Bisimulationen und Model Refinement

Roland Glück[1,2]

[1]Universität Augsburg

[2]Deutsches Zentrum für Luft- und Raumfahrt

8.10.2014
Augsburg

Agenda

- einführendes Beispiel
- Abstraktion zu Modellen und Bisimulationen
- behandelbare Probleme
- algebraischer Ansatz
- Ausblick

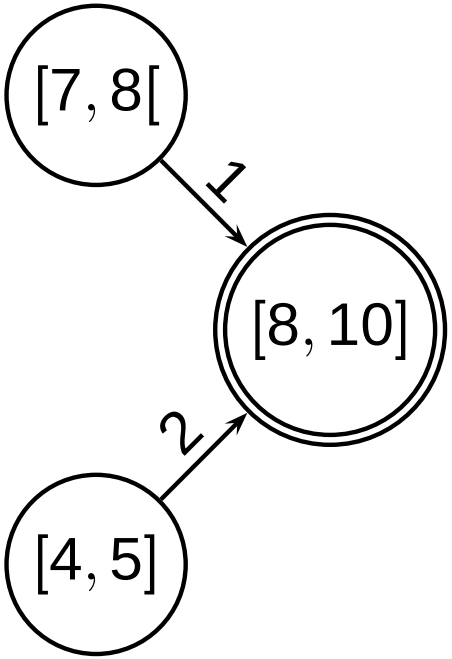
Ein einfaches Spiel

- Wir betrachten folgendes Einpersonenspiel auf $[3, 10]$:
- Jede Zahl in $[3, 8[$ kann um Eins erhöht werden.
- Jede Zahl in $[4, 5]$ kann zusätzlich verdoppelt werden.
- Erhöhen um Eins kostet eine Einheit,
- Verdoppeln zwei Einheiten.
- Ziel: Erreiche Zahl im Zielgebiet $[8, 10]$.

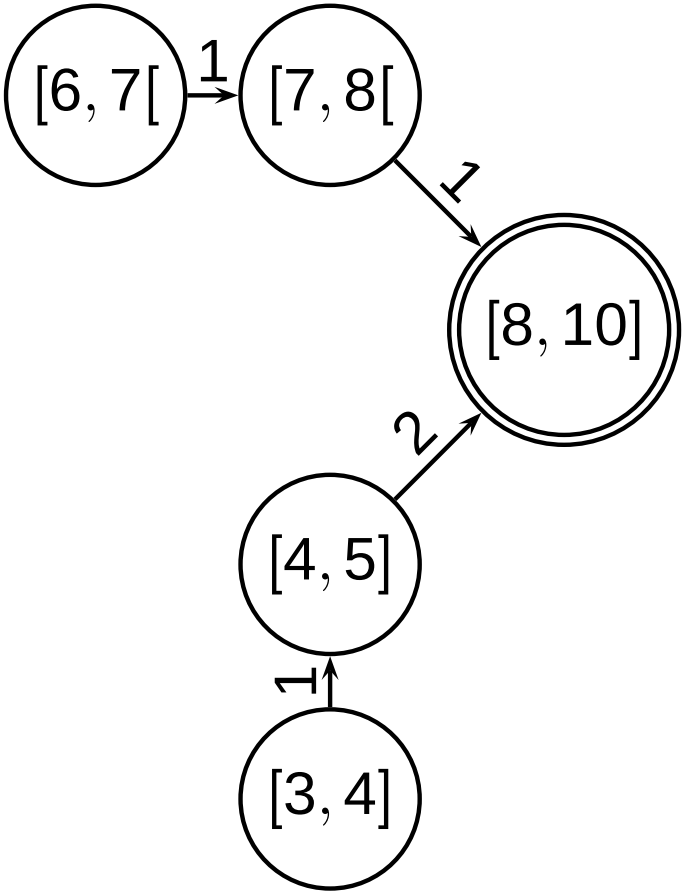
Ein einfaches Spiel

- Das Zielgebiet soll mit möglichst geringen Kosten erreicht werden,
- und zwar von jeder Startzahl aus.
- Aufgabe: Finde passende Routingtabelle.
- Zunächst intuitive Lösung

