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

WS 2006/2007
Übungsblatt 5

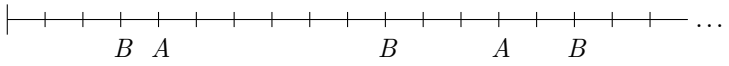
Temporale Logik und Zustandssysteme Lösungsvorschlag

Aufgabe 5-1 **Temporale Aussagen von $\mathcal{L}^{\mathrm{b}}_{\mathrm{LTL}}$** (4 Punkte)

Seien A und B Formeln von $\mathcal{L}^{\mathrm{b}}_{\mathrm{LTL}}$. Geben Sie Formeln von $\mathcal{L}^{\mathrm{b}}_{\mathrm{LTL}}$ mit den folgenden jeweiligen informellen Bedeutungen an.

a) „Falls B unendlich oft zutrifft, trifft A zwischen zwei Zutreffen von B mindestens einmal zu."

Lösung: $\Box\Diamond B \rightarrow \Box(B \rightarrow (A \textbf{ before } B))$

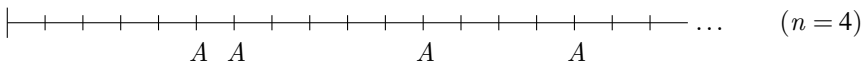


b) „A trifft ab dem nächsten Zustand genau n-mal zu."

Lösung: $\neg A$ **until** $(A \wedge (\neg A$ **until** $A \wedge \ldots (\neg A$ **until** $A \wedge \circ\Box\neg A)\ldots))$ mit n-mal **until**

oder rekursiv geschrieben als

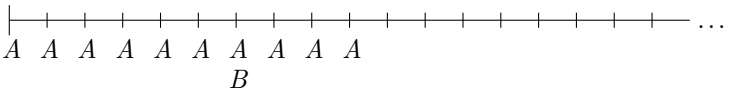
$$\phi_0 \equiv \circ\Box\neg A$$
$$\phi_{i+1} \equiv (\neg A \textbf{ until } A \wedge \phi_i)$$



$(n = 4)$

c) „Solange A ununterbrochen zutrifft, trifft B maximal einmal zu."

Lösung: $(B \rightarrow (\neg B$ **unless** $\neg A))$ **unless** $\neg A$



Aufgabe 5-2 **Allgemeingültigkeit in LTL+b** (4 Punkte)

Seien A, B Formeln von $\mathcal{L}^{\mathrm{b}}_{\mathrm{LTL}}$. Beweisen oder widerlegen Sie folgende Aussagen:

a) $\models \Box A \leftrightarrow A \wedge$ **false atnext** $\neg A$

Lösung: Allgemeingültig, wie man leicht zeigt. Sei K beliebig, $i \in \mathbb{N}$.

$$\begin{aligned}
\mathsf{K}_i(\Box A) = \mathsf{tt} &\text{ gdw. } \mathsf{K}_j(A) = \mathsf{tt} \text{ für alle } j \geq i \\
&\text{gdw. } \mathsf{K}_i(A) = \mathsf{tt} \text{ und } \mathsf{K}_j(A) = \mathsf{tt} \text{ für alle } j > i \\
&\text{gdw. } \mathsf{K}_i(A) = \mathsf{tt} \text{ und } \mathsf{K}_j(\neg A) = \mathsf{ff} \text{ für alle } j > i \\
&\text{gdw. } \mathsf{K}_i(A) = \mathsf{tt} \text{ und entweder } \mathsf{K}_j(\neg A) = \mathsf{ff} \text{ für alle } j > i \\
&\qquad \text{oder } \mathsf{K}_k(\textbf{false}) = \mathsf{tt} \text{ für das kleinste } k > i \text{ mit } K_k(\neg A) = \mathsf{tt} \\
&\text{gdw. } \mathsf{K}_i(A \wedge \textbf{false atnext } \neg A) = \mathsf{tt}
\end{aligned}$$

b) A **unless false** $\models \Box A$

Lösung: Nicht gültig. Betrachte $A \equiv v_0 \in \mathbf{V}$ eine Aussagenvariable und die Struktur $\mathsf{K} = (\eta_0, \eta_1, \ldots)$ mit

$$\eta_i(v_0) = \begin{cases} \mathsf{tt} & \text{für } i \geq 1 \\ \mathsf{ff} & \text{sonst} \end{cases}$$

