Kommunikationsfehler, Verklemmung und Divergenz bei Interface-Automaten

Kolloquium zur Bachelorarbeit

Ayleen Schinko

7. Mai 2016

Inhalt

Motivation

- Modellierung von Systemen und deren Kommunikationsverhalten
- simulation parallel arbeitender Softwarekomponenten

Motivation

- Modellierung von Systemen und deren Kommunikationsverhalten
- simulation parallel arbeitender Softwarekomponenten
- Kommunikationsfehler in Interface-Automaten nicht zulässig, deshalb Error-IO-Transitionssysteme mit optimistischer Fehlererreichbarkeit als Abwandlung davon betrachtet
  - Kommunikationsfehler (bzw. Error) zwischen Komponenten
  - Verklemmung (bzw. Ruhe) innerhalb einer Softwarekomponenten (keine Outputs mehr möglich)
  - Divergenz einer Softwarekomponenten (unendliche viele intere Aktionen)
- Verfeinerungsrelation über den Transitionssystemen (fehlerfreie Spezifikation durch fehlerfreies System verfeinert)

Motivation

- Modellierung von Systemen und deren Kommunikationsverhalten
- simulation parallel arbeitender Softwarekomponenten
- Kommunikationsfehler in Interface-Automaten nicht zulässig, deshalb Error-IO-Transitionssysteme mit optimistischer Fehlererreichbarkeit als Abwandlung davon betrachtet
  - Kommunikationsfehler (bzw. Error) zwischen Komponenten
  - Verklemmung (bzw. Ruhe) innerhalb einer Softwarekomponenten (keine Outputs mehr möglich)
  - Divergenz einer Softwarekomponenten (unendliche viele intere Aktionen)
- Verfeinerungsrelation über den Transitionssystemen (fehlerfreie Spezifikation durch fehlerfreies System verfeinert)
- gewünscht verfeinernde Präkongruenz
- Hiding (bzw. Internalisierung) von Outputs bildet Verbergen in der Parallelkomposition nach

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

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

- $Q = Q_1 \times Q_2$,
- $I = (I_1 \backslash O_2) \cup (I_2 \backslash O_1)$,
- $O = O_1 \cup O_2$,
- $q_0 = (q_{01}, q_{02})$,
- $\ldots$,

mit $\mathrm{Sync}(S_1, S_2) = (I_1 \cap O_2) \cup (O_1 \cap I_2) \cup (I_1 \cap I_2)$.

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

- $\ldots,$
- $$\begin{aligned}\delta = \{&((q_1, q_2), \alpha, (p_1, q_2)) \mid (q_1, \alpha, p_1) \in \delta_1, \\ &\alpha \in (\Sigma_1 \cup \{\tau\}) \backslash \mathrm{Synch}(S_1, S_2)\} \\ &\cup \{((q_1, q_2), \alpha, (q_1, p_2)) \mid (q_2, \alpha, p_2) \in \delta_2, \\ &\alpha \in (\Sigma_2 \cup \{\tau\}) \backslash \mathrm{Synch}(S_1, S_2)\} \\ &\cup \{((q_1, q_2), \alpha, (p_1, p_2)) \mid (q_1, \alpha, p_1) \in \delta_1, (q_2, \alpha, p_2) \in \delta_2, \\ &\alpha \in \mathrm{Synch}(S_1, S_2)\},\end{aligned}$$
- $\ldots,$

mit $\mathrm{Sync}(S_1, S_2) = (I_1 \cap O_2) \cup (O_1 \cap I_2) \cup (I_1 \cap I_2)$.

