

Temporale Logik und Zustandssysteme

Aufgabe 9-1 Herleitungen in temporaler Prädikatenlogik

- a) Die Formel $\Diamond\Box\forall x A \rightarrow \forall x \Diamond\Box A$ ist allgemeingültig: Es sei $K = (S, W)$ eine temporale Struktur, ξ eine Variablenbelegung und $i \in \mathbb{N}_0$ beliebig. Dann gilt:

$$\begin{aligned} & K_i^{(\xi)}(\Diamond\Box\forall x A) = \text{tt} \\ \implies & \text{ es gibt } j \geq i \text{ mit } K_k^{(\xi)}(\forall x A) = \text{tt} \text{ für alle } k \geq j \\ \implies & \text{ es gibt } j \geq i, \text{ so daß für alle } k \geq j \text{ und alle } \xi' \text{ mit } \xi' \sim_x \xi \text{ gilt: } K_k^{(\xi')} (A) = \text{tt} \\ \xRightarrow{(*)} & \text{ für alle } \xi' \text{ mit } \xi' \sim_x \xi \text{ gibt es } j \geq i, \text{ so daß für alle } k \geq j \text{ gilt: } K_k^{(\xi')} (A) = \text{tt} \\ \implies & K_i^{(\xi)}(\forall x \Diamond\Box A) = \text{tt} \end{aligned}$$

Die Folgerung (*) ist richtig, weil "es gibt ... für alle" stärker ist als "für alle ... es gibt".

Die umgekehrte Implikation $\forall x \Diamond\Box A \rightarrow \Diamond\Box\forall x A$ ist nicht allgemeingültig: Es sei A die Formel $a > x$ (für ein flexibles Individuensymbol a), S sei eine Struktur für die natürlichen Zahlen mit $S(>) = \text{"größer als"}$, und $W = (\eta_0, \eta_1, \dots)$ sei eine Folge von Zuständen mit $\eta_i(a) = i$. Dann ist $K_0^{(\xi)}(\forall x \Diamond\Box(a > x)) = \text{tt}$ für beliebige Belegung ξ , denn für jede natürliche Zahl x gilt $\eta_j(a) > x$ für alle $j > x$. Jedoch gilt $K_0^{(\xi)}(\Diamond\Box\forall x a > x) = \text{ff}$, denn für alle i ist $\eta_i(a) \leq i$.

Bemerkung: Für das Gegenbeispiel zur zweiten Formel ist es wesentlich, daß über eine unendliche Wertemenge quantifiziert wird: Aus $\models \Diamond\Box A \wedge \Diamond\Box B \leftrightarrow \Diamond\Box(A \wedge B)$ folgt, daß \forall und $\Diamond\Box$ für endliche Wertebereiche kommutieren.

- b) Die erste Formel ist die "fehlende Richtung" von (tl5):

$$\begin{aligned} (1) \quad & A \rightarrow \exists x A && \text{(tl4)} \\ (2) \quad & \circ(A \rightarrow \exists x A) && \text{(nex)(1)} \\ (3) \quad & \circ A \rightarrow \circ\exists x A && \text{(2)(tl2)(prop)} \\ (4) \quad & \exists x \circ A \rightarrow \circ\exists x A && \text{(par)(3)} \end{aligned}$$

Für die Herleitung braucht man (indunless) und das Rekursionsgesetz für **unless**:

$$\begin{aligned} (1) \quad & A \text{ unless } B \rightarrow \circ B \vee (\circ A \wedge \circ(A \text{ unless } B)) && \text{(unl2)(T15)} \\ (2) \quad & \circ A \rightarrow \circ\exists x A && \text{(s.o.)} \\ (3) \quad & A \text{ unless } B \rightarrow \circ B \vee (\circ\exists x A \wedge \circ(A \text{ unless } B)) && \text{(1)(2)} \\ (4) \quad & A \text{ unless } B \rightarrow (\exists x A) \text{ unless } B && \text{(indunless)(3)} \\ (5) \quad & \exists x (A \text{ unless } B) \rightarrow (\exists x A) \text{ unless } B && \text{(par)(4)} \end{aligned}$$