Es gilt $\mathsf{K}_i(A) = \mathsf{tt}$ für alle $i \geq 1$, und daher $\mathsf{K}_i(A$ **unless false**$) = \mathsf{tt}$ für alle $i \in \mathbb{N}$, d.h. $\models_{\mathsf{K}} A$ **unless false**. Es gilt aber $\eta_0(A) = \mathsf{ff}$, insbesondere also $\mathsf{K}_0(\Box A) = \mathsf{ff}$ und damit folgt $\not\models_{\mathsf{K}} \Box A$.

c) $\models A$ **unless** $B \wedge \neg B$ **unless** $C \rightarrow A$ **unless** C

Lösung: Gültig. Sei K beliebig, $i \in \mathbb{N}$, und gelte $\mathsf{K}_i(A$ **unless** $B \wedge \neg B$ **unless** $C) = \mathsf{tt}$. D.h. es gilt entweder

- $\mathsf{K}_j(\neg B) = \mathsf{tt}$ für alle $j > i$, daher $\mathsf{K}_j(B) = \mathsf{ff}$ für alle $j > i$. Dann muß $\mathsf{K}_j(A) = \mathsf{tt}$ für alle $j > i$ gelten und insofern auch $\mathsf{K}_i(A$ **unless** $C) = \mathsf{tt}$.
- Oder es gilt $\mathsf{K}_k(C) = \mathsf{tt}$ für ein $k > i$ und $\mathsf{K}_l(\neg B) = \mathsf{tt}$ für alle $l \in \mathbb{N}$ mit $i < l < k$, daher $\mathsf{K}_l(B) = \mathsf{ff}$ für alle $l \in \mathbb{N}$ mit $i < l < k$, und daher $\mathsf{K}_l(A) = \mathsf{tt}$ für alle $l \in \mathbb{N}$ mit $i < l < k$, also gilt $\mathsf{K}_i(A$ **unless** $C) = \mathsf{tt}$.

Aufgabe 5-3 **Herleitungen in $\Sigma^{\mathrm{b}}_{\mathrm{LTL}}$** (5 Punkte)

Leiten Sie folgende Formeln in $\Sigma^{\mathrm{b}}_{\mathrm{LTL}}$ her. Sie dürfen dabei neben den Axiomen und Regeln von $\Sigma^{\mathrm{b}}_{\mathrm{LTL}}$ (in der Fassung mit **atnext**) auch das Gesetz (T14) sowie die Regeln (prop), (alw) und (indatnext) und selbst hergeleitete Regeln und Axiome verwenden.

a) $\Box A \rightarrow A$ **atnext** B

Lösung: Im Wesentlichen ist nur die Regel (indatnext) vorzubereiten:

$$\text{(indatnext)} \qquad A \rightarrow \bigcirc(C \rightarrow B) \wedge \bigcirc(\neg C \rightarrow A) \vdash A \rightarrow B \textbf{ atnext } C$$

hier instanziiert als

$$\Box A \rightarrow \bigcirc(B \rightarrow A) \wedge \bigcirc(\neg B \rightarrow \Box A) \vdash \Box A \rightarrow A \textbf{ atnext } B$$