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

- $\ldots$,
- $$\begin{aligned} E =& (Q_1 \times E_2) \cup (E_1 \times Q_2) \\ & \cup \left\{ (q_1, q_2) \mid \exists a \in O_1 \cap I_2 : q_1 \xrightarrow{a} \wedge q_2 \not\xrightarrow{a} \right\} \\ & \cup \left\{ (q_1, q_2) \mid \exists a \in I_1 \cap O_2 : q_1 \not\xrightarrow{a} \wedge q_2 \xrightarrow{a} \right\}, \end{aligned}$$

mit $\mathrm{Sync}(S_1, S_2) = (I_1 \cap O_2) \cup (O_1 \cap I_2) \cup (I_1 \cap I_2)$.

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:

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

Definition (Ruhe)

Ein **Ruhe-Zustand** *ist ein Zustand in einem EIO, der keine Outputs und kein τ zulässt.*
Die Menge der Ruhe-Zustände in einem EIO ist wie folgt formal definiert:

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

Definition (Ruhe)

Ein **Ruhe-Zustand** *ist ein Zustand in einem EIO, der keine Outputs und kein τ zulässt.*
Die Menge der Ruhe-Zustände in einem EIO ist wie folgt formal definiert:

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

Definition (Divergenz)

Ein **Divergenz-Zustand** *ist ein Zustand in einem EIO, der eine unendliche Folge von τs 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 $S_1 \sqsubseteq^{\mathrm{B}}_{Div} S_2$ 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.*
$\sqsubseteq^{\mathrm{C}}_{Div}$ bezeichnet die **vollständige abstrakte Präkongruenz** *von $\sqsubseteq^{\mathrm{B}}_{Div}$ bezüglich $\cdot \| \cdot$.*

Definition (Traces)

Für ein EIO S wird definiert:

- **strikte Errortraces**: $StET(S) := \left\{ w \in \Sigma^* \mid q_0 \overset{w}{\Rightarrow} q \in E \right\}$,
- **gekürzte Errortraces**: $PrET(S) := \bigcup \{\text{prune}(w) \mid w \in StET(S)\}$,
- **Input-kritische Traces**:
  $MIT(S) := \left\{ wa \in \Sigma^* \mid q_0 \overset{w}{\Rightarrow} q \wedge a \in I \wedge q \overset{a}{\not\to} \right\}$,
- **Errortraces**: $ET(S) := \text{cont}(PrET(S)) \cup \text{cont}(MIT(S))$,
- **strikte Ruhetraces**: $StQT(S) := \left\{ w \in \Sigma^* \mid q_0 \overset{w}{\Rightarrow} q \in Qui \right\}$,
- **strikte Divergenztraces**: $StDT(S) := \left\{ w \in \Sigma^* \mid q_0 \overset{w}{\Rightarrow} q \in Div \right\}$,
- **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. $EDT_{12} = \text{cont}\,(\text{prune}\,((EDT_1 \| EDL_2) \cup (EDL_1 \| EDT_2)))$,
2. $QDT_{12} = (QDT_1 \| QDT_2) \cup EDT_{12}$,
3. $EDL_{12} = (EDL_1 \| EDL_2) \cup EDT_{12}$.

Satz (Error-, Ruhe- und Divergenz-Semantik für Parallelkomposition)

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

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

Proposition (Divergenz-Präkongrunez)

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

Definition (ω-Partner)

Ein EIO S_1 ist ein **ω-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 (ω-Partner)

Ein EIO S_1 ist ein **ω-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 $U \| S_1 \sqsubseteq_{Div}^{\mathrm{B}} U \| S_2$ für alle ω-Partner U gilt, dann folgt daraus $S_1 \sqsubseteq_{Div} S_2$.

Satz (Vollstänige Abstraktheit für Divergenz-Semantik)

Seinen S_1 und S_2 zwei EIOs mit derselben Signatur. Dann gilt $S_1 \sqsubseteq^{\mathrm{C}}_{Div} S_2 \Leftrightarrow S_1 \sqsubseteq_{Div} S_2$.

Satz (Vollständige Abstraktheit für Divergenz-Semantik)

Seinen S_1 und S_2 zwei EIOs mit derselben Signatur. Dann gilt $S_1 \sqsubseteq^{\mathrm{C}}_{Div} S_2 \Leftrightarrow S_1 \sqsubseteq_{Div} S_2$.

