

# KOMMUNIKATIONSFEHLER, VERKLEMMUNG UND DIVERGENZ BEI INTERFACE-AUTOMATEN

KOLLOQUIUM ZUR BACHELORARBEIT

Ayleen Schinko

20. März 2016

# INHALT

- 1 MOTIVATION
- 2 DEFINITIONEN
- 3 VERFEINERUNG FÜR ERROR-, RUHE- UND DIVERGENZ-FREIHEIT
- 4 WEITERE VERFEINERUNGEN
- 5 HIDING

# MOTIVATION

- Modellierung von Systemen und deren Kommunikationsverhalten (Parallelkomposition)
- simulation parallel arbeitender Softwarekomponenten
- Kommunikationsfehler in Interface-Automaten nicht zulässig, deshalb Error-IO-Transitionssysteme als Abwandlung davon betrachtet
  - Kommunikationsfehler (bzw. Error) zwischen Komponenten
  - Verklemmung (bzw. Ruhe) innerhalb einer Softwarekomponenten (keine Outputs mehr möglich)
  - Divergenz einer Softwarekomponenten (unendliche viele interne Aktionen)

# DEFINITIONEN

## DEFINITION (ERROR-IO-TRANSITIONSSYSTEME)

Ein **Error-IO-Transitionssysteme (EIO)** ist ein Tupel

$S = (Q, I, O, \delta, q_0, E)$  mit den Komponenten:

- $Q$  - die Menge der Zustände,
- $I, O$  - die disjunkte Menge der (sichtbaren) Input- und Output-Aktionen,
- $\delta \subseteq Q \times (I \cup O \cup \{\tau\}) \times Q$  - die Transitionsrelation,
- $q_0 \in Q$  - der Startzustand,
- $E \subseteq Q$  - die Menge der Error-Zustände.

Aktionsmenge von  $S$ :  $\Sigma = I \cup O$

Signatur:  $\text{Sig}(S) = (I, O)$

## DEFINITION (PARALLELKOMPOSITION)

Zwei EIOs  $S_1, S_2$  sind **komponierbar**, falls  $O_1 \cap O_2 = \emptyset$  gilt. Die Parallelkomposition der EIOs  $S_1$  und  $S_2$  ist

$S_{12} := S_1 \parallel S_2 = (Q, I, O, \delta, q_0, E)$  mit den Komponenten:

- $Q = Q_1 \times Q_2$ ,
- $I = (I_1 \setminus O_2) \cup (I_2 \setminus O_1)$ ,
- $O = O_1 \cup O_2$ ,
- $q_0 = (q_{01}, q_{02})$ ,
- $\delta = \{((q_1, q_2), \alpha, (p_1, q_2)) \mid (q_1, \alpha, p_1) \in \delta_1, \alpha \in (\Sigma_1 \cup \{\tau\}) \setminus \text{Synch}(S_1, S_2)\} \cup \{((q_1, q_2), \alpha, (q_1, p_2)) \mid (q_2, \alpha, p_2) \in \delta_2, \alpha \in (\Sigma_2 \cup \{\tau\}) \setminus \text{Synch}(S_1, S_2)\} \cup \{((q_1, q_2), \alpha, (p_1, p_2)) \mid (q_1, \alpha, p_1) \in \delta_1, (q_2, \alpha, p_2) \in \delta_2, \alpha \in \text{Synch}(S_1, S_2)\} \}$ ,
- $E = \dots$

## DEFINITION (PARALLELKOMPOSITION)

Zwei EIOs  $S_1, S_2$  sind **komponierbar**, falls  $O_1 \cap O_2 = \emptyset$  gilt. Die Parallelkomposition der EIOs  $S_1$  und  $S_2$  ist

$S_{12} := S_1 \parallel S_2 = (Q, I, O, \delta, q_0, E)$  mit den Komponenten:

