Übung 8 – Transitionssysteme

Formale Techniken in der Software-Entwicklung

Christian Kroiß

Aufgabe 5-1

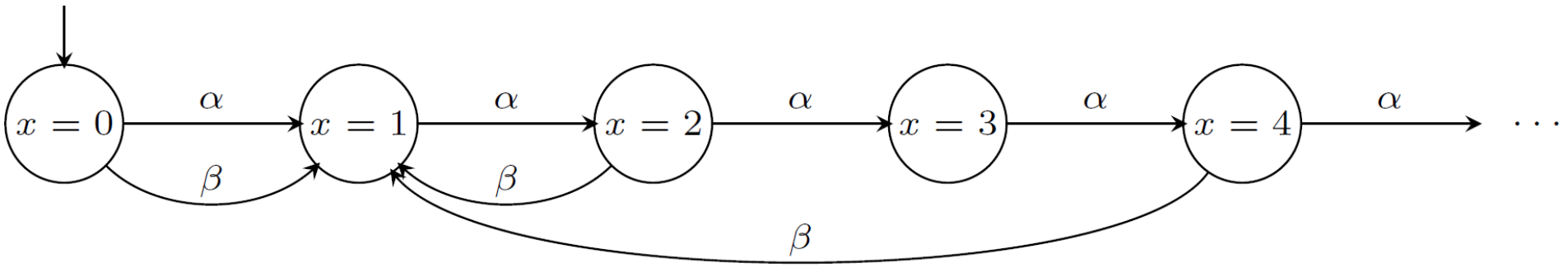
Sei T ein Transitionssystem, dass sich aus dem im Folgenden informell beschriebenen Verhalten zweier Prozesse P_1, P_2 und einer Variable $x \in \mathbb{N}$.

- P_1 kann mit der Aktion α den Wert von x um 1 erhöhen.
- P_2 kann, wenn x einen geraden Wert hat, mit der Aktion α den Wert von x auf 1 setzen.
- Initial gilt $x = 0$.

Aufgabe 5-1

a) Illustrieren Sie in einer (endlichen) Zeichnung den Aufbau des Transitionssystems.

Lösung:



Aufgabe 5-1

b) Geben Sie einen Ablauf an, der stark fair bzgl. der Aktionen α und β ist.

Lösung:

Aktion	-	α	α	β	α	β	α	β	…
x	0	1	2	1	2	1	2	1	…

Aufgabe 5-1

b) Geben Sie einen Ablauf an, der schwach fair, aber nicht stark fair bzgl. der Aktionen α und β ist.

Lösung:

Aktion	-	α	α	α	α	α	α	α	…
x	0	1	2	3	4	5	6	7	…

Schwach fair, da α unendlich oft ausgeführt wird, und β immer wieder nicht ausführbar ist.

Nicht stark fair, da β unendlich oft ausführbar ist, aber nie ausgeführt wird.

- Zeigen Sie: Jeder Ablauf von T ist schwach fair bzgl. der Aktionen α und β.

Lösung:

Betrachte Zustände von T: Alle möglichen Werte von x, also

$Z = \{z_i \mid i \in \mathbb{N}, z_i(x) = i\}$

Schwach fair bezüglich α:

Sei $\sigma = z_1 \xrightarrow{A_1} z_2 \xrightarrow{A_2} \ldots$ Ablauf von T.

- Annahme: σ nicht schwach fair bzgl. α,
  - dann: da α immer ausführbar $\Rightarrow$ α wird nur endlich oft ausgeführt.
- $Sei\ n \in \mathbb{N}, so\ dass\ \forall i \geq n. A_i \neq \alpha.$

  $\Rightarrow \forall i \geq n. A_i = \beta$

  $\Rightarrow z_{n+1}(x) = 1$

  $\Rightarrow \beta$ nicht ausführbar in $z_{n+1} \Rightarrow A_{n+1} = \alpha$

  $\Rightarrow$ WIDERSPRUCH

Schwach fair bzgl. β:

Sei $\sigma = z_1 \xrightarrow{A_1} z_2 \xrightarrow{A_2} \ldots$ Ablauf von T.

