Modellierung verteilter Systeme

Grundlagen der Programm und Systementwicklung

Sommersemester 2012

Prof. Dr. Dr. h.c. Manfred Broy

Unter Mitarbeit von Dr. M. Spichkova, J. Mund, P. Neubeck

Lehrstuhl Software & Systems Engineering

Sichtenintegration

Zustand und Ablauf

- Zusammenhang zwischen Zustandsmodell Ablaufmodell
  - Jedem **Zustand** σ wird eine Menge von Abläufen $abl(\sigma)$ zugeordnet
  - **Zustandsübergänge**: Im Zustand σ ist der endliche Ablauf q ∈ $abl(\sigma)$ möglich und führt vom Zustand σ zum Zustand σ‘

$$\sigma \xrightarrow{q} \sigma'$$

- Zustandsbegriff ist **adäquat**, wenn aus jedem Zustand die Menge der möglichen Abläufe ableitbar ist (d.h. $abl(\sigma)$ ist wohldefiniert)
- Zustandsmenge heißt **voll abstrakt**, wenn je zwei verschiedene Zustände auch unterschiedliche Mengen von Abläufen beschreiben
- voll abstrakt = Zustände redundanzfrei
  (ähnlich zu minimalen Automaten in formalen Sprachen)

Lineare Temporale Logik

- Zustandsmaschinen mit markierten Übergängen besitzen sequentielle Abläufe

$$\sigma_0 \xrightarrow{a_1} \sigma_1 \xrightarrow{a_2} \sigma_2 \xrightarrow{a_3} \ldots \xrightarrow{a_i} \sigma_i \xrightarrow{a_{i+1}} \ldots$$

- Ablauf endet, wenn keine Übergänge mehr möglich sind
  → endliche Berechnung

- Bei totaler Übergangsrelation sind alle Abläufe unendlich
- Jeder Zustand hat dann eine Menge von unendlichen Strömen von Zuständen und eine Menge von unendlichen Strömen von Aktionen
- Ablauf auch als Strom von Paaren (σ_i, a_{i+1}) beschreibbar

Abläufe von Zustandsmaschinen

- Gegeben eine Zustandsmaschine mit markierten Übergängen
- Wir können jedem Zustand einfach eine Menge von sequentiellen Abläufen zuordnen

- Behandlung von nichtsequentielle Abläufe
  - Darstellung von Parallelität auf der Ebene der Zustandsmaschinen
  - Erweiterung der Übergänge auf Übergänge mit Mengen von Aktionen

Lineare Temporale Logik: Fairness

- Abläufe als Strom von Paaren bestehend aus Zustand und ausgeführter Aktion
- Für ein Paar $(\sigma, b) \in \Sigma \times Action$ eines Stroms und eine Aktion a definieren wir die Prädikate:
  - $exec(a)$, falls $a = b$ (Aktion a wird ausgeführt)
  - $enabled(a)$, falls gilt:

$$\$s' : s \xrightarrow{a} s'$$

- Ablauf heißt **schwach fair**, falls für alle Aktionen a gilt:

$$\Box[(\Box\ \text{enabled}(a)) \Rightarrow \Diamond\ \text{exec}(a)]$$

- Ablauf heißt **stark fair**, falls für alle Aktionen a gilt:

$$\Box[(\Box\ \Diamond\ \text{enabled}(a)) \Rightarrow \Diamond\ \text{exec}(a)]$$

Äquivalenz von Zustandsmaschinen

- Verschiedene Systeme können in Hinblick auf bestimmte Beobachtungen gleiches Verhalten realisieren
- Es gibt unterschiedliche Definitionen für die Äquivalenz zweier Systeme (bei Zustandsmaschinen zweier Anfangszustände)
- Ein guter Äquivalenzbegriff erlaubt es, in einer Komposition/Architektur ein Teilsystem gegen ein äquivalentes auszutauschen
  - Kongruenz
  - Kompatibilität
  - Schnittstellengleichheit (Verfeinerung, siehe später)

