Semantik reaktiver Systeme

- Syntax: Definition von Prozesstermen
  - Basisterm 0: Deadlock
  - Operatoren:
    - Präfix a P: erst Ereignis a , dann wie P
    - Choice P | Q: sowohl P als auch Q anbieten
    - Or P ∏ Q: entweder P oder Q
    - Parallel P || Q: P und Q nebenläufig
- Semantik:
  - Zuordnen von Bedeutung zu Prozesstermen
    - Vergleichen von Prozesstermen
    - Vergleichen von Prozesstermen und Eigenschaften
  - Schließen über Prozesse
  - Zentral: Interaktion anstatt Nebenläufigkeit

Operationelle Semantik

- Ursprung: Termersetzung
- Vertreter: CCS, π-Kalkül, StateCharts
- Zwei-Schritt-Semantik:
  - Zuordnung von Beobachtungen:
    - Allgemein: Beobachtung Abarbeitung abstr. Maschine
    - SOS: Zustände = Prozessterme, Abarbeitung = Syntax
  - Äquivalenz Prozesse = Äquivalenz Beobachtungsbäume
    - Bisimulation: R ist starke Bisimulation falls p R q impliziert
      - $p \vdash a\ p' \Rightarrow \exists q.\ q \vdash a\ q' \wedge p'\ R\ q'$
      - $q \vdash a\ q' \Rightarrow \exists p.\ p \vdash a\ p' \wedge p'\ R\ q'$
    - Starke Kongruenz: größte Bisimulationsrelation
- Anmerkungen:
  - Regeln: $a \rightarrow P \vdash a\ P, \quad P \vdash a\ P' \Rightarrow P \parallel Q \vdash a\ P' \parallel Q$
  - Bisimulation mit oder ohne unsichtbare Schritte

Denotationelle Semantik

- Ursprung: Scott-Domains
- Vertreter: Hoare (CSP), Kahn (SPF), Jonsson (IOA)
- Zwei Schritte:
  - Abbildung der Syntax auf mathematisches Modell
  - Schlußfolgern im mathematischen Modell
- Beispiel: Spursemantik T:
  - $T[0] = \{<>\}$, $T[a \rightarrow P] = \{ a \bullet t \mid t \in T[P] \}$
  - $(a \rightarrow b \rightarrow 0 \mid b \rightarrow a \rightarrow 0) = (a \rightarrow 0) || (b \rightarrow 0)$
- Merkmale:
  - Modell ist ein Bereich (vollständige Halbordung)
  - Rekursion ist kleinster Fixpunkt
  - Abbildung oft indirekt als Kalkül

Beoachtung von Prozessen

- Vergleiche von Prozessen
  - Denotationelle Semantik
    - Gleichheit der Prozesse (gleiche Mengen)
    - Ordnung der Prozesse (Teilmengen)
  - Operationelle Semantik:
    - Gleichheit der Prozesse (Bisimulation)
    - Ordnung der Prozesse (Simulation)
  - Algebraische Semantik:
    - Gleichheit von Prozessen
- Feinheit der Unterscheidung:
  - Bisimulation: $a \rightarrow 0 \prod b \rightarrow 0 \prod (a \rightarrow 0 \mid b \rightarrow 0)$
  - Failuresem., algebraisch: $a \rightarrow 0 \prod b \rightarrow 0, (a \rightarrow 0 \mid b \rightarrow 0)$
  - Tracesemantik

True Concurrency

- Beobachtbarkeit der Nebenläufigkeit
  - Kann Nebenläufigkeit effektiv festgestellt werden?
  - Axiom der beliebigen Sequentialisierung
    - Alternative/Nebenläufigkeit nicht unterscheidbar
    - $(a \rightarrow P)||(b \rightarrow Q) = (a \rightarrow P||(b \rightarrow P)) \mid (b \rightarrow (a \rightarrow P)||Q)$
  - Spursemantik:
    - Sequentialisierung von Abläufen
  - CCS:
    - Gleichheit von Prozessen durch Bisimulation
    - Transitionsrelation mit einem Ereignis markiert
  - Algebraisch:
    - Gleichheit nur bei passender Schlussregel
    - Je nach Axiomenmengen
- Echte Nebenläufigkeit: Petrinetze, SPF, ICSP