(1)	$\Box A \rightarrow A$	(ltl3)(prop)
(2)	$\bigcirc\Box A \rightarrow \bigcirc A$	(nex)(1)(ltl2)(prop)
(3)	$\Box A \rightarrow \bigcirc\Box A$	(ltl3)(prop)
(4)	$\Box A \rightarrow \bigcirc A$	(prop)(2)(3)
(5)	$\Box A \wedge \bigcirc B \rightarrow \bigcirc A$	(prop)(4)
(6)	$\Box A \rightarrow (\bigcirc B \rightarrow \bigcirc A)$	(prop)(5)
(7)	$\Box A \rightarrow \bigcirc(B \rightarrow A)$	(T14)(prop)(6)
(8)	$\Box A \rightarrow (\bigcirc\neg B \rightarrow \bigcirc\Box A)$	(prop)(3)
(9)	$\Box A \rightarrow \bigcirc(\neg B \rightarrow \Box A)$	(T14)(prop)(8)
(10)	$\Box A \rightarrow \bigcirc(B \rightarrow A) \wedge \bigcirc(\neg B \rightarrow \Box A)$	(prop)(7)(9)
(11)	$\Box A \rightarrow A$ **atnext** B	(indatnext)(10)

b) $\Box A \leftrightarrow A \wedge A$ **unless false**

Lösung:

(1)	$\Box A \rightarrow A \wedge \bigcirc\Box A$	(ltl3)
(2)	$\bigcirc\Box A \rightarrow A$ **unless false**	(unl1)
(3)	$\Box A \rightarrow A \wedge A$ **unless false**	(prop)(1)(2)
(4)	$A \wedge A$ **unless false** $\rightarrow A$	(taut)
(5)	A **unless false** $\rightarrow \bigcirc$**false** $\vee \bigcirc(A \wedge A$ **unless false**$)$	(unl2)(prop)
(6)	$\neg$**false**	(taut)
(7)	$\bigcirc\neg$**false**	(nex)(6)
(8)	$\neg\bigcirc$**false**	(7)(ltl1)(prop)
(9)	$A \wedge A$ **unless false** $\rightarrow \bigcirc(A \wedge A$ **unless false**$)$	(prop)(5)(8)
(10)	$A \wedge A$ **unless false** $\rightarrow \Box A$	(ind)(4)(9)
(11)	$\Box A \leftrightarrow A \wedge A$ **unless false**	(prop)(3)(10)

Aufgabe 5-4 **Ausdrucksstärke von LTL** (keine Abgabe)

Der Operator **even** mit der informellen Bedeutung „an allen Zeitpunkten mit geradzahligem Abstand“ sei definiert durch:

$$\mathsf{K}_i(\textbf{even}\ A) = \mathsf{tt} \qquad \Longleftrightarrow \qquad \mathsf{K}_{i+2k}(A) = \mathsf{tt} \quad \text{für alle } k \in \mathbb{N}.$$

In dieser Aufgabe soll gezeigt werden, dass der Operator **even** in $\mathcal{L}_{\mathrm{LTL}}$ nicht definierbar ist. Dazu sei v eine Aussagenkonstante, und für alle $j \geq 0$ sei die temporale Struktur $\mathsf{K}^j = (\eta_0^j, \eta_1^j, \ldots)$ gegeben durch

$$\eta_k^j(v) = \mathsf{ff} \iff k = j \qquad \text{und} \qquad \eta_k^j(w) = \mathsf{ff} \text{ für alle } w \not\equiv v$$

a) Zeigen Sie, dass für alle $j \geq 0$ und alle Formeln A von $\mathcal{L}_{\mathrm{LTL}}$ gilt: $\mathsf{K}_0^{j+1}(\bigcirc A) = \mathsf{K}_0^j(A)$.

Lösung: Nach Definition der η_k^j gilt für alle $j, k \in \mathbb{N}$ und alle $w \in \mathbf{V}$, dass $\eta_{k+1}^{j+1} = \eta_k^j$. Nach Lemma 2.1.5 folgt daher $\mathsf{K}_{k+1}^{j+1}(A) = \mathsf{K}_k^j(A)$ für alle j, k und alle Formeln A von $\mathcal{L}_{\mathrm{LTL}}$. Insbesondere folgt

$$\mathsf{K}_0^{j+1}(\bigcirc A) = \mathsf{K}_1^{j+1}(A) = \mathsf{K}_0^j(A)$$

b) Zeigen Sie: Für alle Formeln A in $\mathcal{L}_{\mathrm{LTL}}$ gibt es ein $l \geq 0$, so dass $\mathsf{K}_0^j(A) = \mathsf{K}_0^l(A)$ für alle $j \geq l$.