- Äquivalenzbegriffe für Zustände (erweiterbar auf Mengen von Zuständen und Zustandsmaschinen) von Maschinen mit markierten Übergängen:
  - Spuräquivalenz
  - Bisimulationsäquivalenz
  - Verweigerungs- bzw. Bereitschaftsäquivalenz

Definition: Spuräquivalenz

- Zwei Zustandsmaschinen M_1 und M_2 mit Startzuständen σ_0 und σ'_0 heißen **(aktions-) spuräquivalent**, wenn ihre Mengen von Aktionsspuren übereinstimmen.

- Spuräquivalenz ist formal definiert durch:

$$M_1 \sim_{Spur} M_2 \Leftrightarrow spuren(s_0) = spuren(s'_0)$$

- wobei

$$\text{spuren}(\sigma_0) = \left\{ a \in A^{\infty} : \exists \sigma \in \Sigma^{\infty} : \forall i \geq 0 : \sigma_i \xrightarrow{a_{i+1}} \sigma_{i+1} \right\}$$

Definition: Simulation

- Eine Präordnung $\leq$ über der Menge der Zustände heißt **Simulation**, wenn für alle Zustände σ, φ die Aussage $\sigma \leq \varphi$ genau dann gilt, wenn:

$$\forall a \in A, \sigma' \in \Sigma: \sigma \xrightarrow{a} \sigma' \Rightarrow \exists \varphi' \in \Sigma: \varphi \xrightarrow{a} \varphi' \wedge \sigma' \leq \varphi'$$

- Für Zustandsmaschinen M_1 und M_2 mit Startzustände σ_0 und σ'_0 definieren wir:

  M_1 simuliert M_2 , geschrieben $M_1 \leq M_2$
  wenn eine Simulation $\leq$ mit $\sigma_0 \leq \sigma'_0$ existiert.

Definition: Bisimulation

- Eine Äquivalenzrelation ~ über Zuständen heißt **Bisimulation**, wenn für alle Zustände σ, φ, die Aussage σ ~ φ genau dann gilt, wenn:

$$\forall a \in A, \sigma' \in \Sigma: \sigma \xrightarrow{a} \sigma' \Rightarrow \exists \varphi' \in \Sigma: \varphi \xrightarrow{a} \varphi' \wedge \sigma' \sim \varphi'$$

