Formalisierung von Sicherheits– und Lebendigkeitseigenschaften

Hendrik Tews
Lehrstuhl Algebraische und logische Grundlagen der Informatik
Betreuer: Prof. Dr. rer. nat. habil. Horst Reichel

Zum Promotionsthema

Im Mittelpunkt der geplanten Dissertation zum Thema

Eigenschaften (co–)algebraisch spezifizierter Prozeßsysteme

sollen Untersuchungen stehen, inwieweit das Verhalten bekannter Kalküle zur Darstellung von Parallelität und nichtdeterministischem Verhalten innerhalb der im Lehrstuhl verfolgten Idee, einer dialgebraischen Spezifikation von Prozeßsystemen, nachgebildet werden kann. Dazu wurden eine Reihe der in der theoretischen Informatik verwendeten Prozeßmodelle (u.a. unendliche Spuren, Spurensprachen und Ereignisstrukturen) und Logiken (z.B. der μ-Kalkül), mit denen man Eigenschaften für Prozesse formulieren kann, untersucht. Dabei stellte sich heraus, daß in fast allen Veröffentlichungen ein Konzept von Sicherheits– oder Lebendigkeitseigenschaften diskutiert wurde. Aufgrund des Fehlens einer vom verwendeten Prozeßmodell unabhängigen Charakterisierung dieser Eigenschaften waren diese Konzepte schwer vergleichbar. Zum zweiten war durch die äußerst informale Charakterisierung von Sicherheits– und Lebendigkeitseigenschaften eine Klassifizierung von Prädikaten bezüglich dieser beiden Gruppen nur schwer möglich.

Beispiel

Als Beispiel soll ein beschrankter Bahnübergang im π-Kalkül modelliert werden:

$$\begin{aligned}
\mathsf{Rail} &\overset{\text{def}}{=} \mathsf{train}\,.\,\mathsf{green}\,.\,\overline{\mathsf{tcross}}\,.\,\overline{\mathsf{red}}\,.\,\mathsf{Rail}\\
\mathsf{Road} &\overset{\text{def}}{=} \mathsf{car}\,.\,\mathsf{up}\,.\,\overline{\mathsf{ccross}}\,.\,\overline{\mathsf{down}}\,.\,\mathsf{Road}\\
\mathsf{Signal} &\overset{\text{def}}{=} \overline{\mathsf{green}}\,.\,\mathsf{red}\,.\,\mathsf{Signal} + \overline{\mathsf{up}}\,.\,\mathsf{down}\,.\,\mathsf{Signal}\\
\mathsf{Crossing} &\overset{\text{def}}{=} (\mathsf{green})(\mathsf{red})(\mathsf{up})(\mathsf{down})\ (\mathsf{Road} \mid \mathsf{Rail} \mid \mathsf{Signal})
\end{aligned}$$

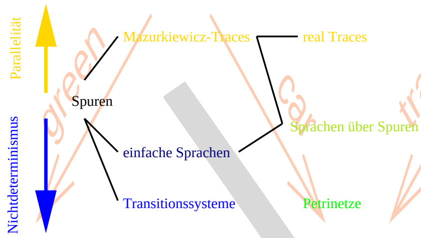
Das zugehörige Transitionssystem ist im Plakathintergrund zu sehen. Eine Sicherheitseigenschaft ist dann Unfallfreiheit:

$$\nu Z\,.\,([-]Z \wedge \neg(\langle\mathsf{tcross}\rangle\mathsf{tt} \wedge \langle\mathsf{ccross}\rangle\mathsf{tt}))$$

Eine Lebendigkeitseigenschaft (die der gegebene Bahnübergang nicht erfüllt) wäre, daß jedes Auto nach endlicher Wartezeit die Schienen überqueren kann:

$$\nu Z\,.\,[-]Z \wedge [\mathsf{car}]\,(\mu Y\,.\,\langle -\rangle tt \wedge [-\overline{\mathsf{ccross}}]Y)$$

Prozeßmodelle



Sicherheits– und Lebendigkeitseigenschaften

Eine **Sicherheitseigenschaft** beschreibt, daß ein (negativ bewertetes) Ereignis im gesamten Prozeßverlauf niemals eintritt.