Kompositionalität

- Idee: modulares Schließen
  - $P \Rightarrow A$, $Q \Rightarrow B$ und damit auch: $P \wedge Q \Rightarrow A\ (\wedge B)$
  - Aber: reaktive Systeme
    - P erfüllt A, Q erfüllt B und trotzdem P||Q erfüllt nicht A
    - Eigenschaften von Modulen „gehen verloren“
    - Ursache: Beoachtungsbegriff berücksichtigt Umgebung nicht
- Modelle:
  - Tracesemantik für CSP: nicht kompositional
    - Betrachte $(a \rightarrow 0 \prod b \rightarrow 0)$, $(a \rightarrow 0 \mid b \rightarrow 0)$
  - Failuresemantik: induktiv und damit kompositional
  - CCS: Bisimulation ist eine Kongruenzrelation
  - Algebren: Gleichheit ist eine Kongruenzrelation

Völlig abstrakt

- Verträglichkeit denotationell, operationell, algebraisch
  - Algebraisch: Prüfen der Axiome
  - Denotationell/operationell: Prozessäquivalenzen
- Völlige Abstraktheit:
  - Gegeben: Beobachtungsbegriff/Äquivalenzrelation ~
  - Gesucht: Semantik mit = größte Kongruenz bzgl. ~
  - Beobachtung: Kompositionalität
- Anschaulich: Kontexte
  - Gleiche Prozesse verhalten sich im selben Kontext gleich
  - Formal: $T[P] = T[Q] \Leftrightarrow K(P) \sim K(Q)$ für beliebige K
  - Intuitiv: Semantik unterscheidet nicht feiner als ~
  - Readiness ist nicht völlig abstrakt: $a \rightarrow 0 \prod b \rightarrow 0$ vs. $a \rightarrow 0 \prod b \rightarrow 0 \prod (a \rightarrow 0 \mid b \rightarrow 0)$

Spezifikation und Semantik

- Systementwicklung: von Spezifikation zu System
  - System: beschrieben durch Prozessterm/Modell
  - Spezifikation: abhängig von der Semantik
    - Algebraisch/Operationell: Prozessäquivalenz
    - Operationell: TL-Aussagen über Beobachtungsbaum
    - Denotationell: Aussagen über mathematisches Modell
  - Spezifikationsarten:
    - Aussagen über Interaktionsfolgen (IOA, CCS, CSP)
    - Aussagen über Zustandsfolgen: Operationale Semantik
  - Zuordnung Spezifikation/System:
    - Direkt: Bestimmung Abbildungen, Nachweis Eigenschaft
    - Indirekt: Kalkül P sat S(t) $\Rightarrow$ a $\rightarrow$P sat t = a • s $\wedge$ P(s)
    - Einheitlich: Modell = Spezifikation

Sicherheit und Lebendigkeit

- Beobachtung: zwei Beweisprinzipien
  - Invarianz:
    - Verletzung zu einem bestimmten Zeitpunkt feststellbar
    - partielle Korrektheit, Sicherheit
  - Noether:
    - Termination, Lebendigkeit
    - Verletzung im Unendlichen feststellbar
- Formalisierung (Alpern/Schneider)
  - Begriffe: P Prädikat über Zustandssequenzen
    - P ist S-Eigenschaft: P zulässig und $P(t) \wedge s \leq t \Rightarrow P(s)$
    - P ist L-Eigenschaft: s endlich $\Rightarrow \exists t.\ s \leq t \wedge P(t)$
  - Kombination: Jede Eigenschaft ist S/L-Kombination
- Randbemerkungen:
  - Maschinenabschluß: Sicherheit erlaubt Lebendigkeit
  - Implementierung: starkes S, schwaches L (Fairness)

Lebendigkeit, Fairness, Zulässigkeit

- Begriffe:
  - Fairness:
    - Elementare Abstraktion (IOA, Parallelität)
    - Schwach: $\Box$enabled(a)$\Rightarrow\Box\Diamond$executed(a)
    - Stark: $\Box\Diamond$ enabled(a)$\Rightarrow\Box\Diamond$executed(a)
  - Lebendigkeit: s endlich $\Rightarrow \exists t.\ s \leq t \wedge P(t)$
  - Zulässigkeit:
    - Ähnlich Stetigkeit: vom Endlichen zur unendlichen Grenze
    - Formal: $\forall i.\ P(t_i) \Rightarrow P(\lim_i t_i)$
- Zusammenhänge:
  - Fairness ist eine Lebendigkeitseigenschaft
  - Fairness ist i.a. nicht zulässig (Beispiel: Zeitbombe)
  - Lebendigkeit ist i.a. nicht zulässig (Beispiel: Termination)
  - Modelle sind i.a. stetig/zulässig

Schlagwörter

- Rückblick:
  - Semantiken und ihre Zusammenhänge
  - Semantiken und Spezifikationen
- Zukünftige:
  - Nichtdeterminismus
  - Synchron/Asynchron
  - Zustandsmodelle (IOA,Kripke,WS1S)
  - Logiken (TL,μ-Kalküle)