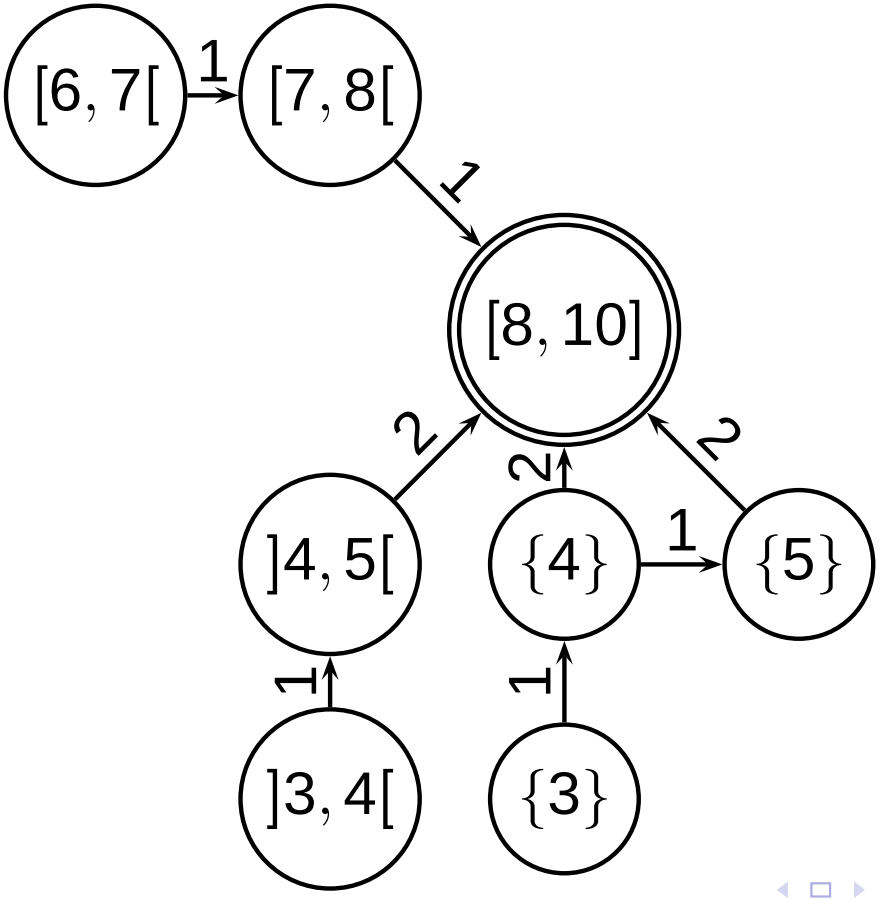
Erster Schritt



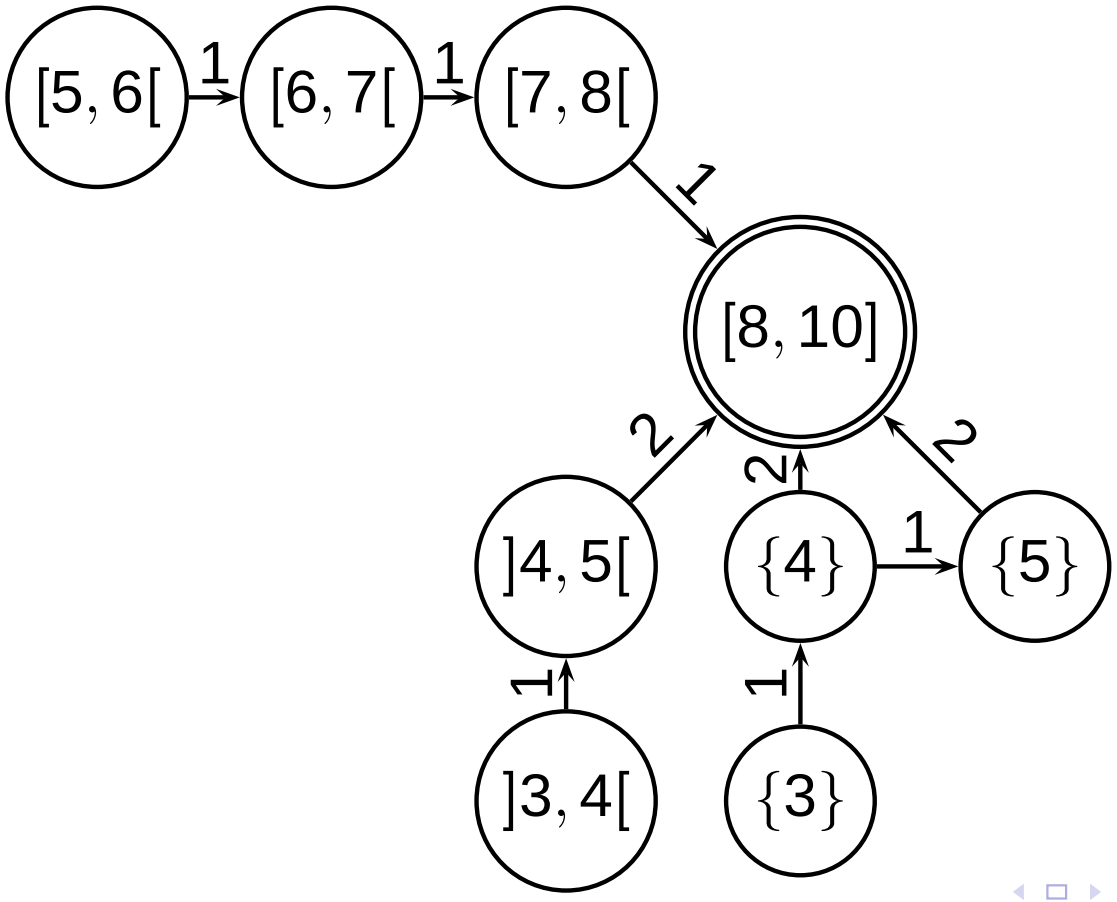
Zweiter Schritt



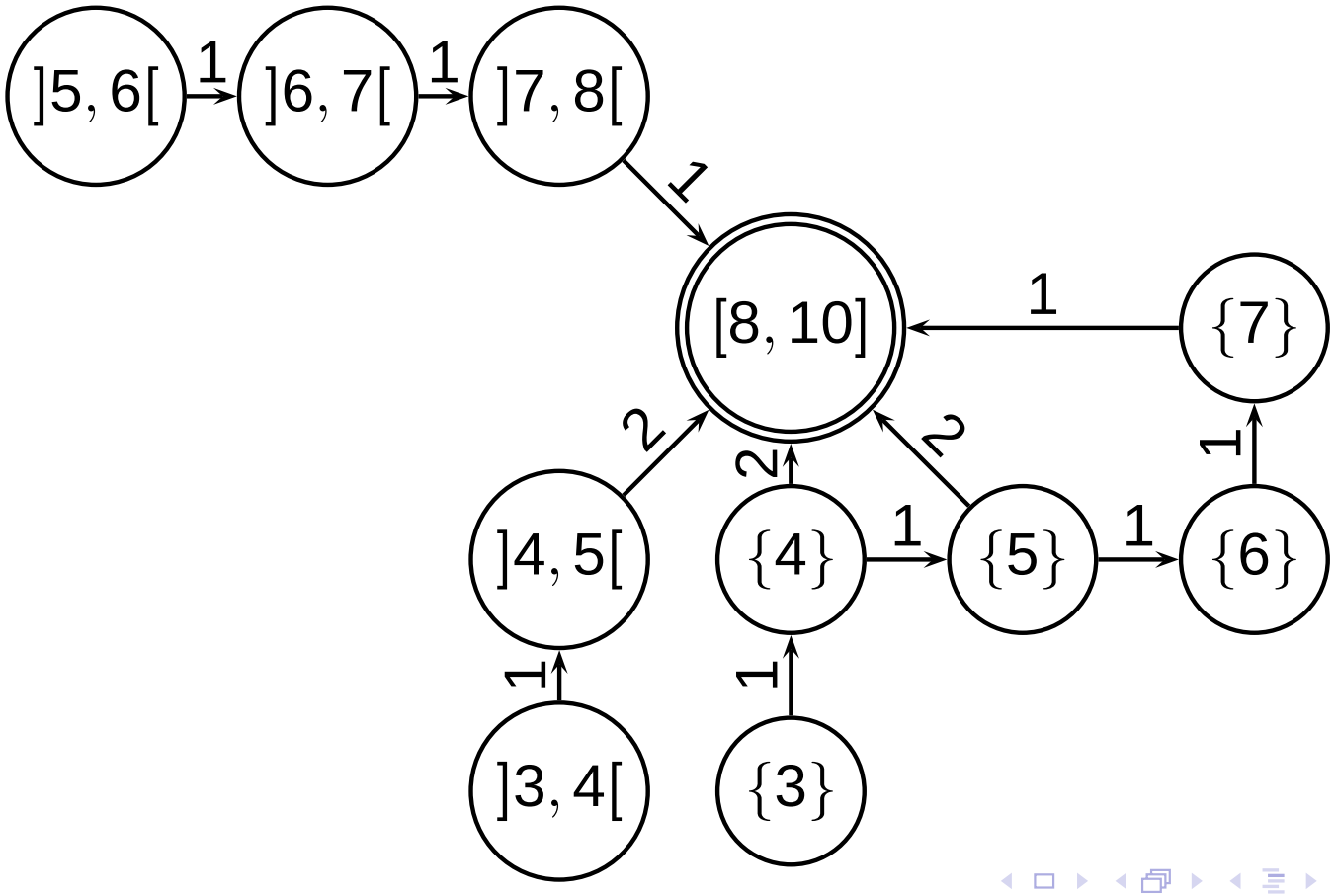
Dritter Schritt



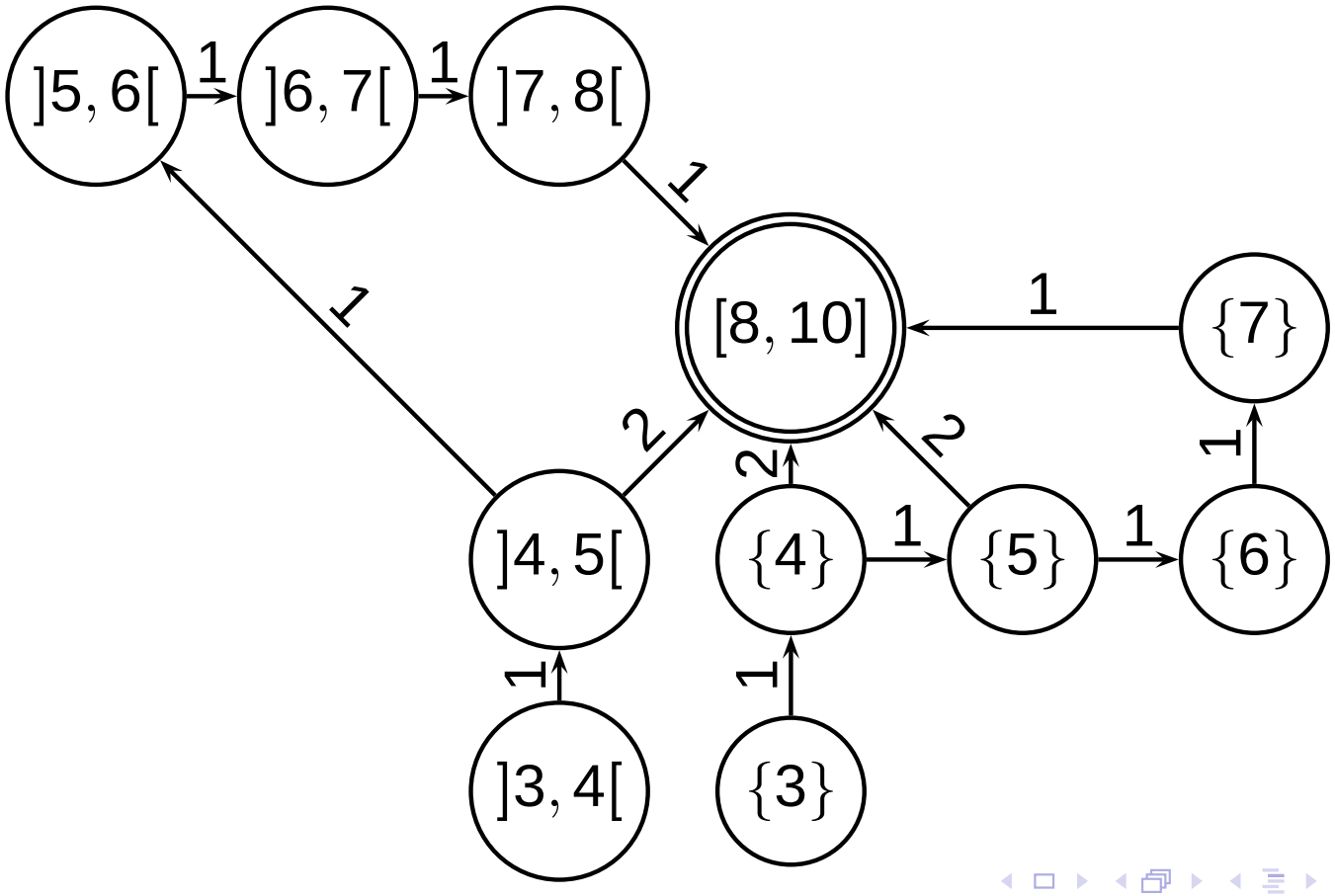
Vierter Schritt



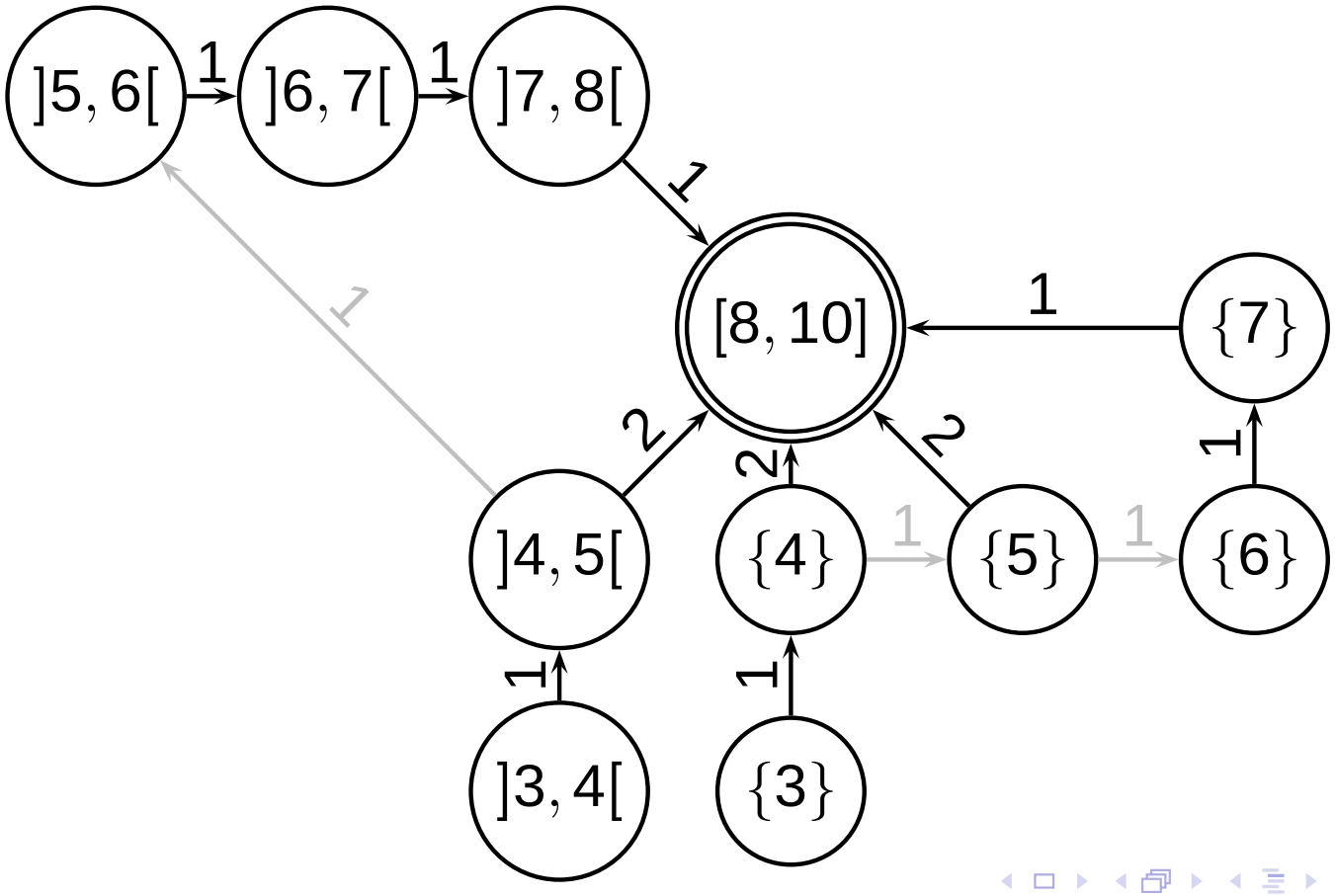