Typisches Beispiel: Deadlock–Freiheit	im μ-Kalkül : $\nu Z.\neg P \wedge [-]Z$ in CLT* : ¬ EF P

Eine **Lebendigkeitseigenschaft** beschreibt, daß ein (positive bewertetes) Ereignis in der Zukunft eintreten wird.

Typisches Beispiel: Antworten auf Anforderungen	im μ-Kalkül : $\mu Z.P \vee (\langle\rangle\mathsf{tt} \wedge [-]Z)$ in CLT* : AF P

Topologie

Mit Hilfe einer Topologie U kann man einer Menge X unendlicher Objekte eine Struktur geben. Die Struktur besteht daraus, daß bestimmte Teilmengen von X als *offen* klassifiziert werden. Dann können Begriffe wie Limite, abgeschlosse und dichte Mengen definiert werden.

Definition

Sei

- M die Menge aller Prozesse in einem gegebenen Prozeßmodell,
- d eine Ultrametrik auf M, so daß

  „p und q verhalten sich länger identisch als q und r“

  impliziert $d(p,q) < d(q,r)$.

Eine Prädikat $P \subseteq M$ heißt **starke Sicherheitseigenschaft**, wenn P in (M,d) abgeschlossen ist,
P heißt **schwache Lebendigkeitseigenschaft**, wenn P dicht in (M,d) ist.

Anwendung der Definition auf Transitionssysteme

Zwei Tranistionssysteme p, q sind n–bisimular $p \overset{n}{\sim} q$, wenn sie vom Startzustand ausgehend über maximal n Aktionen hinweg bisimulares Verhalten zeigen.
Mittels des Abstandes zweier Transitionssysteme:

$$\begin{aligned}
l(p,q) &\overset{\text{def}}{=} \sup\,\{\, n \mid p \overset{n}{\sim} q \}\\
d(p,q) &\overset{\text{def}}{=} 2^{-l(p,q)}
\end{aligned}$$

erhält man eine Topologie.
Ein Prädikat $P \subseteq TS$ ist eine Sicherheitseigenschaft, genau dann wenn

$$\forall p \notin P\,.\,\exists n \leq |p|\,.\,\forall q \in TS\,.\quad p \overset{n}{\sim} q \implies q \notin P$$

Das ungewollte Ereignis ist p bis zur Tiefe n.
Ein Prädikat $P \subseteq TS$ ist eine Lebendigkeitseigenschaft, genau dann wenn

$$\forall p \in TS\,.\,\forall n < |p|\,.\,\exists q \in TS\,.\quad p \overset{n}{\sim} q \ \wedge\ q \in P$$

q ist die Fortsetzung von p, in der das gewünschte Ereignis auftritt.

Anwendung der Definition auf unendliche Spuren (real traces)

Gegeben sei ein endliches Alphabet Σ und eine Abhängigkeitsrelation $D \subseteq \Sigma \times \Sigma$.
Eine unendliche Spur wird informal als Paar (ω, A) beschrieben, wobei $\omega \in \Sigma^* \cup \Sigma^\infty$ und $A \subseteq \Sigma$ die Menge der Aktionen ist, die von den unendlich oft in ω auftretenden Aktionen abhängen. Für zwei Spuren a, b bezeichnet $a \cdot b$ die Verkettung beider.
Mittels der Präfixmetrik d_{pref} erhält man eine Topologie.
Ein Prädikat P ist eine Sicherheitseigenschaft genau dann, wenn für alle Spuren a mit endlicher Länge gilt

$$a \notin P \implies \forall b\,.\,(a \cdot b) \notin P$$

Hierbei beschreibt a einen unsicheren Prozeß.
Ein Prädikat P ist eine Lebendigkeitseigenschaft genau dann, wenn für alle unendlichen Spuren a gilt:

$$\exists b\,.\,(a \cdot b) \in P$$

Der Prozeß b ist hier die Forstzung von a, die das gewünschte Ereignis realisiert.

Begehung des Graduiertenkollegs „Werkzeuge zum effektiven Einsatz paralleler und verteilter Rechnersysteme“ am 24. Juni 1997