Theorie reaktiver Systeme

Axiomatische Sicht

FD Semantik

Korrigierte Fassung 23.1.2008

$X \subseteq \Sigma$ ist *refusal* von P:

$\exists\, P'.P \overset{\langle\rangle}{\Rightarrow} P' \wedge \mathit{stable}(P') \wedge (\forall\, a \in X.a \notin \mathit{first}(P'))$

(s, X) ist *failure* von P:

$s \in \mathit{trace}(P), \mathit{stable}(P/s), X$ ist Refusal von P/s

$[\![P]\!]_{\mathcal{F}} = \{(s, X) \mid (s, X) \text{ ist failure von } P\}$

Äquivalenz und Refinement

$$P \sim_{\mathcal{F}} Q \Leftrightarrow [\![P]\!]_{\mathcal{F}} = [\![Q]\!]_{\mathcal{F}}$$

$$P \sqsubseteq_F Q \Leftrightarrow \begin{array}{l} \mathit{trace}(Q) \subseteq \mathit{trace}(P) \\ \wedge\ \mathit{failures}(Q) \subseteq \mathit{failures}(P) \end{array}$$

Zusammenhang mit Tests

$$P/s = \prod_{i \in I} (\Box\ a : B_i . a \rightarrow Q_i(a))$$

$$Ref(P/s) = \{M \subseteq \Sigma \mid \exists\, i . B_i \cap M = \emptyset\}$$

$$(s, A) \in [\![P]\!]_{\mathcal{F}} \Leftrightarrow \neg(P \textbf{ must } U_C(s, A))$$

$$[\![P]\!]_{\mathcal{F}} = [\![Q]\!]_{\mathcal{F}} \Leftrightarrow P \sim_{TE} Q$$

Axiomatische Semantikdefinition

Idee: Definiere Menge von *Axiomen* $\mathcal{A}_{\mathcal{F}}$, mit denen das Verhalten eines Prozesses präzise beschrieben wird.

Beispiel: Verhalten von SKIP:

$\text{SKIP} \,;\, P = P$

$P \,;\, \text{SKIP} = P$

$\text{SKIP} \setminus X = \text{SKIP}$

$\text{SKIP} \,\|\, \text{SKIP} = \text{SKIP}$

$\text{SKIP} \overset{X}{|||} P = P$

...

$=$ soll hier als $\sim_{\mathcal{F}}$ interpretiert werden.

Notation: $\mathcal{A}_{\mathcal{F}} \vdash P = Q$ falls $P = Q$ aus $\mathcal{A}_{\mathcal{F}}$ abgeleitet werden kann.

Ein Axiomsystem $\mathcal{A}_{\mathcal{F}}$ heisst *korrekt (sound)* wenn für alle P, Q mit $\mathcal{A}_{\mathcal{F}} \vdash P = Q$ gilt, dass $P \sim_{\mathcal{F}} Q$.

Ein Axiomsystem $\mathcal{A}_{\mathcal{F}}$ heisst *vollständig (complete)* wenn für alle P, Q mit $P \sim_{\mathcal{F}} Q$ gilt, dass $\mathcal{A}_{\mathcal{F}} \vdash P = Q$.

Für CSP Prozesse in der Failures-Semantik existiert ein Axiomsystem $\mathcal{A}_{\mathcal{F}}$, das korrekt und vollständig ist [Isobe and Roggenbach 2006]

Divergenz

P ist divergent:

$$\exists \langle P_i \rangle_{i \in \mathbb{N}}. P = P_0 \wedge \forall\, i. P_i \xrightarrow{\tau} P_{i+1}$$

divergierende Berechnungen von P:

$$\mathit{divergences}(P) = \{s \hat{} t \mid s \in \Sigma^* \wedge t \in (\Sigma \cup \{\surd\})^* \wedge \exists\, Q. P \overset{s}{\Rightarrow} Q \wedge Q \text{ ist divergent}\}$$

Failures/Divergences Semantik für CSP:

$$\mathit{failures}_\perp(P) = \mathit{failures}(P) \cup \{(s, X) \mid s \in \mathit{divergences}(P)\}$$

$$[\![P]\!]_{\mathcal{FD}} = \{(F, D) \mid F \in \mathit{failures}_\perp(P), D \in \mathit{divergences}(P)\}$$