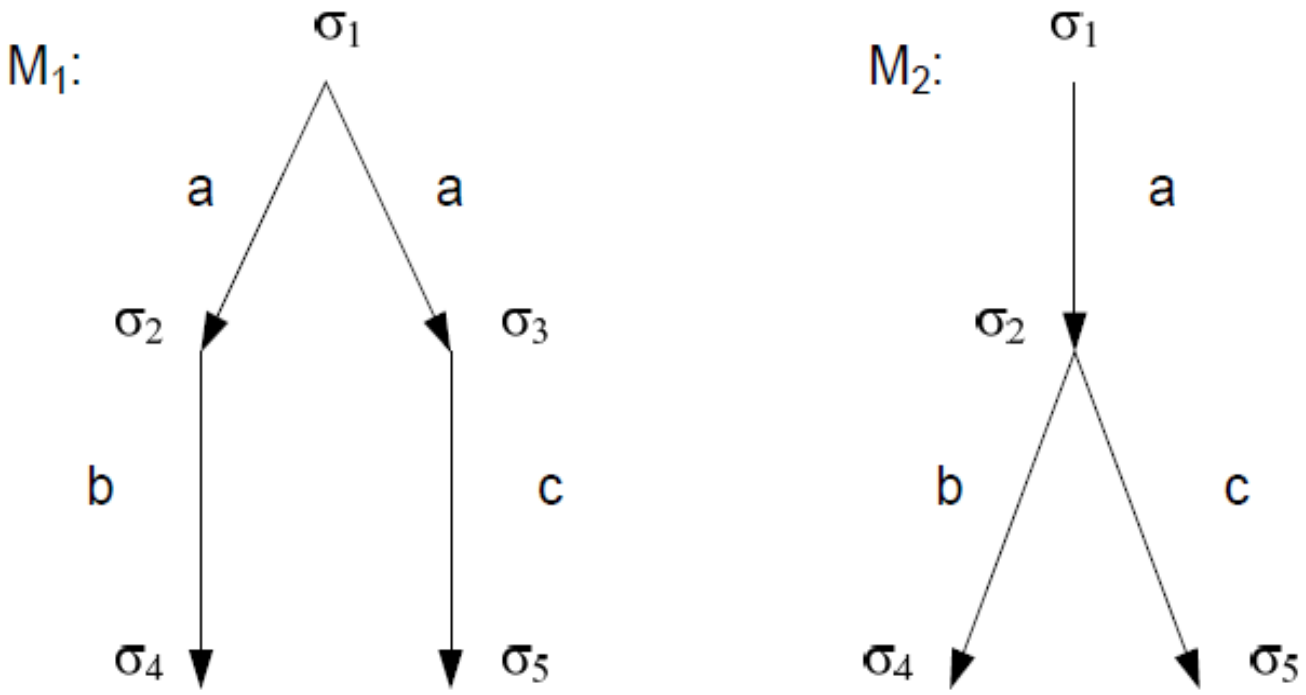
und

$$\forall a \in A, \varphi' \in \Sigma: \varphi \xrightarrow{a} \varphi' \Rightarrow \exists \sigma' \in \Sigma: \sigma \xrightarrow{a} \sigma' \wedge \sigma' \sim \varphi'$$

- Zwei Zustandsmaschinen M_1 und M_2 mit Startzuständen σ_0 und σ_0' heißen **bisimulationsäquivalent**, geschrieben $M_1 \sim_{bi} M_2$, wenn eine Bisimulation ~ mit $\sigma_0 \sim \sigma_0$' existiert.

Beispiel: Vergleich Spur- und Bisimulationsäquivalenz

Die Zustandsmaschinen M_1 und M_2 sind spuräquivalent, aber nicht bisimulationsäquivalent.



Vergleich Spur- und Bisimulationsäquivalenz

- Bisimulationsäquivalenz impliziert Spuräquivalenz
- Je nach gewähltem Kompositionoperator ist eine andere Äquivalenz geeignet
  - Bei asynchroner Kommunikation Spuräquivalenz
  - Bei synchroner Kommunikation Bisimulationsäquivalenz
- z.B. gilt die *Kongruenz*

$$\Delta_2 \sim_{\text{Spur}} \Delta_3 \Rightarrow \Delta_1 \| \Delta_2 \sim_{\text{Spur}} \Delta_1 \| \Delta_3$$

Definition: Bereitschaftsäquivalenz

- Zwei Zustände σ_0 und σ_1 heißen **bereitschaftsäquivalent**, wenn

$$\sigma_1 \approx \sigma_2 \equiv \sigma_1 \sqsubseteq \sigma_2 \wedge \sigma_2 \sqsubseteq \sigma_1$$

- Die Relation $\sqsubseteq$ ist dabei definiert durch:

$$\sigma_1 \sqsubseteq \sigma_2 \equiv \forall t \in A^* : R_t(\sigma_1) \angle R_t(\sigma_2)$$

- Weiterhin sei definiert:

