

# Übung 6 – Hausaufgaben

Formale Techniken in der Software-Entwicklung

Christian Kroiß



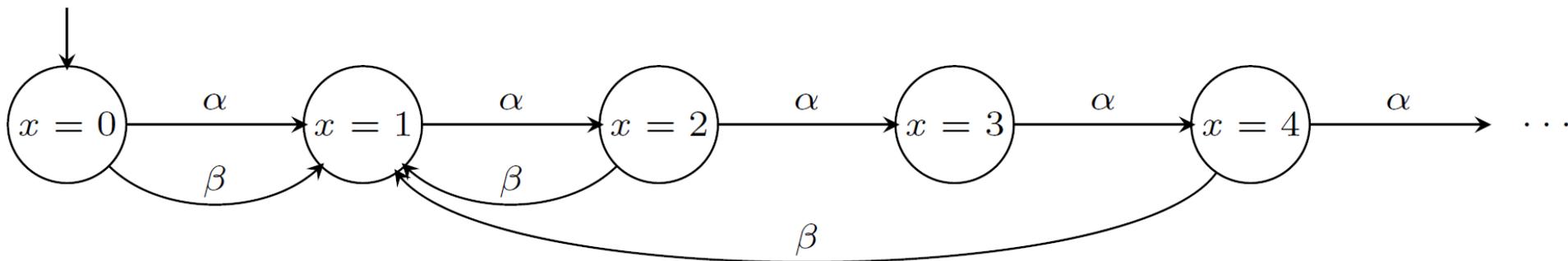
Sei  $T$  ein Transitionssystem, das sich aus dem im Folgenden informell beschriebenen Verhalten zweier Prozesse  $P_1, P_2$  und einer Variable  $x \in \mathbb{N}$ .

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



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

**Lösung:**





b) Geben Sie einen Ablauf an, der stark fair bzgl. der Aktionen  $\alpha$  und  $\beta$  ist.

**Lösung:**

<b>Aktion</b>	-	$\alpha$	$\alpha$	$\beta$	$\alpha$	$\beta$	$\alpha$	$\beta$	...
<b>x</b>	0	1	2	1	2	1	2	1	...



b) Geben Sie einen Ablauf an, der schwach fair, aber nicht stark fair bzgl. der Aktionen  $\alpha$  und  $\beta$  ist.

**Lösung:**

<b>Aktion</b>	-	$\alpha$	...						
<b>x</b>	0	1	2	3	4	5	6	7	...

**Schwach fair**, da  $\alpha$  unendlich oft ausgeführt wird, und  $\beta$  immer wieder nicht ausführbar ist.

**Nicht stark fair**, da  $\beta$  unendlich oft ausführbar ist, aber nie ausgeführt wird.



- Zeigen Sie: Jeder Ablauf von  $T$  ist schwach fair bzgl. der Aktionen  $\alpha$  und  $\beta$ .

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 $\alpha$ :

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

- Annahme:  $\sigma$  nicht schwach fair bzgl.  $\alpha$ ,
  - dann: da  $\alpha$  immer ausführbar  $\Rightarrow \alpha$  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

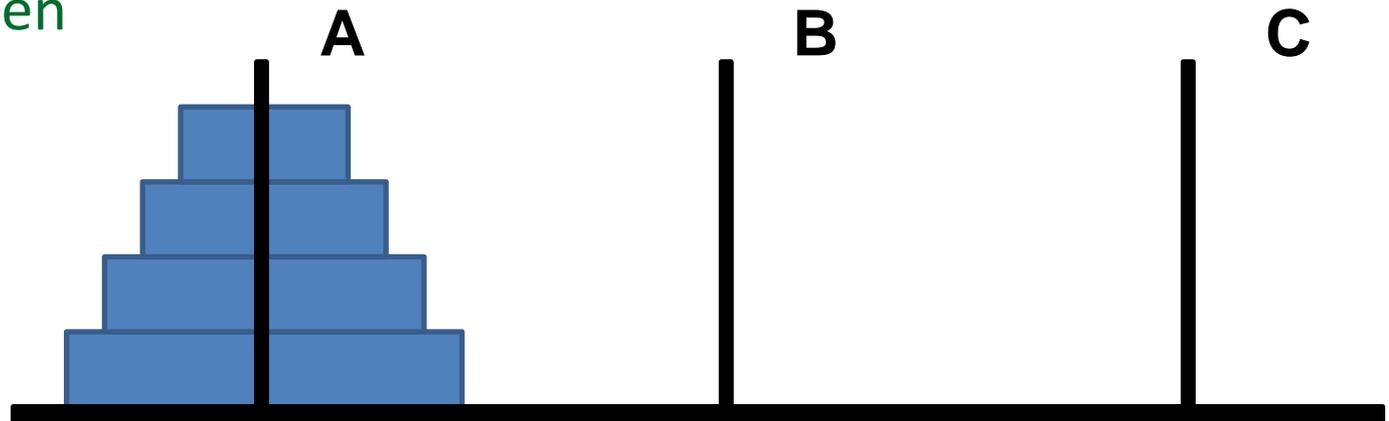
## Schwach fair bzgl. $\beta$ :