- $Q = Q_1 \times Q_2$ ,
- $I = (I_1 \setminus O_2) \cup (I_2 \setminus O_1)$ ,
- $O = O_1 \cup O_2$ ,
- $q_0 = (q_{01}, q_{02})$ ,
- $\delta = \dots$ ,
- $E = (Q_1 \times E_2) \cup (E_1 \times Q_2)$

$$\cup \left\{ (q_1, q_2) \mid \exists a \in O_1 \cap I_2 : q_1 \xrightarrow{a} \wedge q_2 \not\xrightarrow{a} \right\}$$

$$\cup \left\{ (q_1, q_2) \mid \exists a \in I_1 \cap O_2 : q_1 \not\xrightarrow{a} \wedge q_2 \xrightarrow{a} \right\}.$$

*Traces* sind die möglichen Wege eines EIOs, mit ihrer Transitionsbeschriftung.

*Traces* sind die möglichen Wege eines EIOs, mit ihrer Transitionsbeschriftung.

### DEFINITION (PRUNING- UND FORTSETZUNGS-FUNKTION)

Für ein EIO  $S$  wird definiert:

- $\text{prune} : \Sigma^* \rightarrow \Sigma^*, w \mapsto u$ , mit  $w = uv, u = \varepsilon \wedge u \in \Sigma^* \cdot I$  und  $v \in O^*$ ,
- $\text{cont} : \Sigma^* \rightarrow \mathfrak{P}(\Sigma^*), w \mapsto \{wu \mid u \in \Sigma^*\}$ ,
- $\text{cont} : \mathfrak{P}(\Sigma^*) \rightarrow \mathfrak{P}(\Sigma^*), L \mapsto \bigcup \{\text{cont}(w) \mid w \in L\}$ .



## DEFINITION (RUHE)

Ein **Ruhe-Zustand** ist ein Zustand in einem EIO, der keine Outputs und kein  $\tau$  zulässt.

Die Menge der Ruhe-Zustände in einem EIO ist wie folgt formal definiert:

$$Qui := \left\{ q \in Q \mid \forall \alpha \in (O \cap \{\tau\}) : q \not\stackrel{\alpha}{\rightarrow} \right\}.$$

### DEFINITION (RUHE)

Ein **Ruhe-Zustand** ist ein Zustand in einem EIO, der keine Outputs und kein  $\tau$  zulässt.

Die Menge der Ruhe-Zustände in einem EIO ist wie folgt formal definiert:

$$Qui := \left\{ q \in Q \mid \forall \alpha \in (O \cap \{\tau\}) : q \not\stackrel{\alpha}{\rightarrow} \right\}.$$

### DEFINITION (DIVERGENZ)

Ein **Divergenz-Zustand** ist ein Zustand in einem EIO, der eine unendliche Folge von  $\tau$ s ausführen kann.

Die Menge  $Div(S)$  besteht aus all diesen divergenten Zuständen des EIOs  $S$ .

# VERFEINERUNG

## DEFINITION (DIVERGENZ-VERFEINERUNGS-BASISRELATION)

Für EIOs  $S_1$  und  $S_2$  mit der gleichen Signatur wird  $S_1 \sqsubseteq_{Div}^B S_2$  geschrieben, wenn ein Error-, Ruhe- oder Divergenz-Zustand in  $S_1$  nur dann lokal erreichbar ist, wenn er auch in  $S_2$  lokal erreichbar ist. Diese **Basisrelation** stellt eine **Verfeinerung** bezüglich **Error**, **Ruhe** und **Divergenz** dar.

$\sqsubseteq_{Div}^C$  bezeichnet die **vollständige abstrakte Präkongruenz** von  $\sqsubseteq_{Div}^B$  bezüglich  $\cdot\|\cdot$ .