Lösung: Dies ist das eigentliche Kernstück des Beweises: Jede Formel in $\mathcal{L}_{\mathrm{LTL}}$ kann nur endlich viele Strukturen K^j unterscheiden. Formal zeigen wir: Für jede $\mathcal{L}_{\mathrm{LTL}}$-Formel A gibt es ein $l \in \mathbb{N}$, so dass gilt:

(b1) für alle $j \geq l$ ist $\mathsf{K}_0^j(A) = \mathsf{tt}$ oder

(b2) für alle $j \geq l$ ist $\mathsf{K}_0^j(A) = \mathsf{ff}$.

Der Beweis erfolgt durch Induktion nach dem Formelaufbau.

$A \in \mathbf{V}$: Ist $A \equiv v$, so ist $\mathsf{K}_0^j(A) = \mathsf{tt}$ für alle $j \geq 1$; die Behauptung gilt also für $l = 1$. Für $\mathbf{V} \ni A \not\equiv v$ ist $\mathsf{K}_0^j(A) = \mathsf{ff}$ für alle $j \in \mathbb{N}$, also gilt die Behauptung für $l = 0$.

$A \equiv \textbf{false}$: trivial mit $l = 0$.

$A \equiv A_1 \to A_2$: Nach Ind.ann. existieren l_1, l_2 wie gefordert für A_1 und A_2. Es sei $l = \max(l_1, l_2)$.

- Ist $\mathsf{K}_0^j(A_1) = \mathsf{ff}$ oder $\mathsf{K}_0^j(A_2) = \mathsf{tt}$ für alle $j \geq l$, so folgt $\mathsf{K}_0^j(A) = \mathsf{tt}$ für alle $j \geq l$.
- Ist $\mathsf{K}_0^j(A_1) = \mathsf{tt}$ und $\mathsf{K}_0^j(A_2) = \mathsf{ff}$ für alle $j \geq l$, so folgt $\mathsf{K}_0^j(A) = \mathsf{ff}$ für alle $j \geq l$.

$A \equiv \bigcirc A_1$: Nach Ind.ann. existiert l_1 wie gefordert für A_1. Daher gilt für alle $j \geq l_1$

$$\mathsf{K}_0^{j+1}(\bigcirc A_1) \overset{(a)}{=} \mathsf{K}_0^j(A_1) \overset{I.V.}{=} \mathsf{K}_0^{l_1}(A_1) \overset{(a)}{=} \mathsf{K}_0^{l_1+1}(\bigcirc A)$$

Die Aussage gilt also für $l = l_1 + 1$.

$A \equiv \Box A_1$: Nach Ind.ann. existiert l_1 wie gefordert für A_1. Wir setzen $l = l_1$ und zeigen, dass $\mathsf{K}_0^j(\Box A_1) = \mathsf{K}_0^l(\Box A_1)$ gilt für alle $j \geq l$. Der Beweis erfolgt durch (Neben-)Induktion nach $j \geq l$.

$j = l$: trivial.

$j \to j+1$:

$$\begin{array}{lll} & \mathsf{K}_0^{j+1}(\Box A_1) = \mathsf{tt} & \\ \Longleftrightarrow & \mathsf{K}_0^{j+1}(A_1) = \mathsf{tt} \text{ und } \mathsf{K}_0^{j+1}(\bigcirc\Box A_1) = \mathsf{tt} & \text{[T23]} \\ \Longleftrightarrow & \mathsf{K}_0^{l}(A_1) = \mathsf{tt} \text{ und } \mathsf{K}_0^{j}(\Box A_1) = \mathsf{tt} & \text{[Haupt-Ind.vor., Teilaufg. (a)]} \\ \Longleftrightarrow & \mathsf{K}_0^{l}(A_1) = \mathsf{tt} \text{ und } \mathsf{K}_0^{l}(\Box A_1) = \mathsf{tt} & \text{[Neben-Ind.vor.]} \\ \Longleftrightarrow & \mathsf{K}_0^{l}(\Box A_1) = \mathsf{tt} & \text{[T4]} \end{array}$$

c) Folgern Sie, dass es keine Formel A von $\mathcal{L}_{\mathrm{LTL}}$ gibt mit $\models A \leftrightarrow \textbf{even}\ v$.