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

- Annahme:  $\sigma$  nicht schwach fair bzgl.  $\beta$ ,
  - dann:
    - $\exists n \in \mathbb{N}. \forall i \geq n. \text{enabled}(z_i, \beta) \wedge A_i \neq \beta$
    - $\Rightarrow \forall i \geq n. A_i = \alpha$
  - (1)  $\text{enabled}(z_{n+1}, \beta) \Rightarrow \text{even}(z_{n+1}(x))$
  - (2)  $\text{enabled}(z_n, \beta) \Rightarrow \text{even}(z_n(x))$
  - (3)  $A_n = \alpha \Rightarrow z_{n+1}(x) = z_n(x) + 1$
  - mit (2)  
 $\implies \text{odd}(z_{n+1}(x)) \Rightarrow \text{WIDERSPRUCH!}$

## Die Türme von Hanoi

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





**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:

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

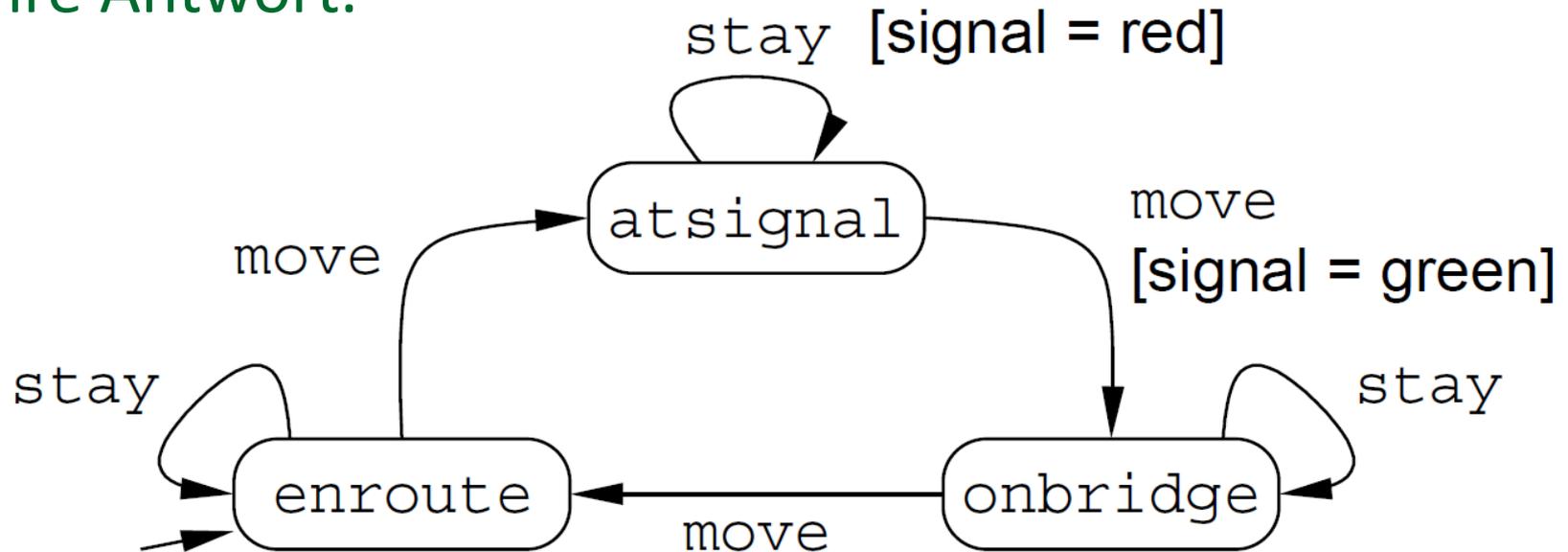
- Im Zustand  $s$  enthält der Turm  $x \in \{A, B, C\}$  also gerade die aufsteigend Sortierte Folge der Scheiben  $(i_1, i_2, \dots, i_m)$  mit  $s(i_j) = x$  für  $1 \leq j \leq m$



- Anfangszustand: alle Scheiben auf A  
 $I = \{s_0\}$  mit  $s_0(i) = A$  für alle  $i \in \{1, \dots, n\}$
- Aktionsmenge: hier ohne Beachtung der Richtung  
 $A = \{move\}$
- Transitionsrelation  $\delta$ :  
 $(s, move, s')$  gdw.  $\exists i \exists x \exists y. i \in \{1, \dots, n\}. x, y \in \{A, B, C\}$ , so dass
  - $s(i) = x \wedge s(j) \notin \{x, y\}$  für alle  $i < j \leq n$ .
  - $t(i) = y \wedge t(j) = s(j)$  für alle  $j \in \{1, \dots, n\} \setminus \{i\}$