## DEFINITION (TRACES)

Für ein EIO  $S$  wird definiert:

- **strikte Errortraces:**  $StET(S) := \left\{ w \in \Sigma^* \mid q_0 \xRightarrow{w} q \in E \right\},$
- **gekürzte Errortraces:**  $PrET(S) := \bigcup \{ \text{prune}(w) \mid w \in StET(S) \},$
- **Input-kritische Traces:**  
 $MIT(S) := \left\{ wa \in \Sigma^* \mid q_0 \xRightarrow{w} q \wedge a \in I \wedge q \not\xrightarrow{a} \right\},$
- **Errortraces:**  $ET(S) := \text{cont}(PrET(S)) \cup \text{cont}(MIT(S)),$
- **strikte Ruhetraces:**  $StQT(S) := \left\{ w \in \Sigma^* \mid q_0 \xRightarrow{w} q \in Qui \right\},$
- **strikte Divergenztraces:**  $StDT(S) := \left\{ w \in \Sigma^* \mid q_0 \xRightarrow{w} q \in Div \right\},$
- **gekürzte Divergenztraces:**  
 $PrDT(S) := \bigcup \{ \text{prune}(w) \mid w \in StDT(S) \}.$
- **Divergenztraces:**  $DT(S) := \text{cont}(PrDT(S)).$

## DEFINITION (ERROR-, DIVERGENZ- UND RUHE-SEMANTIK)

Sei  $S$  ein EIO.

- Die Menge der **Error-Divergenztraces** von  $S$  ist  $EDT(S) := ET(S) \cup DT(S)$ .
- Die Menge der **error-divergenz-gefluteten Ruhetraces** von  $S$  ist  $QDT(S) := StQT(S) \cup EDT(S)$ .
- Die Menge der **error-divergenz-gefluteten Sprache** von  $S$  ist  $EDL(S) := L(S) \cup EDT(S)$ .

Für zwei EIOs  $S_1, S_2$  mit der gleichen Signatur schreibt man  $S_1 \sqsubseteq_{Div} S_2$ , wenn  $EDT_1 \subseteq EDT_2$ ,  $QDT_1 \subseteq QDT_2$  und  $EDL_1 \subseteq EDL_2$  gilt.

## SATZ (ERROR-, RUHE- UND DIVERGENZ-SEMANTIK FÜR PARALLELKOMPOSITION)

Für zwei komponierbare EIOs  $S_1, S_2$  und ihre Komposition  $S_{12}$  gilt:

- ①  $EDT_{12} = \text{cont}(\text{prune}((EDT_1 \parallel EDL_2) \cup (EDL_1 \parallel EDT_2))),$
- ②  $QDT_{12} = (QDT_1 \parallel QDT_2) \cup EDT_{12},$
- ③  $EDL_{12} = (EDL_1 \parallel EDL_2) \cup EDT_{12}.$

## SATZ (ERROR-, RUHE- UND DIVERGENZ-SEMANTIK FÜR PARALLELKOMPOSITION)

Für zwei komponierbare EIOs  $S_1, S_2$  und ihre Komposition  $S_{12}$  gilt:

- ①  $EDT_{12} = \text{cont}(\text{prune}((EDT_1 \parallel EDL_2) \cup (EDL_1 \parallel EDT_2)))$ ,
- ②  $QDT_{12} = (QDT_1 \parallel QDT_2) \cup EDT_{12}$ ,
- ③  $EDL_{12} = (EDL_1 \parallel EDL_2) \cup EDT_{12}$ .

## PROPOSITION (DIVERGENZ-PRÄKONGRUEZ)

Die Relation  $\sqsubseteq_{Div}$  ist eine Präkongruenz bezüglich  $\cdot \parallel \cdot$ .

