Theorie reaktiver Systeme

Requirement Coverage

Robustness

Korrigierte Fassung 9.1.2008

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

Konstruktion von Requirement Coverage Tests

Gegeben ist P in Head-Normal-Form,

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

Ziel: Konstruktion einer *minimalen* Menge von Tests

Nötig:

- Abdecken der verschiedenen Möglichkeiten *nach* der internen Auswahl.

$$\forall\, i \in I.\ (\{a_1, \ldots, a_l\} \cap B_i) \neq \emptyset$$

- Minimalität

$$\forall\, j \in \{1, \ldots, l\},\ \exists\, i \in I.\ (\{a_1, \ldots, a_l\} - \{a_j\}) \cap B_i = \emptyset$$

$$M = \{\, \{a_1, \ldots, a_l\} \mid \forall\, i \in I.\ (\{a_1, \ldots, a_l\} \cap B_i) \neq \emptyset \\ \wedge\ \forall\, j \in \{1, \ldots, l\},\ \exists\, i \in I.\ (\{a_1, \ldots, a_l\} - \{a_j\}) \cap B_i = \emptyset \,\}$$

Requirement Coverage Tests

Gegeben ist P in Head-Normal-Form,

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

A ist minimale Coverage-Testmenge der Länge 1 für P:
$U_A = (\Box\ a \in A . a \rightarrow \omega \rightarrow \mathrm{STOP})$
mit $A = \{a_1, \ldots, a_l\}$ mit
$\forall\, i \in I : \{a_1, \ldots, a_l\} \cap B_i \neq \emptyset$
$\wedge\ \forall\, j \in \{1, \ldots, l\} . \exists\, i \in I . (\{a_1, \ldots, a_l\} - \{a_j\}) \cap B_i = \emptyset$

Requirement Coverage Tests

$$
\begin{aligned}
U_C(s, A) = \quad & \textbf{if } s = \langle\,\rangle \\
& \textbf{then } \Box\ a : A.a \rightarrow \omega \rightarrow \mathrm{STOP} \\
& \textbf{else } \omega \rightarrow \mathrm{STOP} \ \Box\ head(s) \rightarrow U_C(tail(s), A)
\end{aligned}
$$

für $s \in trace(P)$ und A minimale Coverage Testmenge der Länge 1 für P/s.

Requirement Coverage Tests

$\mathcal{H}_{Req}(P) = \{U_C(s, A) \mid s \in trace(P) \wedge$

A minimale Coverage-Testmenge der Länge 1 für $P/s\}$.

P *must* $U_C(s, A)$ für alle $U_C(s, A) \in \mathcal{H}_{Req}(P)$.

$\mathcal{H}_{Req}(P)$ ist minimal.

Falls Q $\underline{must}$ $U_C(s, A)$ für alle $U_C(s, A) \in \mathcal{H}_{Req}(P)$,
so folgt Q erfüllt *Requirement Coverage* für P.

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

$trace(SPEC) \subseteq trace(IMP)$.

Damit folgt: *Safety* und *Robustness* $\Longleftrightarrow$ Traceäquivalenz.

Robustness Tests

$$U_R(s) = \begin{array}{l} \textbf{if } s = \langle\,\rangle \\ \textbf{then } \omega \rightarrow \mathrm{STOP} \\ \textbf{else } head(s) \rightarrow U_R(tail(s)) \end{array}$$

$$\mathcal{H}_{Robust}(P) = \{U_R(s) \mid \begin{array}{l} s \in trace(P) \wedge \forall\, u \in trace(P) : \\ s \leq u \wedge first(P/u) = \emptyset \rightarrow s = u\}. \end{array}$$

Falls Q $\underline{may}$ $U_R(s)$ für alle $U_R(s) \in \mathcal{H}_{Robust}(P)$, so gilt $\overline{trace(P) \subseteq trace(Q)}$.