3)	$a = y \wedge y \leq x \to a \leq x$	(pred)
(4)	$\circ(a = y) \wedge \circ(y \leq x) \to \circ(a \leq x)$	(nex)(3)(ltl2)(T15)(prop)
(5)	$a < x \wedge \circ(a = y) \wedge y = a + 1 \to \circ(a \leq x)$	(1)(2)(4)(prop)
(6)	$\exists y(a < x \wedge \circ(a = y) \wedge y = a + 1) \to \circ(a \leq x)$	(par)(5)
(7)	$A \to \exists y(a < x \wedge \circ(a = y) \wedge y = a + 1)$	(prop)(ltl2)(pred)
(8)	$A \to \circ(a \leq x)$	(6)(7)(prop)

b) $\mathcal{F} \vdash a < x \wedge z = x - a \wedge \Box(a' = a + 1) \to \circ(z - 1 = x - a)$. (keine Abgabe)

Lösung: Setze $A \equiv a < x \wedge z = x - a \wedge \Box(a' = a + 1)$.

(1)	$(z = x - a) \wedge (y = a + 1) \to (z - 1 = x - y)$	Annahme
(2)	$(z - 1 = x - y) \to \circ(z - 1 = x - y)$	(ltl6)
(3)	$(z - 1 = x - y) \wedge (a = y) \to (z - 1 = x - a)$	Annahme (oder (pred))
(4)	$\circ(z - 1 = x - y) \wedge \circ(a = y) \to \circ(z - 1 = x - a)$	(nex)(3)(ltl2)(T15)(prop)
(5)	$(z = x - a) \wedge (y = a + 1) \wedge \circ(a = y) \to \circ(z - 1 = x - a)$	(1)(2)(4)(prop)
(6)	$\exists y(z = x - a \wedge y = a + 1 \wedge \circ(a = y)) \to \circ(z - 1 = x - a)$	(par)(5)
(7)	$A \to \exists y(z = x - a \wedge y = a + 1 \wedge \circ(a = y))$	(pred)(ltl3)(prop)
(8)	$A \to \circ(z - 1 = x - a)$	(6)(7)(prop)

c) $\mathcal{F} \vdash a = 0 \wedge \Box(a' = a + 1) \to \Diamond a = x$. (3 Punkte)

Lösung: Die Formel leiten wir mit Hilfe der Regel (wfr) her. Da die Regel (wfr) eine Formel $\exists z A \to \Diamond B$ liefert, versuchen wir zunächst Formeln A und B zu finden, für die

1. $\mathcal{F} \vdash a = 0 \wedge \Box(a' = a + 1) \to \exists z A$ sowie
2. $\mathcal{F} \vdash \Diamond B \to \Diamond a = x$

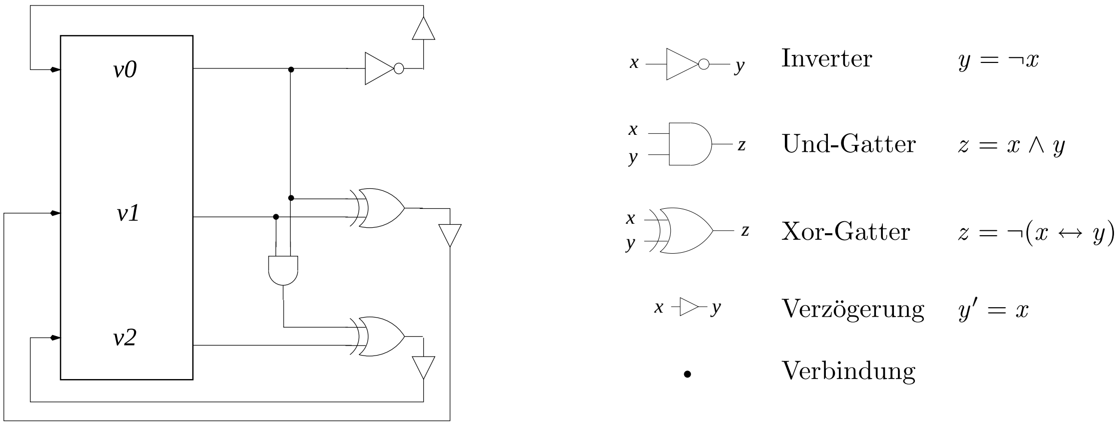
gilt und für die wir die Prämissen von (wfr) herleiten können. Da a in jedem Schritt um eins erhöht wird, wird offenbar die Zahl $x - a$ in jedem Schritt kleiner. Daher bietet $x - a = z$ sich als ein Konjunkt der Formel A an.

Wir wählen $A \equiv a < x \wedge z = x - a \wedge \Box(a' = a + 1)$ und $B \equiv a = x$. Beachte, dass $a' = a + 1$ eine Abkürzung von $\Box \exists y(\circ(a = y) \wedge y = a + 1)$ ist. Wir können für diese Formeln 1. nicht zeigen, da die linke Seite auch den Fall $a = x$ erlaubt, wogegen dieser durch $\exists z A$ ausgeschlossen wird. Es ist jedoch möglich, $\mathcal{F} \vdash a = 0 \wedge \Box(a' = a + 1) \to \exists z A \vee B$ zu zeigen. Zusammen mit $\mathcal{F} \vdash \exists z A \to \Diamond B$ genügt dies, um die Behauptung zu zeigen.

