Übungen zu Grundlagen der Systementwicklung
(Prof. Dr. M. Wirsing, Dr. P. Kosiuczenko, A. Rauschmayer)

Aufgabe 26

Welche der folgenden Eigenschaften (im Kontext des Eisenbahnbeispiels aus der Vorlesung) sind Sicherheits- bzw. Lebendigkeitseigenschaften? Stellen Sie die übrigen Eigenschaften als Durchschnitt von geeigneten Sicherheits- und Lebendigkeitseigenschaften dar. Begründen Sie jeweils kurz Ihre Antwort.

a) “Wann immer ein Zug auf der Brücke ist, stehen die Signale auf rot”.

Formal: P_1 ist die Menge aller Zustands-Aktions-Folgen $s_0 \xrightarrow{A_0} s_1 \ldots$, so dass für alle $i \in \mathbb{N}$ gilt: Ist $s_i(\mathit{trainW}) = \mathsf{onbridge}$ oder $s_i(\mathit{trainE}) = \mathsf{onbridge}$, so gilt $s_i(\mathit{signalW}) = s_i(\mathit{signalE}) = \mathsf{rot}$.

b) “Der Zug *trainW* bleibt so lange vor einem roten Signal stehen, bis dieses auf grün schaltet.”

Formal: P_2 ist die Menge aller Zustands-Aktions-Folgen $s_0 \xrightarrow{A_0} s_1 \ldots$, so dass für alle $i \in \mathbb{N}$ gilt: Ist $s_i(\mathit{trainW}) = \mathsf{atsignal}$ und $s_i(\mathit{signalW}) = \mathsf{rot}$, so gibt es ein $j \geq i$ mit $s_j(\mathit{signalW}) = \mathsf{grün}$, und für alle k mit $i \leq k < j$ gilt $s_k(\mathit{trainW}) = \mathsf{atsignal}$.

c) “Der Zug *trainW* fährt immer wieder auf die Brücke.”

Formal: P_3 ist die Menge aller Zustands-Aktions-Folgen $s_0 \xrightarrow{A_0} s_1 \ldots$, so dass für alle $i \in \mathbb{N}$ ein $j \geq i$ existiert mit $s_j(\mathit{trainW}) = \mathsf{onbridge}$.

d) “Stehen beide Züge am Signal, so darf *trainE* höchstens einmal auf die Brücke, bevor *trainW* auf die Brücke fährt.”

Formal: P_4 ist die Menge aller Zustands-Aktions-Folgen $s_0 \xrightarrow{A_0} s_1 \ldots$, so dass für alle $i < j < k < l \in \mathbb{N}$ gilt: Ist $s_i(\mathit{trainW}) = s_i(\mathit{trainE}) = \mathsf{atsignal}$ und gelten $s_j(\mathit{trainE}) = \mathsf{onbridge}$, $s_k(\mathit{trainE}) \neq \mathsf{onbridge}$ und $s_l(\mathit{trainE}) = \mathsf{onbridge}$, so gibt es ein m mit $i < m < l$ und $s_m(\mathit{trainW}) = \mathsf{onbridge}$.

Aufgabe 27

Beschreiben Sie das Spiel *Türme von Hanoi* (vgl. Aufgabe 22) durch eine TLA-Spezifikation.

Aufgabe 28 (Hausaufgabe)

TLA-Formeln lassen sich, für eine exakte Definition ihrer Semantik, in eine prädikatenlogische Formel transformieren. Wir lassen im folgenden den Index ξ weg, F und G seien temporallogische Formeln. Beispiele:

- $[\![F \wedge G]\!]_\sigma \Leftrightarrow [\![F]\!]_\sigma \wedge [\![G]\!]_\sigma$
- $[\![\Box F]\!]_\sigma \Leftrightarrow \forall n \in \mathbb{N} \, . \, [\![F]\!]_{\sigma[n..]}$

Transformieren Sie die folgenden temporallogischen Ausdrücke genauso in Ausdrücke der Prädikatenlogik. Beschreiben Sie außerdem umgangssprachlich die Bedeutung jedes Ausdrucks. Beachten Sie, daß Sie die Ausdrücke für eine Ableitung (wie in den obenstehenden Beispielen) in $[\![\text{Klammern}]\!]_\sigma$ setzen müssen.

Es sei $\sigma = s_0 s_1 \ldots$ und $\sigma[n..]$ stehe für $s_n s_{n+1} \ldots$ Sie können die Abkürzung $\exists_\infty x$ für „es gibt unendlich viele x“ verwenden.

a) $\Diamond F$ (definiert als $\neg\Box\neg F$)

b) $F \leadsto G$ (definiert als $\Box(F \Rightarrow \Diamond G)$)

c) $\Box(F \Rightarrow \Box G)$

d) $\Diamond\langle A\rangle_{v,w}$ (definiert als $\neg\Box[\neg A]_{v,w}$)

e) $\Box\Diamond F$

Aufgabe 29 (Hausaufgabe)

x	2	0	0	9	3	5	1	6	4	$\cdots$	(immer $= 0$)
y	1	1	2	3	4	5	6	7	8	$\cdots$	(etc.)

Welche der folgenden Formeln gelten in diesem Ablauf? Begründen Sie jeweils kurz anschaulich.

a) $\Diamond\Box[\mathbf{false}]_y$

b) $\Box[y' = y + 1]_y$

c) $\Box[y' = y + 1]_{x,y}$

d) $\Diamond\langle x = 0 \wedge x' = 0\rangle_{x,y}$

e) $y \neq 5$

f) $y' = y \wedge x' = x - 2$

Abgabe der Hausaufgabe: bis nächste Woche, vor Beginn der Übung – deren genauer Termin in der Übungsstunde am Freitag (bzw. danach auf der GSE-Web-Site) bekanntgegeben wird.