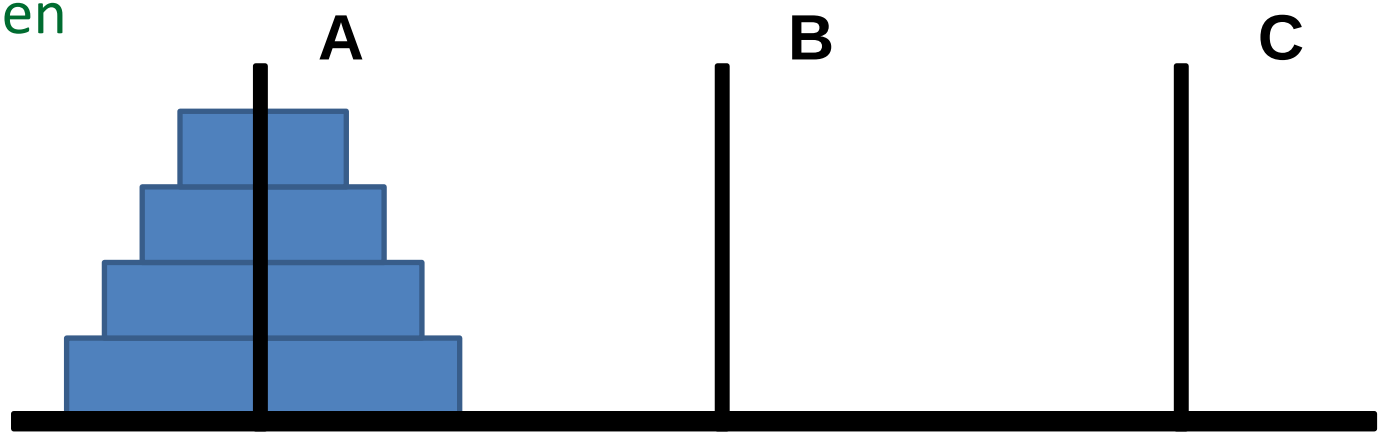
- Annahme: σ nicht schwach fair bzgl. β,
  - dann:

$$\exists n \in \mathbb{N}. \forall i \geq n. enabled(z_i, \beta) \wedge A_i \neq \beta$$
$$\Rightarrow \forall i \geq n. A_i = \alpha$$

- $(1) enabled(z_{n+1}, \beta) \Rightarrow \mathrm{even}(\mathrm{z_{n+1}(x)})$
  $(2) enabled(z_n, \beta) \Rightarrow even(z_n(x))$
  $(3) \mathrm{A_n} = \alpha \Rightarrow z_{n+1}(x) = z_n(x) + 1$
  $\overset{mit\ (2)}{\Longrightarrow} odd(z_{n+1}(x)) \Rightarrow WIDERSPRUCH!$

Die Türme von Hanoi

- Ziel: Turm mit n Scheiben von A nach C
- In jedem Zug:
  - Oberste Scheibe von Turm X → oben auf Turm Y
  - Nur Plätze A, B und C dürfen benutzt werden
  - Es darf keine größere Scheibe auf eine kleinere gelegt werden



Aufgabe 5-2

Aufgabe: Beschreiben Sie die erlaubten Zugfolgen durch ein Transitionssystem.

Lösung:

- Scheiben mit 1 bis n absteigend nach ihrer Größe nummeriert
- Zustandsraum: Menge der Funktionen, die jeder Scheibe ihren aktuellen Turm zuordnen:

$$S = \{s: \{1, \dots, n\} \to \{A, B, C\}\}$$

- Im Zustand s enthält der Turm $x \in \{A, B, C\}$ also gerade die aufsteigend Sortierte Folge der Scheiben $(i_1, i_2, \dots, i_m)$ mit $s(i_j) = x$ für $1 \leq j \leq m$

Aufgabe 5-2

- Anfangszustand: alle Scheiben auf A

$$I = \{s_0\} \text{ mit } s_0(i) = A \text{ für alle } i \in \{1, \dots, n\}$$

- Aktionsmenge: Züge von Turm zu Turm

$$A = \begin{Bmatrix} move_{A\to B}, move_{A\to C}, move_{B\to A}, move_{B\to C}, \\ move_{C\to A}, move_{C\to B} \end{Bmatrix}$$

- Transitionsrelation δ:

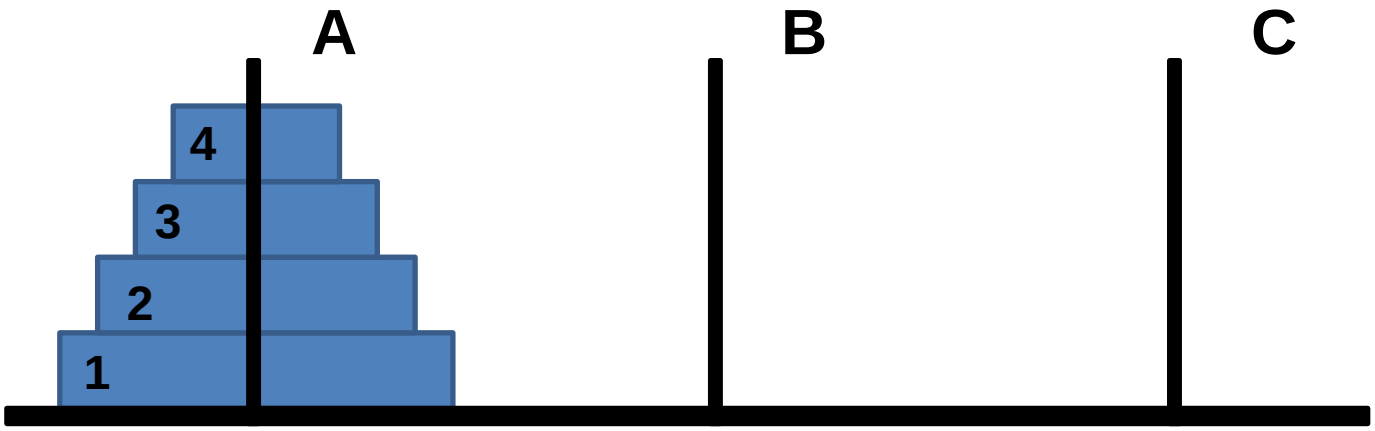
$$\left(s, move_{x\to y}, s'\right) \in \delta \text{ gdw. } \exists i \exists x \exists y.\, i \in \{1, \dots, n\}.\, x, y \in \{A, B, C\}, \text{ so dass}$$

  - $s(i) = x \wedge s(j) \notin \{x, y\}$ für alle $i < j \leq n$.
  - $s'(i) = y \wedge s'(j) = s(j)$ für alle $j \in \{1, \dots n\} \setminus \{i\}$

Beispiel

Sei $\delta^s \subseteq \delta$ definiert als $\delta^s := \{(t, a, s') \in \delta | t = s\}$

