Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Prof. Dr. B. Beckert
Dr. Vladimir Klebanov

Formale Systeme, WS 2009/2010

Übungsblatt 10

Dieses Übungsblatt wird in der Übung am 05.02.2010 besprochen.

Aufgabe 1

Wir betrachten die Modallogik T, bei der nur Modelle $\mathcal{K} = (W, R, I)$ mit einer reflexiven Übergangsrelation R betrachtet werden. Geben Sie ein konkretes T-Modell $\mathcal{K}$ an, so daß $\mathcal{K} \models P \rightarrow \Box\Diamond P$, jedoch $\mathcal{K} \not\models \Diamond P \rightarrow \Box\Diamond P$.

Aufgabe 2

Gegeben sei eine modallogische Signatur, die nur eine atomare Aussage beinhaltet: P. Außerdem sei ein Modell $\mathcal{K} = (W, R, I)$ über dieser Signatur teilweise wie folgt festgelegt:

$$\begin{aligned} W &= \{w_1, w_2, w_3, w_4\} \\ R &= \{(w_1, w_1), (w_2, w_3), (w_2, w_4)\}. \end{aligned}$$

(a) Geben Sie eine Interpretation I für dieses Modell an, so daß: für jedes Weltenpaar $x, y \in W, x \neq y$ gibt es mindestens eine Formel $\phi_{x,y}$ mit $val_x(\phi_{x,y}) \neq val_y(\phi_{x,y})$. Geben Sie die Formel an.

(b) Sei $[\![\phi]\!] = \{w \in W \mid val_w(\phi) = W\}$ für ein $\mathcal{K} = (W, R, I)$. Wir nennen $[\![\phi]\!]$ die *Extension* von ϕ (im Modell $\mathcal{K}$). Ausgehend von dem Modell aus (a) bestimmen Sie:

$$\begin{array}{ll} [\![P]\!] & [\![\neg P]\!] \\ [\![\Box P]\!] & [\![\Diamond P]\!] \\ [\![\Diamond\Box P]\!] & [\![\Box\Diamond P]\!] \end{array}$$

Aufgabe 3

Sind die folgenden modallogischen Formeln in allen Kripke-Strukturen (S, R, I) gültig, deren Erreichbarkeitsrelation R eine Äquivalenzrelation ist? Gebens Sie jeweils, falls die Antwort ja ist, eine Begründung und, falls sie nein ist, ein Gegenbeispiel an.

1. $\Box A \leftrightarrow \Box\Box A$
2. $\Box A \rightarrow \Diamond A$
3. $\Box\Diamond A \rightarrow \Diamond\Box A$
4. $\Diamond A \leftrightarrow \Box\Diamond A$

Aufgabe 4

Java Card DL ist die Logik des KeY-Systems für Verifkation von Java Card Programmen. Es ist eine Modallogik erster Stufe, basiert also auf der PL1, und besitzt für jedes Programm p die Modalitäten $\langle \mathtt{p} \rangle \cdot$ und $[\mathtt{p}]\cdot$. Die Semantik der Modalitäten läßt sich dabei (etwas vereinfacht) anhand einer Kripke-Struktur mit der Menge der Welten[1] S folgendermaßen definieren:

$$val_s([p]\phi) \quad = \quad \begin{cases} W & \text{falls für alle } s' \in S \text{ mit der Eigenschaft} \\ & \text{„}p \text{ gestartet im Zustand } s \text{ terminiert normal (nicht abrupt) in } s'\text{“} \\ & \text{gilt } val_{s'}(\phi) = W \\ F & \text{sonst} \end{cases}$$

$$val_s(\langle p \rangle\phi) \quad = \quad \begin{cases} W & \text{falls ein } s' \in S \text{ existiert mit der Eigenschaft} \\ & \text{„}p \text{ gestartet im Zustand } s \text{ terminiert normal (nicht abrupt) in } s'\text{“} \\ & \text{und } val_{s'}(A) = W \\ F & \text{sonst} \end{cases}$$

Wir nehmen an, daß die Signatur die Symbole für die lokalen Programmvariablen `x` und `y` vom Typ `int` enthält[2] sowie die üblichen mathematischen Operationen auf ganzen Zahlen. Wir beschränken uns auf solche Modelle, in denen diese Operatoren ihre kanonische Bedeutung haben. Was ist dann der Gültigkeitsstatus folgender Java Card DL-Formeln:

1. $\mathtt{x} \doteq 0 \rightarrow \langle \mathtt{x++;} \rangle \mathtt{x} \doteq 1$
2. $[\mathtt{while\ (true);}]\mathit{false}$
3. $\langle \mathtt{while\ (true);} \rangle \mathit{true}$
4. $\mathtt{x} > \mathtt{y} \rightarrow \langle \mathtt{x++;\ y++;} \rangle \mathtt{x} > \mathtt{y}$
5. $\langle p \rangle \phi \rightarrow [p]\phi$ für ein beliebiges Java Card-Programm p und eine beliebige Formel ϕ

Begründen Sie Ihre Antwort.

[1] Die Welten $s \in S$ nennt man bei Programmlogiken üblicherweise auch *Zustände* (engl.: states).

[2] Genaugenommen sind dies sog. *nicht-rigide Konstanten*, also konstante Funktionen, deren Interpretation von Zustand zu Zustand variieren kann.