

Theorie reaktiver Systeme

Acceptance Trees

Refusals

Failures

Failures Semantik

Bemerkung: Distributivität von $\sqcap$:

CSP-Operatoren sind distributiv über $\sqcap$.

Beispiele:

$$a \rightarrow (P \sqcap Q) = (a \rightarrow P) \sqcap (a \rightarrow Q)$$

$$(P \sqcap Q) \sqcup R = (P \sqcup R) \sqcap (Q \sqcup R)$$

Safety: Die Implementierung darf nur solche Berechnungen ausführen, die die Spezifikation auch ausführen kann

$$\text{traces}(\text{IMP}) \subseteq \text{traces}(\text{SPEC})$$

Requirement Coverage: Nach einer Berechnung mit Ereignisfolge s von IMP und SPEC darf IMP keine Fortsetzung verweigern, die SPEC nicht verweigern kann.

Robustness: Jede Berechnung die SPEC erlaubt, kann von IMP ausgeführt werden:

$$\text{trace}(\text{SPEC}) \subseteq \text{trace}(\text{IMP}).$$

Testing Äquivalenz

$$P \sim_{TE} Q \Leftrightarrow$$

$$1. \ P \text{ must } U_S(s, a) \Rightarrow Q \text{ must } U_S(s, a)$$

$$2. \ P \text{ may } U_R(s) \Rightarrow Q \text{ may } U_R(s)$$

$$3. \ P \text{ must } U_C(s, A) \Leftrightarrow Q \text{ must } U_C(s, A)$$

Konstruktion des *acceptance tree* von P .

Wurzel: P (eigentlich $P/\langle\rangle$)

Knoten: $\{P/s \mid s \in \text{trace}(P)\}$

Kanten: $P/s \xrightarrow{a} P/s \frown \langle a \rangle$, falls Transition $Q \xrightarrow{a} Q'$ existiert mit $Q \in P/s$, $Q' \in P/s \frown \langle a \rangle$.

– Deterministischer Graph

Refusals

Prozess P ist *stabil*:

$$stable(P) \Leftrightarrow \forall e, P' : P \xrightarrow{e} P' \Rightarrow e \neq \tau$$

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

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

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

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

$$\llbracket P \rrbracket_{\mathcal{F}} = \{(s, X) \mid (s, X) \text{ failure von } P\}$$

Eigenschaften der Failures-Semantik

- $(s, X) \in \llbracket P \rrbracket_{\mathcal{F}} \Rightarrow s \in \text{traces}(P)$
- $(s, X) \in \llbracket P \rrbracket_{\mathcal{F}} \wedge X' \subseteq X \Rightarrow (s, X') \in \llbracket P \rrbracket_{\mathcal{F}}.$
- $(s, X) \in \llbracket P \rrbracket_{\mathcal{F}} \wedge \forall a \in X'. s \hat{\langle a \rangle} \notin \text{traces}(P) \Rightarrow (s, X \cup X') \in \llbracket P \rrbracket_{\mathcal{F}}$
- $s \hat{\langle \checkmark \rangle} \in \text{traces}(P) \Rightarrow (s \hat{\langle \checkmark \rangle}, X) \in \llbracket P \rrbracket_{\mathcal{F}}$

- $(s \hat{\ } s', X) \in \llbracket P \rrbracket_{\mathcal{F}} \Rightarrow (s, \emptyset) \in \llbracket P \rrbracket_{\mathcal{F}}$
- $(s, X) \in \llbracket P \rrbracket_{\mathcal{F}} \wedge a \in \Sigma \Rightarrow (s \hat{\ } \langle a \rangle, \emptyset) \in \llbracket P \rrbracket_{\mathcal{F}} \vee (s, X \cup \{a\}) \in \llbracket P \rrbracket_{\mathcal{F}}$

CSP Prozesse

- $\llbracket \text{STOP} \rrbracket_{\mathcal{F}} = \{(\langle \rangle, X) \mid X \subseteq \Sigma \cup \{\checkmark\}\}$
- $\llbracket \text{SKIP} \rrbracket_{\mathcal{F}} = \{(\langle \rangle, X) \mid \checkmark \notin X\} \cup \{(\langle \checkmark \rangle, X) \mid X \subseteq \Sigma \cup \{\checkmark\}\}$
- $\llbracket a \rightarrow P \rrbracket_{\mathcal{F}} = \{(\langle \rangle, X) \mid a \notin X\} \cup \{(\langle a \rangle^s, X) \mid (s, X) \in \llbracket P \rrbracket_{\mathcal{F}}\}$
- $\llbracket P_1 \sqcap P_2 \rrbracket_{\mathcal{F}} = \{(\langle \rangle, X) \mid (\langle \rangle, X) \in \llbracket P_1 \rrbracket_{\mathcal{F}} \cap \llbracket P_2 \rrbracket_{\mathcal{F}}\} \\ \cup \{(s, X) \mid s \neq \langle \rangle \wedge (s, X) \in \llbracket P_1 \rrbracket_{\mathcal{F}} \cup \llbracket P_2 \rrbracket_{\mathcal{F}}\}$

- $\llbracket P_1 \sqcap P_2 \rrbracket_{\mathcal{F}} = \llbracket P_1 \rrbracket_{\mathcal{F}} \cup \llbracket P_2 \rrbracket_{\mathcal{F}}$

- ...

[Schneider 2000], Kapitel 6.