Fünfter Schritt



Sechster Schritt



Endergebnis



Rekapitulation

- Ziel: Verfeinerung eines großen Systems
- 1. Schritt: Großes System wurde auf ein kleineres mit äquivalentem Verhalten reduziert
- 2. Schritt: Reduziertes System wurde verfeinert
- 3. Schritt: Verfeinerung des großen Systems wurde aus Verfeinerung des reduzierten Systems gewonnen

Definition des Modells

Definition

Ein *Modell* ist eine Struktur $M = (((V, E), g), a)$ mit folgenden Anforderungen:

- (V, E) ist ein gerichteter Graph.
- $g : E \to 2^L \setminus \{\emptyset\}$ ist die *Kantenbeschriftungsfunktion*.
- $a : V \to A$ ist die *Knotenbeschriftungsfunktion*.

Abstraktion der Strategie

- Strategie entstand durch Entfernen unerwünschter Übergänge
- Abstraktion: Verfeinerung
- beschreibt Entfernen von Kanten und Kantenbeschriftungen

Definition der Verfeinerung

Definition

Ein Modell $M' = (((V', E'), g'), a')$ heißt *Verfeinerung* oder *Untermodell* eines Modells $M = (((V, E), g), a)$, falls folgendes gilt:

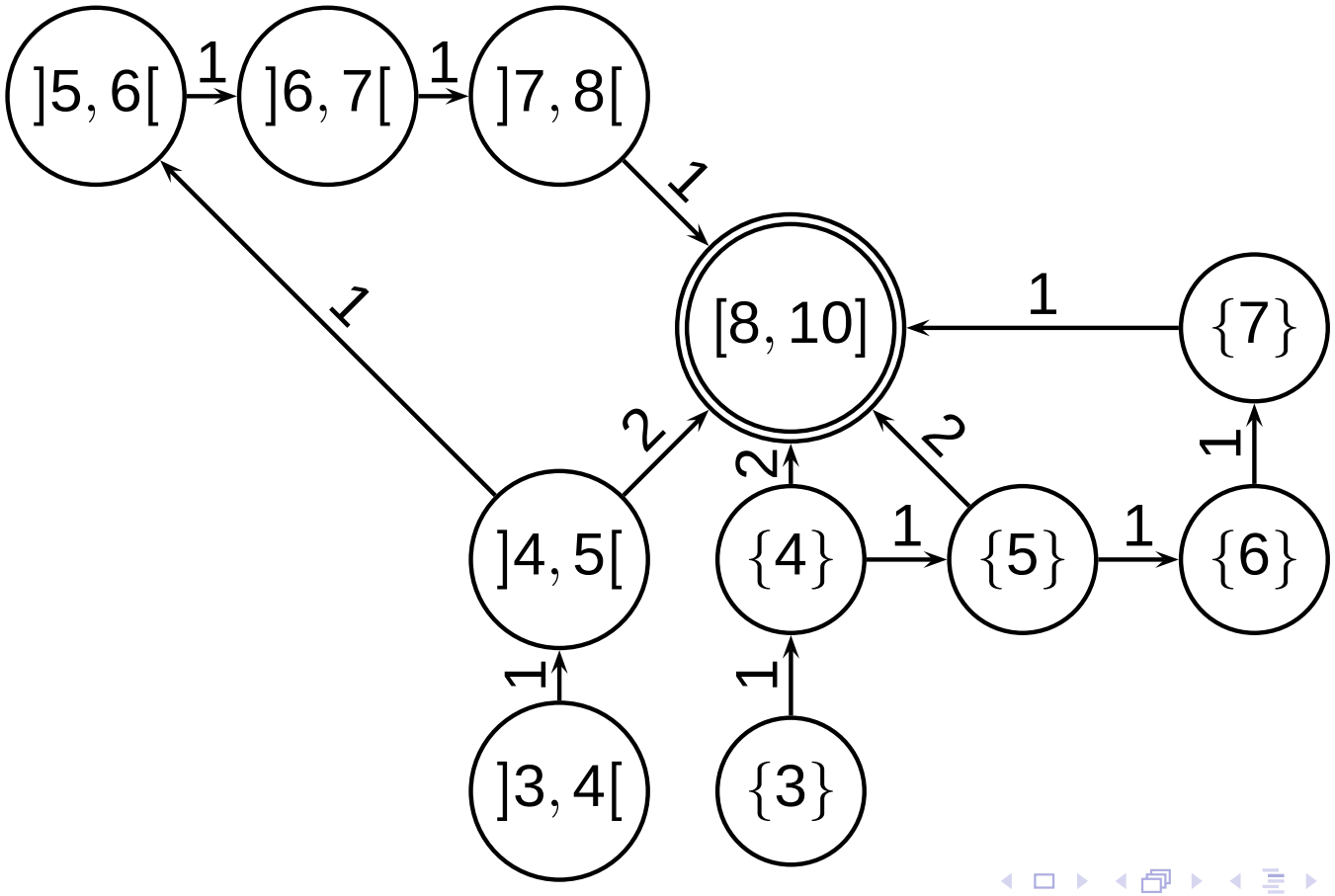
- $V' = V$ und $a' = a$.
- $E' \subseteq E$
- $\forall (u, v) \in E' : g'(u, v) \subseteq g(u, v)$