Aufgabe 9-2 Programmverifikation mit Temporallogik

In den folgenden Herleitungen benutzen wir meist die leichter lesbaren Schreibweisen mit gestrichenen Variablen. Die Anwendung arithmetisch gültiger Aussagen markieren wir mit (data), und dies selbst dann, wenn die jeweilige Instanz gestrichene Variablen enthält. Ferner benutzen wir das Axiom

$$\text{(prime)} \quad P' \leftrightarrow \circ P$$

falls P eine Formel von $\text{kern}(\mathcal{L}_{\text{FOLTL}})$ ohne gestrichene Individuensymbole ist und P' die Formel bezeichnet, die aus P durch Ersetzen aller Individuensymbole $a \in \mathcal{X}^F$ durch a' entsteht.

- a) $I \rightarrow \Box(b = 2 * a + 1 \wedge c = (a + 1) * (a + 1) \wedge a * a \leq n)$
- (1) $c \leq n \rightarrow a' = a + 1 \wedge b' = b + 2 \wedge c' = c + b'$ (Ann.)
 - (2) $c > n \rightarrow a' = a \wedge b' = b \wedge c' = c$ (Ann.)
 - (3) $I \rightarrow b = 2 * a + 1 \wedge c = (a + 1) * (a + 1) \wedge a * a \leq n$ (data)
 - (4) $b = 2 * a + 1 \wedge b' = b + 2 \rightarrow b' = 2 * (a + 1) + 1$ (data)
 - (5) $b' = 2 * (a + 1) + 1 \wedge a' = a + 1 \rightarrow b' = 2 * a' + 1$ (pred)
 - (6) $c = (a + 1) * (a + 1) \wedge c' = c + b' \wedge b' = 2 * a' + 1 \wedge a' = a + 1$
 $\rightarrow c' = (a + 1) * (a + 1) + 2 * (a + 1) + 1$ (pred)
 - (7) $c' = (a + 1) * (a + 1) + 2 * (a + 1) + 1 \wedge a' = a + 1$
 $\rightarrow c' = (a' + 1) * (a' + 1)$ (data)
 - (8) $c = (a + 1) * (a + 1) \wedge a' = a + 1 \wedge c \leq n \rightarrow a' * a' \leq n$ (pred)
 - (9) $c \leq n \wedge b = 2 * a + 1 \wedge c = (a + 1) * (a + 1) \wedge a * a \leq n$
 $\rightarrow b' = 2 * a' + 1 \wedge c' = (a' + 1) * (a' + 1) \wedge a' * a' \leq n$ (1)(4)–(8)
 - (10) $b = 2 * (a + 1) \wedge a' = a \wedge b' = b \rightarrow b' = 2 * (a' + 1)$ (pred)
 - (11) $c = (a + 1) * (a + 1) \wedge a' = a \wedge c' = c \rightarrow c' = (a' + 1) * (a' + 1)$ (pred)
 - (12) $a * a \leq n \wedge a' = a \rightarrow a' * a' \leq n$ (pred)
 - (13) $c > n \wedge b = 2 * a + 1 \wedge c = (a + 1) * (a + 1) \wedge a * a \leq n$
 $\rightarrow b' = 2 * a' + 1 \wedge c' = (a' + 1) * (a' + 1) \wedge a' * a' \leq n$ (2)(10)–(12)
 - (14) $b = 2 * a + 1 \wedge c = (a + 1) * (a + 1) \wedge a * a \leq n$
 $\rightarrow \circ(b = 2 * a + 1 \wedge c = (a + 1) * (a + 1) \wedge a * a \leq n)$ (9)(13)
 - (15) $I \rightarrow \Box(b = 2 * a + 1 \wedge c = (a + 1) * (a + 1))$ (ind2)(3)(14)

