Name	Vorname	Matrikelnummer
Hauptfach	Nebenfach	Universität/Geburtsdatum (falls nicht Stud. der LMU)

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

WS 2006/2007
Klausur
7.2.2007, 12 – 14 Uhr

Temporale Logik und Zustandssysteme

Aufgabe 1 **Semantik** (8 Punkte)

Beweisen oder widerlegen Sie folgende Beziehungen:

a) $\models \boxminus\Box A \rightarrow \ominus\bigcirc A$ in der Logik LTL+p.

Lösung: Nicht gültig. Sei $\mathsf{K} = (\eta_0, \eta_1, \ldots)$ eine Kripkestruktur mit $K_i(A) = \mathsf{tt}$ für alle $i \in \mathbb{N}$. Es gilt $\mathsf{K}_0(\Box A) = \mathsf{tt}$ und somit auch $\mathsf{K}_0(\boxminus\Box A) = \mathsf{tt}$, nach Definition gilt jedoch $\mathsf{K}_0(\ominus B) = \mathsf{ff}$ und insofern $\mathsf{K}_0(\boxminus\Box A \rightarrow \ominus\bigcirc A) = \mathsf{ff}$. Dies ist ein Zeuge für $\not\models \boxminus\Box A \rightarrow \ominus\bigcirc A$. (3 Punkte.)

b) $A \rightarrow B, A \rightarrow \mathsf{A}\bigcirc A \models A \rightarrow \mathsf{A}\Box B$ in der Logik BTL.

Lösung: Sei $\mathsf{K} = (\{\eta_\iota\}_{\iota \in I}, \twoheadrightarrow)$ eine verzweigte temporale Struktur mit $\mathsf{K}_\iota(A \rightarrow B) = \mathsf{tt}$ und $\mathsf{K}_\iota(A \rightarrow \mathsf{A}\bigcirc A) = \mathsf{tt}$. Wähle $\kappa \in I$ beliebig. Wenn $\eta_\kappa(A) = \mathsf{ff}$, sind wir fertig, gelte also $\eta_\kappa(A) = \mathsf{tt}$. Zu zeigen ist $\mathsf{K}_{\kappa_i}(B) = \mathsf{tt}$ für alle Pfade $(\kappa_0, \kappa_1, \ldots)$ in I mit $\kappa_0 = \kappa$. Annahme: es gibt einen Pfad $(\kappa_0, \kappa_1, \ldots)$ in I, der dies verletzt, also es gibt ein $i \in \mathbb{N}$ mit $\eta_{\kappa_i}(B) = \mathsf{ff}$. Dann gilt auch $\eta_{\kappa_i}(A) = \mathsf{ff}$. Sei $j \leq i$ minimal mit $\eta_{\kappa_j}(A) = \mathsf{ff}$. Da $\eta_{\kappa_0}(A) = \mathsf{tt}$, gilt $0 < j \leq i$. Da $\mathsf{K}_{\kappa_{j-1}}(A \rightarrow \mathsf{A}\bigcirc A) = \mathsf{tt}$ gilt, muß $\eta_{\kappa_{j-1}}(A) = \mathsf{ff}$ gelten, Widerspruch zu j minimal. (5 Punkte.)

Aufgabe 2 **Herleitungen** (10 Punkte)

Beweisen Sie folgende Beziehungen für Formeln der Logik LTL+b. Verwenden Sie dabei in Herleitungen nur die Axiome und Regeln von Σ^b_{LTL} sowie (T15) und (prop). Außerdem dürfen Sie gegebenenfalls das Deduktionstheorem anwenden.

a) $\bigcirc A \vdash \bigcirc\Box A$.

Lösung:

(1)	$\bigcirc A$	(Ann)
(2)	$A \rightarrow \bigcirc A$	(prop)(1)
(3)	$A \rightarrow A$	(taut)
(4)	$A \rightarrow \Box A$	(ind)(2)(3)
(5)	$\bigcirc(A \rightarrow \Box A)$	(nex)(4)
(6)	$\bigcirc(A \rightarrow \Box A) \rightarrow (\bigcirc A \rightarrow \bigcirc\Box A)$	(ltl2)
(7)	$\bigcirc A \rightarrow \bigcirc\Box A$	(mp)(5)(6)
(8)	$\bigcirc\Box A$	(mp)(1)(7)

(4 Punkte)

b) $\vdash A$ **unless** $B \wedge \Box\neg B \rightarrow \circ\Box A$.