Lösung: Betrachten wir zunächst einige naheliegende Versuche einer Definition von **even** A in $\mathcal{L}_{\mathrm{LTL}}$:

$A \wedge \Box(A \to \bigcirc\neg A \wedge \bigcirc\bigcirc A)$: Diese Formel verlangt, dass A *genau* in den Zeitpunkten mit geradzahligem Abstand zutrifft, also in den Zeitpunkten mit ungeradem Abstand falsch ist. Dagegen trifft **even** A keine Aussage über das Zutreffen von A in Zeitpunkten mit ungeradem Abstand.

$A \wedge \Box(A \to \bigcirc\bigcirc A)$: Diese Formel verlangt immer noch, dass von “jetzt” an (Zeitpunkt i) A jeweils im Zeitpunkt $i + n + 2$ gilt, wenn A im Zeitpunkt $i + n$ gilt. Ist insbesondere A in einem zukünftigen Zeitpunkt mit ungeradem Abstand wahr, so muss A ab diesem Zeitpunkt in allen Zuständen wahr sein; auch dies ist stärker als **even** A. Ähnliches gilt für $A \wedge \Box(A \leftrightarrow \bigcirc\bigcirc A)$.

$p \wedge \Box(p \to \bigcirc\neg p \wedge \bigcirc\bigcirc p) \wedge \Box(p \to A)$: Dabei sei p eine "neue" atomare Aussage, die nicht in A vorkommt. Diese Formel verlangt, dass p *genau* in den Zeitpunkten mit geradzahligem Abstand zutrifft, und dass A mindestens dann wahr ist, wenn p wahr ist. Dies trifft die Aussage von **even** A ziemlich gut, insbesondere fordert die Formel nichts über das Zutreffen von A in Zeitpunkten mit ungeradem Abstand. Allerdings macht die Formel Aussagen über p (ein "Implementierungsdetail"), was **even** A offensichtlich nicht macht.

Der letzte Versuch führt uns zu folgender Beobachtung: Würden wir quantifizierte Aussagenvariablen in der temporalen Aussagenlogik erlauben, so könnten wir **even** A definieren durch

$$\textbf{even}\ A \ =_{\text{def}}\ \exists p : p \wedge \Box(p \leftrightarrow \bigcirc\bigcirc p) \wedge \Box(p \to A)$$

Zur Aufgabenlösung: Angenommen, A wäre eine $\mathcal{L}_{\text{LTL}}$-Formel mit $\models\ A \leftrightarrow$ **even** v, insbesondere $\mathsf{K}_0^j(A) = \mathsf{K}_0^j(\textbf{even}\ v)$ für alle $j \in \mathbb{N}$. Nach Teilaufgabe (b) existiert ein $l \geq 0$, so dass entweder Bedingung (b1) oder Bedingung (b2) gilt für alle $j \geq l$. Andererseits gilt $\mathsf{K}_0^j(\textbf{even}\ v) = \mathsf{tt}$ genau dann, wenn j ungerade ist, Widerspruch.