**DEFINITION ( $\omega$ -PARTNER)**

*Ein EIO  $S_1$  ist ein  $\omega$ -**Partner** von einem EIO  $S_2$ , wenn  $I_1 = O_2$  und  $O_1 = I_2 \cup \{\omega\}$  mit  $\omega \notin I_2 \cup O_2$  gilt.*



**DEFINITION ( $\omega$ -PARTNER)**

*Ein EIO  $S_1$  ist ein  $\omega$ -PARTNER von einem EIO  $S_2$ , wenn  $I_1 = O_2$  und  $O_1 = I_2 \cup \{\omega\}$  mit  $\omega \notin I_2 \cup O_2$  gilt.*

**LEMMA (VERFEINERUNG MIT DIVERGENZ-ZUSTÄNDEN)**

*Gegeben sind zwei EIOs  $S_1$  und  $S_2$  mit der gleichen Signatur. Wenn  $U \parallel S_1 \sqsubseteq_{Div}^B U \parallel S_2$  für alle  $\omega$ -Partner  $U$  gilt, dann folgt daraus  $S_1 \sqsubseteq_{Div} S_2$ .*

$x?$  bezeichnet den Input  $x$  und  $x!$  den Output  $x$

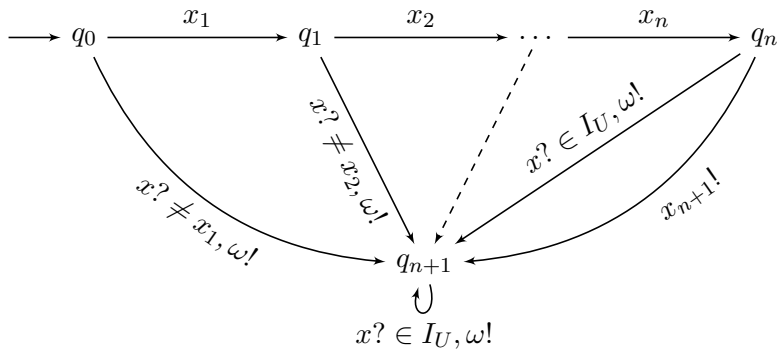


ABBILDUNG :  $x? \neq x_i$  steht für alle  $x \in I_U \setminus \{x_i\}$

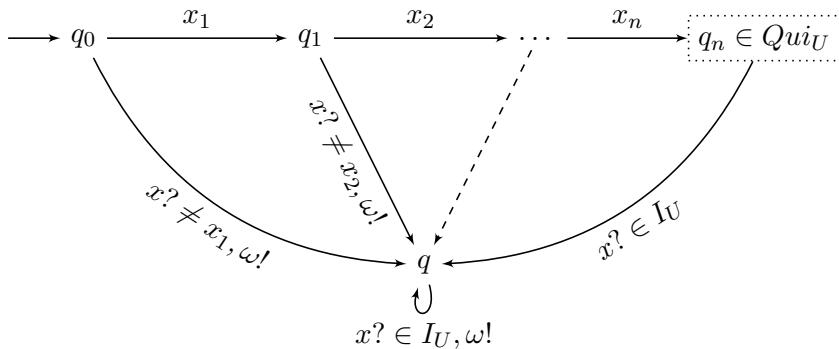


ABBILDUNG :  $x? \neq x_i$  steht für alle  $x \in I_U \setminus \{x_i\}$ ,  $q_n$  ist der einzige Ruhe-Zustand

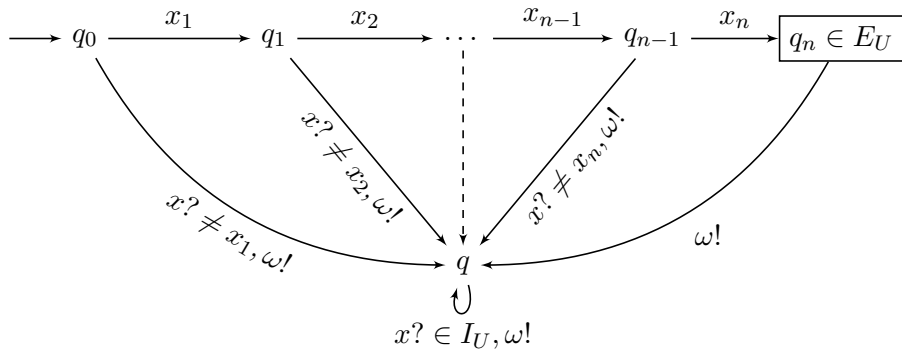


ABBILDUNG :  $x? \neq x_i$  steht für alle  $x \in I_U \setminus \{x_i\}$ ,  $q_n$  ist der einzige Error-Zustand