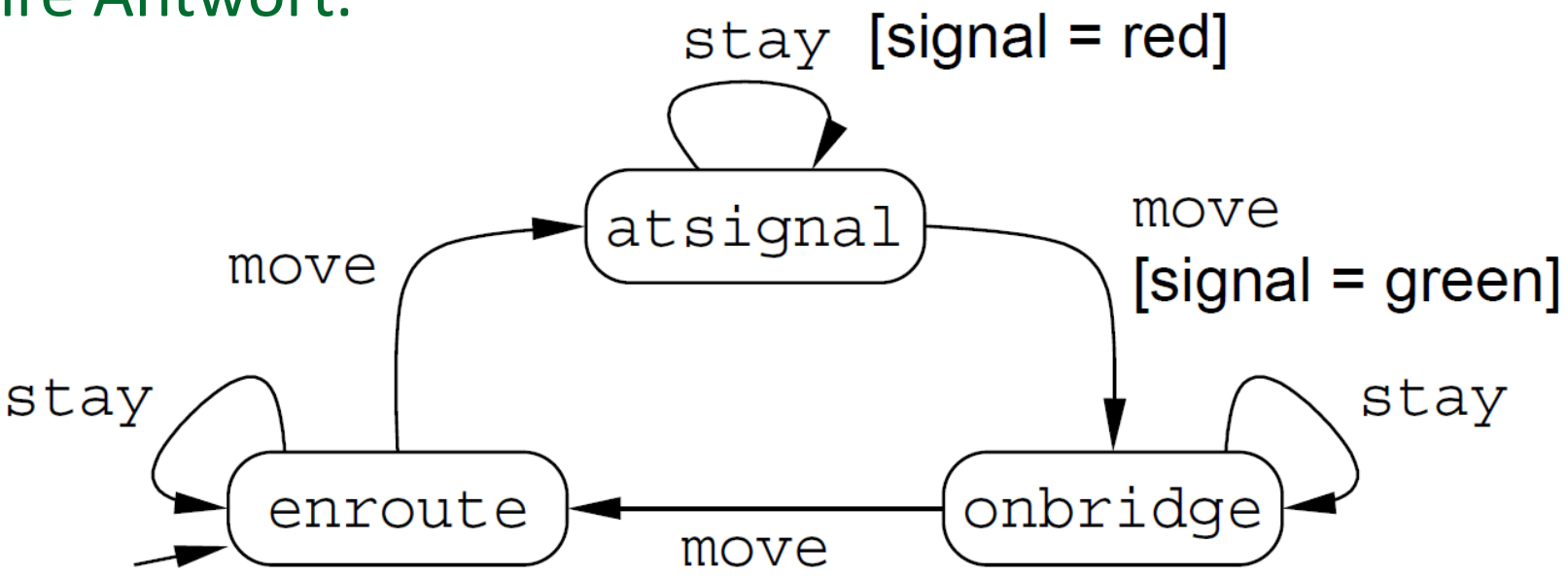
$Zustand\ s_1$



$\delta^{s_1} = \{(s_1, move_{A\to B}, s_2'), (s_1, move_{A\to C}, s_2'')\}$ mit $s_2'(4) = B \wedge s_2''(4) = C$
$\wedge\ s_2'(i) = s_2''(i) = s(i)\ \forall i \neq 4$

Aufgabe 5-3

Welche der folgenden Eigenschaften (im Kontext des Eisenbahnbeispiels aus der Vorlesung) sind Sicherheits- bzw. Lebendigkeitseigenschaften? Begründen Sie kurz Ihre Antwort.



Aufgabe 5-3

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

Formal:

P_1 ist die Menge aller Zustands−Folgen $s_0 \xrightarrow{A_0} s_1 \rightarrow \cdots$,
so dass für alle $i \in \mathbb{N}$ gilt:

$$\mathrm{s_i(trainW)} = \mathrm{onbridge} \vee s_i(trainE) = onbridge \Rightarrow s_i(signalW) = s_i(signalE) = red.$$

Aufgabe 5-3

P_1 ist die Menge aller Zustands−Folgen $s_0 \xrightarrow{A_0} s_1 \rightarrow \cdots$, so dass für alle $i \in \mathbb{N}$ gilt:

$$s_i(\text{trainW}) = \text{onbridge} \vee s_i(trainE) = onbridge \Rightarrow s_i(signalW) = s_i(signalE) = red.$$

Lösung: P_1 ist **Sicherheitseigenschaft:**

- $Sei\ \sigma = s_1 \xrightarrow{A_1} s_2 \xrightarrow{A_2}$ …ein Ablauf mit $\sigma[\ldots n] \in P_1$ für alle $n \in \mathbb{N}$.
- Angenommen $\sigma \notin P_1$, dann: $\exists i \in \mathbb{N}\ mit$
  $(s_i(\text{trainW}) = \text{onbridge} \vee s_i(trainE) = onbridge) \wedge (s_i(signalW) \neq red \vee s_i(signalE) \neq red)$
- Dann aber gilt: $\sigma[..i]$ lässt sich nicht zu Ablauf in P_1 erweitern. **WIDERSPUCH!**

Aufgabe 5-3

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 $s_0 \overset{A_1}{\rightarrow} s_1, \ldots$, so dass für alle $i \in \mathbb{N}$ gilt:
Ist $s_i(trainW) =$ atsignal und $s_i(signalW) =$ red, so gibt es ein $j \geq i$ mit $s_j(signalW) =$ green, und für alle k mit $i \leq k < j$ gilt $s_k(trainW) =$ atsignal.

Aufgabe 5-3

P_2 ist die Menge aller Zustands-Aktions-Folgen $s_0 \stackrel{A_1}{\rightarrow} s_1, \ldots$, so dass für alle $i \in \mathbb{N}$ gilt:
Ist $s_i(trainW) = \mathsf{atsignal}$ und $s_i(signalW) = \mathsf{red}$, so gibt es ein $j \geq i$ mit $s_j(signalW) = \mathsf{green}$, und für alle k mit $i \leq k < j$ gilt $s_k(trainW) = \mathsf{atsignal}$.

Lösung: P_2 ist weder reine Sicherheits- noch reine Lebendigkeitseigenschaft.

Es gilt $P_2 = S_2 \cap L_2$ mit

1. $\sigma \in S_2 = C(P_2)$ genau dann, wenn gilt: für alle $i \in \mathbb{N}$ mit $s_i(trainW) = \mathsf{atsignal}$ und $s_i(signalW) = \mathsf{rot}$ gibt es
   - entweder ein $j \geq i$ wie angegeben
   - **oder** für alle $k \geq i$ gilt $s_k(trainW) = \mathsf{atsignal}$.