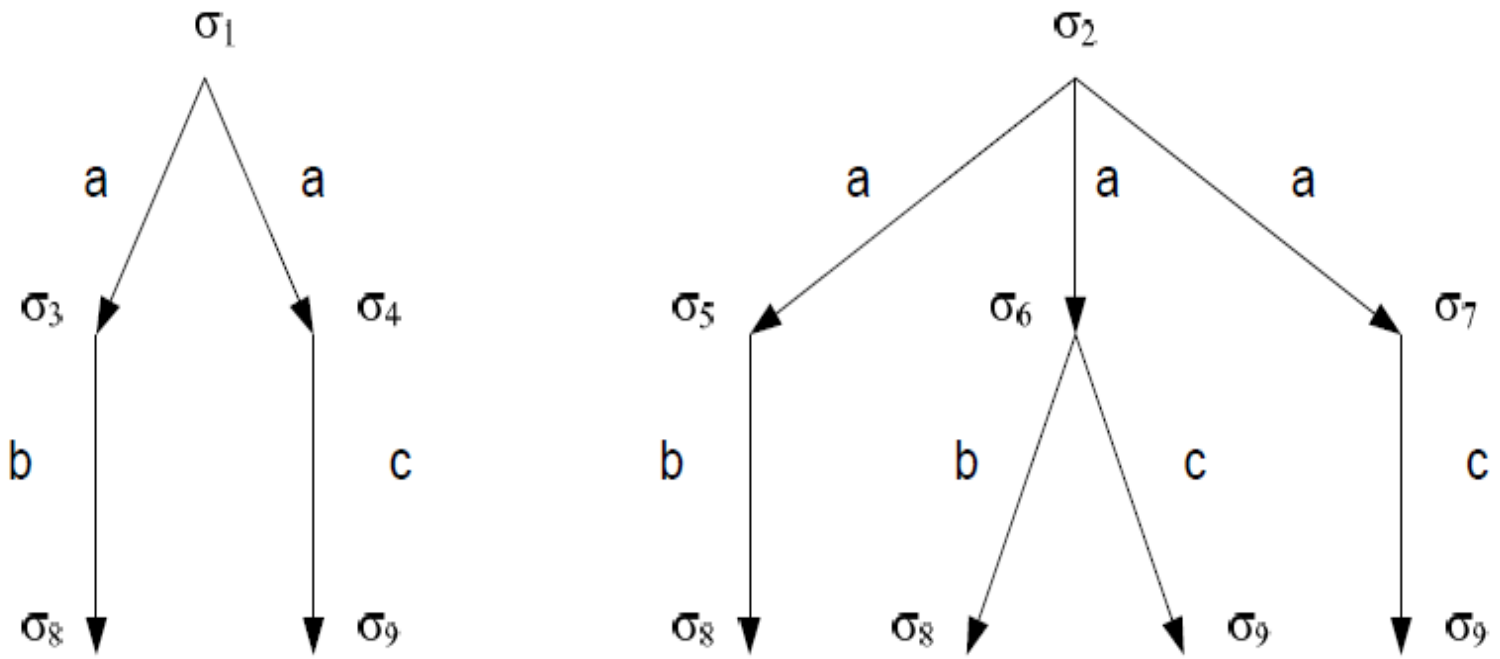
$$enabled(\sigma) = \{a \in A : \exists \sigma' \in \Sigma : \sigma \xrightarrow{a} \sigma'\}$$

$$R_t(\sigma_0) = \{enabled(\sigma) : \sigma_0 \xrightarrow{t} \sigma\}$$

$$S_1 \angle S_2 \equiv (S_1 = \emptyset) \vee (S_2 \neq \emptyset \wedge \forall M \subseteq A : (\exists M_2 \in S_2 : M_2 \cap M = \emptyset) \Rightarrow (\exists M_1 \in S_1 : M_1 \cap M = \emptyset))$$

Vergleich Bereitschafts- und Bisimulationsäquivalenz

Die Zustände σ_1 und σ_2 sind spur- und bereitschaftsäquivalent, aber nicht bisimulationsäquivalent



Vergleich der Äquivalenzbegriffe

- Bisimulationsäquivalenz impliziert Bereitschaftsäquivalenz

$$\sim_{bi} \Rightarrow \approx$$

- Bereitschaftsäquivalenz impliziert Spuräquivalenz

$$\approx \Rightarrow \sim_{Spur}$$