(1)	$A \to \circ\Box\exists y(\circ(a = y) \wedge y = a + 1)$	(ltl3)(prop)
(2)	$A \to \circ(B \vee (a < x \wedge z - 1 = x - a \wedge \Box(a' = a + 1))$	(Aufg. a))(Aufg.b))(1)(T15)(T16)
(3)	$A \to \Diamond(B \vee A_z(z - 1))$	(T7)(2)(prop)
(4)	$\Box(A_z(z - 1) \to \exists \overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})))$	(ltl4)(alw)
(5)	$\Diamond A_z(z - 1) \to \Diamond(\exists \overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})))$	(T26)(prop)(4)
(6)	$A \to \Diamond(B \vee \exists \overline{z}(\overline{z} \prec z \wedge A_z(\overline{z})))$	(3)(T18)(5)
(7)	$\exists z A \to \Diamond B$	(wfr)(6)
(8)	$a = 0 \wedge \Box(a' = a + 1) \to a = x \vee \exists z A$	(pred)
(9)	$a = 0 \wedge \Box(a' = a + 1) \to B \vee \Diamond B$	(7)(8)(prop)
(10)	$a = 0 \wedge \Box(a' = a + 1) \to \Diamond B$	(9)(T5)(prop)

Aufgabe 8-3 **Elektronisches Schaltwerk** (6 Punkte)

Das folgende Schaltwerk realisiert einen Zähler modulo 8, dessen aktueller Stand durch die drei Bits v_0, v_1 und v_2 dargestellt wird.



Das Schaltwerk läuft getaktet ab; in jedem Takt werden die drei Bits ausgelesen, ihr neuer Wert ergibt sich gemäß den angegebenen Verknüpfungen. Die Verzögerungsglieder speichern ein Bit über einen Takt.

a) Beschreiben Sie das Schaltwerk durch ein propositionales Zustandsübergangssystem Γ.

Lösung: Das Schaltwerk wird modelliert durch das propositionale STS $\Gamma = (\emptyset, \{v_0, v_1, v_2\}, S, T)$ mit der vollen Zustandsmenge S (d.h. jede Abbildung $\eta : \{v_0, v_1, v_2\} \to \{\mathsf{tt}, \mathsf{ff}\}$ ist in S enthalten) und der Zustandsübergangsrelation T wie folgt:

$$(\eta, \eta') \in T \quad \Longleftrightarrow \quad \left\{ \begin{array}{lcl} \eta'(v_0) = \mathsf{tt} & \Longleftrightarrow & \eta(v_0) = \mathsf{ff}, \\ \eta'(v_1) = \mathsf{tt} & \Longleftrightarrow & \eta(v_1) \neq \eta(v_0), \\ \eta'(v_2) = \mathsf{tt} & \Longleftrightarrow & \eta(v_2) \neq \eta(v_0 \wedge v_1) \end{array} \right\}$$

Insbesondere ist T (links-)total.

b) Beschreiben Sie die Abläufe von Γ durch eine axiomatische FOLTL-Spezifikation $\mathcal{A}$.

Lösung: Die Abläufe von Γ werden (z.B.) durch die folgenden nicht-logischen Axiome $\mathcal{A}$ charakterisiert.

$$\begin{array}{lccl} \text{(S0)} & \bigcirc v_0 & \leftrightarrow & \neg v_0 \\ \text{(S1)} & \bigcirc v_1 & \leftrightarrow & \neg(v_1 \leftrightarrow v_0) \\ \text{(S2)} & \bigcirc v_2 & \leftrightarrow & \neg(v_2 \leftrightarrow v_0 \wedge v_1) \end{array}$$

c) Beweisen Sie, dass das Bit v_1 immer wieder den Wert 0 hat, indem Sie eine Herleitung einer entsprechenden Formel aus $\mathcal{A}$ angeben; hierbei dürfen die Gesetze (T1) bis (T59) benutzt werden.

Lösung: Wir leiten die Formel $\Diamond\neg v_1$ (und daraus $\Box\Diamond\neg v_1$) her, durch Fallunterscheidung nach dem Ausgangszustand.

(1)	$\neg v_1 \to \Diamond\neg v_1$	(T5)
(2)	$v_1 \wedge v_0 \to (v_1 \leftrightarrow v_0)$	(taut)
(3)	$v_1 \wedge v_0 \to \neg\bigcirc v_1$	(2)(S1)
(4)	$v_1 \wedge v_0 \to \Diamond\neg v_1$	(3)(T1)(T7)
(5)	$v_1 \wedge \neg v_0 \to \neg(v_1 \leftrightarrow v_0)$	(taut)
(6)	$v_1 \wedge \neg v_0 \to \bigcirc v_1$	(5)(S1)
(7)	$\neg v_0 \to \bigcirc v_0$	(S0)
(8)	$v_1 \wedge \neg v_0 \to \bigcirc(v_1 \wedge v_0)$	(6)(7)(T15)
(9)	$\bigcirc(v_1 \wedge v_0) \to \bigcirc\Diamond\neg v_1$	(4)(T25)
(10)	$v_1 \wedge \neg v_0 \to \Diamond\neg v_1$	(8)(9)(T24)
(11)	$\Diamond\neg v_1$	(1)(4)(10)
(12)	$\Box\Diamond\neg v_1$	(alw)(11)

Abgabe: Mittwoch, den 13.12.2006, vor der Übung.