Aufgabe 5-3

S_2 ist Sicherheitseigenschaft, denn:
Sei $\rho \in \Sigma^\omega$ mit $\forall n \in \mathbb{N}.\ \rho[..n] \in S_2$. Zu zeigen ist: $\rho \in S_2$.

Sei also $\rho \notin S_2$. dann:
$\exists i \in \mathbb{N}.\ s_i(trainW) = \mathsf{atsignal}$ und $s_i(signalW) = \mathsf{red}$,
so dass $\forall j \geq i.\ s_j(signalW) = \mathsf{green}$ gilt:
$\exists i \leq k < j.\ s_k(trainW) \neq \mathsf{atsignal}$.

Sei $j \geq i$ minimal s.d. $s_j(signalW) = \mathsf{green}$. Dann gilt für auch dieses j:
$\exists i \leq k < j.\ s_k(trainW) \neq \mathsf{atsignal}$, und für dieses k gilt dass $s_k(signalW) = \mathsf{red}$.
Dann ist aber $\rho[..k] \notin S_2$!
Zweiter Fall $\forall j \geq i.\ s_j(signalW) = \mathsf{red}$ geht analog.

Aufgabe 5-3

1. $\sigma \in L_2$ genau dann, wenn gilt:

   für alle $i \in \mathbb{N}$ mit $s_i(trainW) =$ atsignal und $s_i(signalW) =$ red existiert ein $j \geq i$ mit $s_j(signalW) =$ green.

   L_2 ist Lebendigkeitseigenschaft, denn:
   Sei $\rho \in \Sigma^\omega, \rho = s_1 \overset{A_1}{\to} s_2 \overset{A_2}{\to} \ldots$, sei $n \in \mathbb{N}$. $\rho[..n]$ lässt sich ergänzen durch $\rho' = s_n \overset{A_n}{\to} s_{n+1} \overset{A_{n+1}}{\to} \ldots \in \Sigma^\omega$ mit $s_{n+1}(signalW) =$ green.

Laut Definition gilt $\rho \circ \rho' \in L_2$

Aufgabe 5-3

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

P_3 ist die Menge aller Zustands-Aktions-Folgen $s_0 \xrightarrow{A_1} s_1 \xrightarrow{A_2} \ldots$
so dass für alle $i \in \mathbb{N}$ ein $j \geq i$ existiert mit $s_j(trainW) = \mathsf{onbridge}$.

P_3 ist Lebendigkeitseigenschaft:

Sei s Zustand mit $s(trainW) = \mathsf{onbridge}$ und σ beliebig.

Dann ist $\sigma[..n] \circ s_n \xrightarrow{A} s \xrightarrow{A} s \ldots \in P_3$ (für beliebige Aktion A).

Aufgabe 5-3

d) “Stehen beide Züge am Signal, so darf trainE höchstens einmal auf die Bücke, 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 $s_i(trainW) = s_i(trainE) =$ atsignal und gelten
$s_j(trainE) =$ onbridge, $s_k(trainE) \neq$ onbridge und $s_l(trainE) =$ onbridge,
so gibt es ein m mit $i < m < l$ und $s_m(trainW) =$ onbridge

Aufgabe 5-3

Lösung:

P_4 ist eine Sicherheitseigenschaft:

Gilt $\sigma \notin P_4$, so existieren $i < j < k < l \in \mathbb{N}$, so dass
alle folgenden Bedingungen gelten:

$s_i(trainW) = s_i(trainE) = \mathsf{atsignal}$,
$s_j(trainE) = \mathsf{onbridge}$, $s_k(trainE) \neq \mathsf{onbridge}$
und $s_l(trainE) = \mathsf{onbridge}$, aber für alle m mit $i < m < l$ gilt
$s_m(trainW) \neq \mathsf{onbridge}$.

In diesem Fall kann $\sigma[..l]$ nicht mehr zu einem Ablauf $\sigma[..l] \circ \tau \in P_4$ verlängert werden, d.h. es gilt nicht $\sigma[..n] \in P_4$ für alle $n \in \mathbb{N}$.
Intuitiv ist das "schlechte Ereignis" das zweite Befahren der Brücke durch $trainE$, ohne dass $trainW$ inzwischen auf die Brücke gefahren wäre.