- b) $I \rightarrow \Box(c > n \rightarrow a * a \leq n \wedge n < (a + 1) * (a + 1))$
- (1) $I \rightarrow \Box(a * a \leq n \wedge c = (a + 1) * (a + 1))$ (Teilaufg. a)
 - (2) $a * a \leq n \wedge c = (a + 1) * (a + 1)$
 $\rightarrow (c > n \rightarrow a * a \leq n \wedge n < (a + 1) * (a + 1))$ (pred)
 - (3) $\Box(a * a \leq n \wedge c = (a + 1) * (a + 1))$
 $\rightarrow \Box(c > n \rightarrow a * a \leq n \wedge n < (a + 1) * (a + 1))$ (2)(alw)(T19)
 - (4) $I \rightarrow \Box(c > n \rightarrow a * a \leq n \wedge n < (a + 1) * (a + 1))$ (1)(3)

- c) $I \rightarrow \Diamond(c > n)$

Die Ordnung \leq auf \mathbb{N}_0 ist fundiert, wir können also einfach NAT als Sorte wf einer Sprache \mathcal{L}_{FOLTL}^f mit fundierter Ordnung \leq benutzen. Als Maß für den Fortschritt der Berechnung bietet es sich an, die Differenz $n - c$ zu benutzen, da c mit jedem Schritt wächst, solange $c \leq n$ gilt.

Formal setzen wir $A \equiv c + z = n$ und benutzen die Regel (wfo). Zunächst leiten wir her

$$\mathcal{F}, b > 0 \vdash \Diamond(c > n)$$

- (1) $c \leq n \rightarrow a' = a + 1 \wedge b' = b + 2 \wedge c' = c + b'$ (Ann.)
- (2) $b > 0$ (Ann.)
- (3) $c + z = n \rightarrow c \leq n$ (data)
- (4) $c + z = n \wedge c' = c + b' \wedge b' > 0 \rightarrow c' > n \vee \exists \bar{z}(\bar{z} < z \wedge c' + \bar{z} = n)$ (data)
- (5) $b' > 0$ (2)(nex)
- (6) $c + z = n \rightarrow \circ(c > n \vee \exists \bar{z}(\bar{z} < z \wedge c + \bar{z} = n))$ (1)(3)(4)(5)

- (7) $A \rightarrow \diamond(c > n \vee \exists \bar{z}(\bar{z} < z \wedge A_z(\bar{z})))$ (6)(T7)
(8) $\exists z A \rightarrow \diamond(c > n)$ (wfo)(7)
(9) $c \leq n \rightarrow \exists z(c + z = n)$ (data)
(10) $c > n \rightarrow \diamond(c > n)$ (T5)
(11) $\diamond(c > n)$ (8)–(10)

Mit dem Deduktionstheorem folgt daraus

$$\mathcal{F} \vdash \Box(b > 0) \rightarrow \diamond(c > n)$$

Andererseits folgt mit Teilaufgabe (a), einfacher Temporallogik und (data)

$$\mathcal{F} \vdash I \rightarrow \Box(b > 0)$$

Zusammen erhalten wir daher $\mathcal{F} \vdash I \rightarrow \diamond(c > n)$, was zu zeigen war.

Aufgabe 9-3

Elektronisches Schaltwerk

- a) 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 $\eta : \{v_0, v_1, v_2\} \rightarrow \{\text{tt}, \text{ff}\}$ ist in S enthalten) und der Zustandsübergangsrelation T wie folgt:

$$(\eta, \eta') \in T \iff \left\{ \begin{array}{l} \eta'(v_0) = \text{tt} \iff \eta(v_0) = \text{ff}, \\ \eta'(v_1) = \text{tt} \iff \eta(v_1) \neq \eta(v_0), \\ \eta'(v_2) = \text{tt} \iff \eta(v_2) \neq \eta(v_0 \wedge v_1) \end{array} \right\}$$

Insbesondere ist T (links-)total.

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

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

- c) Wir leiten die Formel $\diamond \neg v_1$ (und daraus $\Box \diamond \neg v_1$) her, durch Fallunterscheidung nach dem Ausgangszustand.

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