Lösung:

(1)	A **unless** $B \rightarrow \circ B \vee \circ A$	(unl2)(T15)(prop)
(2)	$\Box\neg B \rightarrow \neg B$	(ltl3)(prop)
(3)	$\circ\Box\neg B \rightarrow \circ\neg B$	(nex)(2)(ltl2)(prop)
(4)	$\Box\neg B \rightarrow \circ\Box\neg B$	(ltl3)(prop)
(5)	$\Box\neg B \rightarrow \circ\neg B$	(3)(4)(prop)
(6)	$\Box\neg B \rightarrow \neg\circ B$	(ltl1)(prop)(5)
(7)	A **unless** $B \wedge \Box\neg B \rightarrow \circ A$	(prop)(1)(6)
(8)	A **unless** $B \wedge \Box\neg B \rightarrow \circ(A \wedge A$ **unless** $B) \wedge \circ\Box\neg B$	(unl2)(6)(4)(prop)
(9)	A **unless** $B \wedge \Box\neg B \rightarrow \circ(A$ **unless** $B \wedge \Box\neg B)$	(T15)(8)(prop)
(10)	A **unless** $B \wedge \Box\neg B \rightarrow \Box\circ A$	(ind)(7)(9)
(11)	$\Box\circ A \rightarrow \circ\Box A$	a), Deduktionstheorem
(12)	A **unless** $B \wedge \Box\neg B \rightarrow \circ\Box A$	(prop)(10)(11)

(6 Punkte)

Aufgabe 3 **Modifizierter Zähler** (8 Punkte)

In der Vorlesung wurde ein Zähler Γ_{count} angegeben, der durch die Menge $\mathcal{A}_{\Gamma_{count}}$ folgender Axiome spezifiziert wurde:

- (data$_{\Gamma_{count}}$),
- $ein \rightarrow (ein' \wedge c' = c + 1) \vee (\neg ein' \wedge c' = c)$,
- $\neg ein \rightarrow (\neg ein' \wedge c' = c) \vee (ein' \wedge c' = 0)$.

a) Der Zähler soll nun soweit verändert werden, dass er nur noch bis 100 zählen kann und, falls er diesen Wert erreicht, sich automatisch ausschaltet. Er soll dann auch nicht mehr gestartet werden können. Geben Sie eine passende Axiomenmenge $\mathcal{A}_{\Gamma_{bcount}}$ zur Spezifikation eines solchen Zählers an.

Lösung:

(CB1) (data$_{\Gamma_{bcount}}$),

(CB2) $ein \rightarrow (c < 100 \wedge ein' \wedge c' = c + 1) \vee (c = 100 \wedge \neg ein' \wedge c' = 100) \vee (\neg ein' \wedge c' = c)$,

(CB3) $\neg ein \rightarrow (\neg ein' \wedge c' = c) \vee (c < 100 \wedge ein' \wedge c' = 0)$.

(3 Punkte.)

b) Zeigen Sie, dass

$$\mathcal{A}_{\Gamma_{bcount}} \cup \{c < 100\} \vdash F$$

für alle $F \in \mathcal{A}_{\Gamma_{count}}$ gilt.

Lösung:

(1)	A für alle Zustandsformeln A von Γ mit $\models_{S_{\Gamma_{count}}} A$	(data$_{\Gamma_{bcount}}$)
(2)	$ein \rightarrow (c < 100 \wedge ein' \wedge c' = c + 1) \vee (c = 100 \wedge \neg ein' \wedge c' = 100) \vee (\neg ein' \wedge c' = c)$	(CB2)
(3)	$c < 100$	(Vorr)(ltl3)(prop)
(4)	$ein \rightarrow (c < 100 \wedge ein' \wedge c' = c + 1) \vee (\neg ein' \wedge c' = c)$	(prop)(2)(3)
(5)	$ein \rightarrow (ein' \wedge c' = c + 1) \vee (\neg ein' \wedge c' = c)$	(prop)(2)(4)
(6)	$\neg ein \rightarrow (\neg ein' \wedge c' = c) \vee (c < 100 \wedge ein' \wedge c' = 0)$	(CB3)
(7)	$\neg ein \rightarrow (\neg ein' \wedge c' = c) \vee (ein' \wedge c' = 0)$	(prop)(3)(6)
(8)	F für alle $F \in \mathcal{A}_{\Gamma_{count}}$	(1)(5)(7)

(3 Punkte)

c) Was bedeutet die Aussage in Teilaufgabe b) informell?

Lösung: „Ein System, dass sich wie der modifizierte Zähler verhält und dabei nie bis 100 zählt, verhält sich wie der ursprüngliche Zähler.“ (2 Punkte)

Aufgabe 4 **Lamports Bakery-Protokoll** (14 Punkte)

Folgendes PAR-Programm modelliert eine vereinfachte Version von Lamports Bakery-Protokoll zum wechselseitigen Ausschluss kritischer Abschnitte in zwei Prozessen. Dabei wird ein Verfahren verwendet, das man aus Behörden kennt: jeder Prozess, der in seinen kritischen Abschnitt eintreten will, zieht ein Ticket mit einer Nummer und wartet dann, bis er das Ticket mit der niedrigsten Nummer hält.