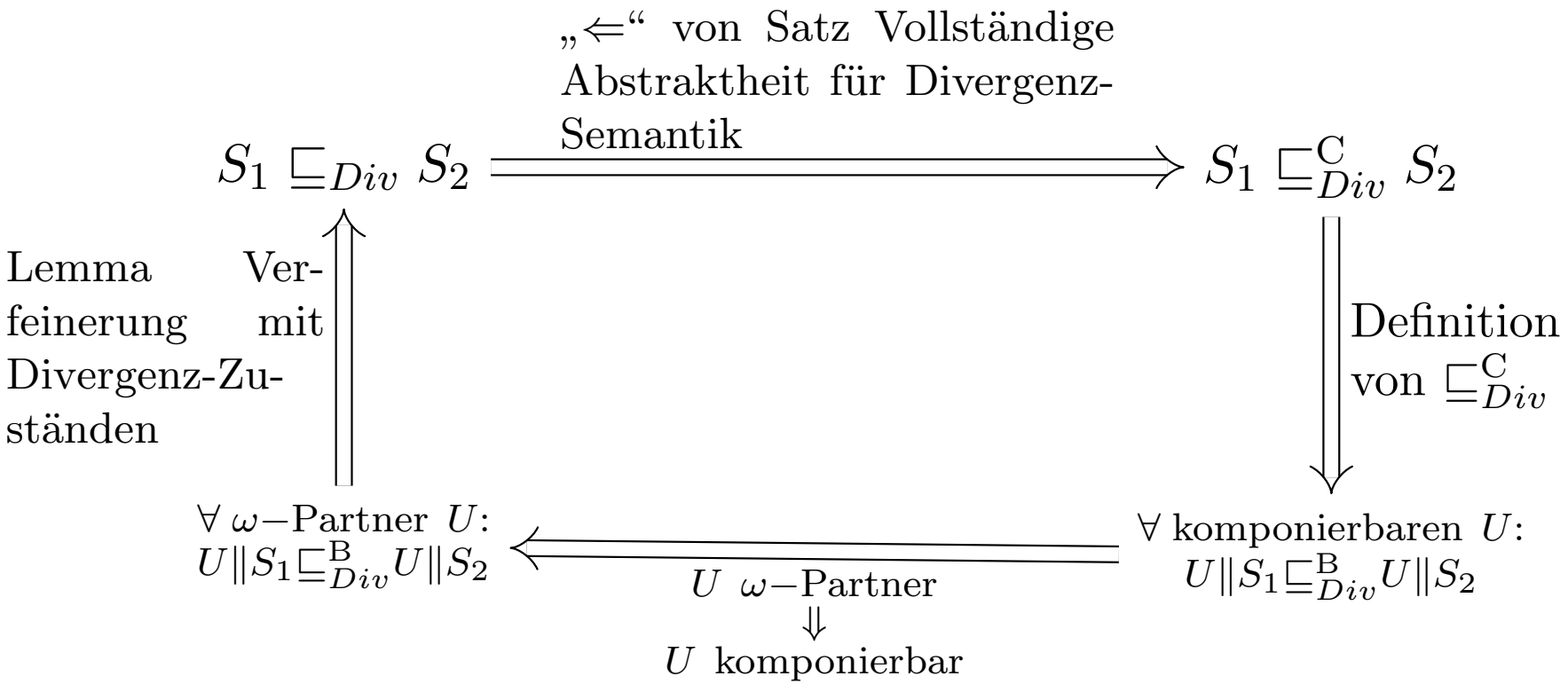

Abbildung : Folgerungskette

Korollar

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

Hiding

Definition (Internalisierungsoperator)

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:*

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

Hiding

Definition (Internalisierungsoperator)

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:*

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

Definition (Parallelkomposition mit Internalisierung)

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