Aufgabe 5-5 **Idempotenz und Absorption** (keine Abgabe)

Sei A eine Formel von $\mathcal{L}_{\text{LTL}}$. Beweisen Sie die folgenden Aussagen:

a) $\models \Diamond\Box\Diamond A \leftrightarrow \Box\Diamond A$

Lösung: Für beliebiges K und beliebiges $i \in \mathbb{N}$:

$$\begin{aligned}
\mathsf{K}_i(\Diamond\Box\Diamond A) = \mathsf{tt} &\Leftrightarrow \mathsf{K}_j(\Box\Diamond A) = \mathsf{tt} \text{ für ein } j \geq i \\
&\Leftrightarrow \mathsf{K}_k(\Diamond A) = \mathsf{tt} \text{ für alle } k \geq j \text{ für ein } j \geq i \\
&\Leftrightarrow \mathsf{K}_l(A) = \mathsf{tt} \text{ für ein } l \geq k \text{ für alle } k \geq j \text{ für ein } j \geq i \\
&\Leftrightarrow \mathsf{K}_l(A) = \mathsf{tt} \text{ für ein } l \geq k \text{ für alle } k \geq i \\
&\Leftrightarrow \mathsf{K}_k(\Diamond A) = \mathsf{tt} \text{ für alle } k \geq i \\
&\Leftrightarrow \mathsf{K}_k(\Box\Diamond A) = \mathsf{tt}
\end{aligned}$$

b) $\models \Box\Diamond\Box A \leftrightarrow \Diamond\Box A$

Lösung:

$$\begin{aligned}
\mathsf{K}_i(\Box\Diamond\Box A) = \mathsf{tt} &\Leftrightarrow \mathsf{K}_j(\Diamond\Box A) = \mathsf{tt} \text{ für alle } j \geq i \\
&\Leftrightarrow \mathsf{K}_k(\Box A) = \mathsf{tt} \text{ für ein } k \geq j \text{ für alle } j \geq i \\
&\Leftrightarrow \mathsf{K}_l(A) = \mathsf{tt} \text{ für alle } l \geq k \text{ für ein } k \geq j \text{ für alle } j \geq i \\
&\Leftrightarrow \mathsf{K}_l(A) = \mathsf{tt} \text{ für alle } l \geq k \text{ für ein } k \geq i \\
&\Leftrightarrow \mathsf{K}_k(\Box A) = \mathsf{tt} \text{ für ein } k \geq i \\
&\Leftrightarrow \mathsf{K}_k(\Diamond\Box A) = \mathsf{tt}
\end{aligned}$$

Nimmt man noch die Regeln $\models \Diamond\Diamond A \leftrightarrow \Diamond A$ und $\models \Box\Box A \leftrightarrow \Box A$ hinzu, kann man einen interessanten Satz zeigen:

Satz 1. *Sei $F \equiv \boxtimes_1 \boxtimes_2 \ldots \boxtimes_n A$ mit $n \geq 1$ eine Formel von $\mathcal{L}_{\text{LTL}}$, wobei $\boxtimes_i$ entweder $\Box$ oder $\Diamond$ ist. Dann gibt es eine Formel $F' \equiv$ **pref**A mit* **pref** *aus $\Box, \Diamond, \Box\Diamond, \Diamond\Box$, und es gilt*

$$\models F \leftrightarrow F'$$

Beweis. Per Induktion über n. Der Fall $n = 1$ ist trivial ($F \equiv \Box A$ oder $F \equiv \Diamond A$). Für $n > 1$ gilt nach Induktionsvoraussetzung, daß $\boxtimes_1 \ldots \boxtimes_{n-1} A$ äquivalent zu einer Formel **pref**$'A$ ist, mit **pref**$'$ wie beschrieben. Ist **pref**$'$ entweder $\Box$ oder $\Diamond$, so ist entweder **pref**$' \boxtimes_n A$ bereits syntaktisch gleich zu einer geforderten Formel, oder die Regel $\models \Box\Box A \leftrightarrow \Box A$ respektive $\models \Diamond\Diamond A \leftrightarrow \Diamond A$ kann angewendet werden. Ist **pref**$'$ entweder $\Box\Diamond$ oder $\Diamond\Box$, so kann entweder die eben genannten Regeln auf **pref**$' \boxtimes_n A$ angewendet werden, oder die Regeln b. und c.; in jedem Fall findet sich eine zu F äquivalente Formel $F' \equiv$ **pref**A. □

Abgabe: Mittwoch, den 22.11.2006, vor der Übung.