$\Pi \equiv$ **var** $t_1, t_2 : NAT$
start $t_1 = 0 \wedge t_2 = 0$
cobegin

loop	$\alpha_0 : t_1 := t_2 + 1;$		**loop**	$\beta_0 : t_2 := t_1 + 1;$
	α_1 : **await** $t_2 = 0 \vee t_1 < t_2;$			β_1 : **await** $t_1 = 0 \vee t_2 < t_1;$
	α_2 : „kritischer Abschnitt“;	$\|$		β_2 : „kritischer Abschnitt“;
	$\alpha_3 : t_1 := 0;$			$\beta_3 : t_2 := 0;$
end			**end**	

coend

Es sei

$$A \equiv at\,\alpha_2 \rightarrow (t_1 < t_2 \vee t_2 = 0) \wedge t_1 > 0.$$

Es soll gezeigt werden, dass

$$\mathcal{A}_\Pi \vdash \Box A$$

gilt.

a) Für eine Anwendung einer Invarianzregel kann man zunächst versuchen, A selbst als geeignete Invariante zu nehmen, d.h. direkt

$$A \textbf{ invof } Act_\Pi$$

herzuleiten. Begründen Sie, warum A für diesen Ansatz „zu schwach“ ist.

Lösung: Problematisch ist die Aktion α_1: Für einen direkten Nachweis von A **invof** α_1 fehlt die Information, dass $t_1 > 0$ tatsächlich gilt. Direkt gilt $exec\,\alpha_1 \wedge A$ trivialerweise (da $\neg at\,\alpha_2$ gilt), aber $\circ A$ gilt wegen des möglichen $t_1 = 0$ nicht. Man müsste also weiter zurückblicken, um $at\,\alpha_1 \rightarrow t_1 > 0$ zu zeigen. (3 Punkte.)

b) „Verstärken“ Sie A zu einer geeigneten Formel I, und zeigen Sie damit $\mathcal{A}_\Pi \vdash \Box A$.

Lösung: Wir zeigen die Invarianz von $I \equiv (at\,\alpha_2 \rightarrow t_1 < t_2 \vee t_2 = 0) \wedge (at\,\alpha_1 \vee at\,\alpha_2 \rightarrow t_1 > 0)$.

(1)	$start_\Pi \rightarrow I$	(root_Π)(PC)
(2)	I **invof** α_3	(PC)(T14)(T15)
(3)	$exec\,\alpha_0 \rightarrow \circ at\,\alpha_1 \wedge \circ t_1 > 0$	(C1)(ASSIGN)(data)
(4)	$\circ at\,\alpha_1 \rightarrow \circ\neg at\,\alpha_2$	(PC)(nex)(T14)
(5)	$exec\,\alpha_0 \rightarrow \circ\neg at\,\alpha_2$	(3)(4)
(6)	I **invof** α_0	(3)(5)(T14)(T15)
(7)	$exec\,\alpha_1 \rightarrow \circ(t_1 < t_2 \vee t_2 = 0)$	(action)(ASSIGN)(pred)
(8)	$exec\,\alpha_1 \wedge I \rightarrow \circ(t_1 > 0)$	(action)(ASSIGN)(pred)
(9)	I **invof** α_1	(7)(8)(T14)(T15)
(10)	$exec\,\alpha_2 \rightarrow \circ(\neg at\,\alpha_2 \wedge \neg at\,\alpha_1)$	(action)(T15)
(11)	I **invof** α_2	(10)(T14)(T15)
(12)	$exec\,\beta_0 \wedge I \rightarrow \circ(at\,\alpha_1 \vee at\,\alpha_2 \rightarrow t_1 > 0)$	(ASSIGN)(pred)
(13)	$exec\,\beta_0 \rightarrow \circ(t_1 < t2)$	(action)(ASSIGN)(pred)
(14)	I **invof** β_0	(12)(13)(T14)(T15)
(15)	I **invof** $\{\beta_1, \beta_2\}$	(ASSIGN)(pred)(T13)(T14)
(16)	$exec\,\beta_3 \rightarrow \circ(t_2 = 0)$	(ASSIGN)(pred)
(17)	I **invof** β_3	(ASSIGN)(pred)(14)(T14)(T15)
(18)	I **invof** Act_Π	(2)(6)(9)(11)(14)(15)(17)
(19)	$\Box I$	(indstart_Π)(1)(16)
(20)	$I \rightarrow A$	(prop)
(21)	$\Box A$	(alw)(20)(T19)(mp)(19)

(8 Punkte.)

c) Geben Sie eine Formel der Logik FOLTL+b an, die folgenden Sachverhalt beschreibt: „Wenn Prozess 1 sein Ticket gezogen hat, dann tritt Prozess 2 höchstens einmal in seinen kritischen Abschnitt ein, bevor Prozess 1 in seinen kritischen Abschnitt eintritt."

Lösung:

$$t_1 > 0 \rightarrow (exec\,\beta_1 \rightarrow \neg exec\,\beta_1 \textbf{ until } exec\,\alpha_1) \textbf{ until } exec\,\alpha_1$$

(3 Punkte.)