Welche der folgenden Eigenschaften (im Kontext des Eisenbahnbeispiels aus der Vorlesung) sind Sicherheits- bzw. Lebendigkeitseigenschaften? Begründen Sie 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-Folgen  $s_0 \xrightarrow{A_0} s_1 \rightarrow \dots$ ,  
so dass für alle  $i \in \mathbb{N}$  gilt:

$$s_i(\text{train}W) = \text{onbridge} \vee s_i(\text{train}E) = \text{onbridge} \\ \Rightarrow s_i(\text{signal}W) = s_i(\text{signal}E) = \text{red}.$$



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

$$s_i(\text{train}W) = \text{onbridge} \vee s_i(\text{train}E) = \text{onbridge} \\ \Rightarrow s_i(\text{signal}W) = s_i(\text{signal}E) = \text{red}.$$

**Lösung:**  $P_1$  ist Sicherheitseigenschaft:

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



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  $s_0 \xrightarrow{A_1} s_1, \dots$ , so dass für alle  $i \in \mathbb{N}$  gilt:

Ist  $s_i(\text{train}W) = \text{atsignal}$  und  $s_i(\text{signal}W) = \text{red}$ , so gibt es ein  $j \geq i$  mit  $s_j(\text{signal}W) = \text{green}$ , und für alle  $k$  mit  $i \leq k < j$  gilt  $s_k(\text{train}W) = \text{atsignal}$ .



$P_2$  ist die Menge aller Zustands-Aktions-Folgen  $s_0 \xrightarrow{A_1} s_1, \dots$ , so dass für alle  $i \in \mathbb{N}$  gilt:

Ist  $s_i(\text{train}W) = \text{atsignal}$  und  $s_i(\text{signal}W) = \text{red}$ , so gibt es ein  $j \geq i$  mit  $s_j(\text{signal}W) = \text{green}$ , und für alle  $k$  mit  $i \leq k < j$  gilt  $s_k(\text{train}W) = \text{atsignal}$ .

**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  $s_i(\text{train}W) = \text{atsignal}$  und  $s_i(\text{signal}W) = \text{rot}$  gibt es
  - entweder ein  $j \geq i$  wie angegeben
  - **oder** für alle  $k \geq i$  gilt  $s_k(\text{train}W) = \text{atsignal}$ .



$S_2$  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:

$\exists i \in \mathbb{N}. s_i(\text{train}W) = \text{atsignal}$  und  $s_i(\text{signal}W) = \text{red}$ ,

so dass  $\forall j \geq i. s_j(\text{signal}W) = \text{green}$  gilt:

$\exists i \leq k < j. s_k(\text{train}W) \neq \text{atsignal}$ .

Sei  $j \geq i$  minimal s.d.  $s_j(\text{signal}W) = \text{green}$ . Dann gilt für auch dieses  $j$ :

$\exists i \leq k < j. s_k(\text{train}W) \neq \text{atsignal}$ , und für dieses  $k$  gilt dass  $s_k(\text{signal}W) = \text{red}$ .

Dann ist aber  $\rho[..k] \notin S_2$ !

Zweiter Fall  $\forall j \geq i. s_j(\text{signal}W) = \text{red}$  geht analog.



②  $\sigma \in L_2$  genau dann, wenn gilt:

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

$L_2$  ist Lebendigkeitseigenschaft, denn:

Sei  $\rho \in \Sigma^\omega$ ,  $\rho = s_1 \xrightarrow{A_1} s_2 \xrightarrow{A_2} \dots$ , sei  $n \in \mathbb{N}$ .  $\rho[..n]$  lässt sich ergänzen durch  $\rho' = s_n \xrightarrow{A_n} s_{n+1} \xrightarrow{A_{n+1}} \dots \in \Sigma^\omega$  mit  $s_{n+1}(\text{signal}W) = \text{green}$ .  
Laut Definition gilt  $\rho \circ \rho' \in L_2$  und



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

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

$P_3$  ist Lebendigkeitseigenschaft:

Sei  $s$  Zustand mit  $s(\text{train}W) = \text{onbridge}$  und  $\sigma$  beliebig.

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



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  $s_0 \xrightarrow{A_0} s_1 \dots$ , so dass für alle  $i < j < k < l \in \mathbb{N}$  gilt:

Ist  $s_i(\text{train}W) = s_i(\text{train}E) = \text{atsignal}$  und gelten  $s_j(\text{train}E) = \text{onbridge}$ ,  $s_k(\text{train}E) \neq \text{onbridge}$  und  $s_l(\text{train}E) = \text{onbridge}$ , so gibt es ein  $m$  mit  $i < m < l$  und  $s_m(\text{train}W) = \text{onbridge}$

## 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:

$s_i(\text{train}W) = s_i(\text{train}E) = \text{atsignal}$ ,

$s_j(\text{train}E) = \text{onbridge}$ ,  $s_k(\text{train}E) \neq \text{onbridge}$

und  $s_l(\text{train}E) = \text{onbridge}$ , aber für alle  $m$  mit  $i < m < l$  gilt

$s_m(\text{train}W) \neq \text{onbridge}$ .

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  $\text{train}E$ , ohne dass  $\text{train}W$  inzwischen auf die Brücke gefahren wäre.