**SATZ (VOLLSTÄNIGE ABSTRAKTHEIT FÜR DIVERGENZ-SEMANTIK)**

*Seien  $S_1$  und  $S_2$  zwei EIOs mit derselben Signatur. Dann gilt*

$$S_1 \sqsubseteq_{Div}^C S_2 \Leftrightarrow S_1 \sqsubseteq_{Div} S_2.$$

# SATZ (VOLLSTÄNDIGE ABSTRAKTHEIT FÜR DIVERGENZ-SEMANTIK)

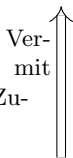
Seien  $S_1$  und  $S_2$  zwei EIOs mit derselben Signatur. Dann gilt

$$S_1 \sqsubseteq_{Div}^C S_2 \Leftrightarrow S_1 \sqsubseteq_{Div} S_2.$$

„ $\Leftarrow$ “ von Satz Vollständige  
Abstraktheit für Divergenz-  
Semantik

$$S_1 \sqsubseteq_{Div} S_2 \xrightarrow{\quad} S_1 \sqsubseteq_{Div}^C S_2$$

Lemma  
feinerung  
Divergenz-Zu-  
ständen



$$\forall \omega\text{-Partner } U: \\ U \parallel S_1 \sqsubseteq_{Div}^B U \parallel S_2$$

$$\xleftarrow{\quad}$$

$U$   $\omega$ -Partner

$\Downarrow$   
 $U$  komponierbar

$$\forall \omega\text{-komponierbaren } U: \\ U \parallel S_1 \sqsubseteq_{Div}^B U \parallel S_2$$

Definition  
von  $\sqsubseteq_{Div}^C$



ABBILDUNG : Folgerungskette

## KOROLLAR

*Es gilt:  $S_1 \sqsubseteq_{Div} S_2 \Leftrightarrow U \parallel S_1 \sqsubseteq_{Div}^B U \parallel S_2$  für alle komponierbaren  $U$ .*

# WEITERE VERFEINERUNGEN

- Verfeinerung für Error-Freiheit
- Verfeinerung für Error- und Ruhe-Freiheit



## HIDING

## DEFINITION (INTERNALISIERUNGSOOPERATOR)

Für ein EIO  $S = (Q, I, O, \delta, q_0, E)$  ist  $S/X$ , mit dem  
**Internalisierungsoperator**  $\cdot/\cdot$ , definiert als  $(Q, I, O', \delta', q_0, E)$  mit:

- $\tau \notin X$ ,
- $X \subseteq O$ ,
- $O' = O \setminus X$ ,
- $\delta' = (\delta \cup \{(q, \tau, q') \mid (q, x, q') \in \delta, x \in X\}) \setminus \{(q, x, q') \mid x \in X\}$ .

# HIDING

## DEFINITION (INTERNALISIERUNGSOOPERATOR)

Für ein EIO  $S = (Q, I, O, \delta, q_0, E)$  ist  $S/X$ , mit dem **Internalisierungsoperator**  $\cdot/\cdot$ , definiert als  $(Q, I, O', \delta', q_0, E)$  mit:

- $\tau \notin X$ ,
- $X \subseteq O$ ,
- $O' = O \setminus X$ ,
- $\delta' = (\delta \cup \{(q, \tau, q') \mid (q, x, q') \in \delta, x \in X\}) \setminus \{(q, x, q') \mid x \in X\}$ .

## DEFINITION (PARALLELKOMPOSITION MIT INTERNALISIERUNG)

Seien  $S_1$  und  $S_2$  komponierbare EIOs, dann ist die Parallelkomposition mit Internalisierung definiert als  $S_1|S_2 = S_{12}/(\text{Synch}(S_1, S_2) \cap O_{12})$ .