Ziel der Verfeinerung

Ziele der Verfeinerung:

- Sicherheits- und Lebendigkeitseigenschaften
- Optimalität von Wegen
- Optimalität von stochastischen Spielen
- ...

Rekapitulation



Bisimulation

Definition

Seien $M_1 = (((V_1, E_1), g_1), a_1)$ und $M_2 = (((V_2, E_2), g_2), a_2)$ zwei Modelle. Eine Relation $B \subseteq V_1 \times V_2$ heißt *Bisimulation* zwischen M_1 und M_2, falls sie die folgenden Eigenschaften erfüllt:

- B ist links- und rechtstotal.
- $v_1 B v_2 \Rightarrow a_1(v_1) = a_2(v_2)$
- $v_1 \xrightarrow{\ell}_{E_1} w_1 \wedge v_1 B v_2 \Rightarrow \exists w_2 : v_2 \xrightarrow{\ell}_{E_2} w_2 \wedge w_1 B w_2$
- $v_2 \xrightarrow{\ell}_{E_2} w_2 \wedge v_2 B^{\smile} v_1 \Rightarrow \exists w_1 : v_1 \xrightarrow{\ell}_{E_1} w_1 \wedge w_2 B^{\smile} w_1$

Autobisimulation

- Autobisimulation: Bisimulation zwischen einem Modell und sich selbst
- abgeschlossen unter Komposition, Konversenbildung und Vereinigung
- somit existiert größte Autobisimulation für ein Modell
- ist gleichzeitig Äquivalenzrelation
- Äquivalenzklassen enthalten maximale Mengen von Knoten mit gleichartigem Verhalten
- Äquivalenzklassen in $O(|E| \cdot log(|V|))$ Zeit berechenbar (Paige und Tarjan)

Der Quotient

Definition

Sei $M = (((V, E), g), a)$ ein Modell und B eine Bisimulationsäquivalenz für M. Dann ist der *Quotient* $M/B = (((V/B, E/B), g/B), a/B)$ das wie folgt definierte Modell:

- V/B ist die Menge der Äquivalenzklassen von B.
- $a/B(v/B) = a(v)$.
- $(v/B, w/B) \in E/B \Leftrightarrow \exists v' \in v/B\, \exists w' \in w/B : (v', w') \in E$.
- $\ell \in g/B(v/B, w/B) \Leftrightarrow \exists v' \in v/B\, \exists w' \in w/B : (v', w') \in E \wedge \ell \in g(v', w')$.

Expansion einer Verfeinerung

- Quotient hat höchstens so viele Knoten wie das ursprüngliche Modell
- Verfeinerung des Quotienten einfacher
- Notwendigkeit einer Zurückübersetzung
- formalisiert durch Expansionsoperation

Die Expansionsoperation

Definition

Sei $M = (((V, E), g), a)$ ein Modell, B eine Bisimulationsäquivalenz für M und $(M/B)' = ((((V/B)', (E/B)'), (g/B)'), (a/B)')$ eine Verfeinerung des Quotienten (M/B). Dann ist die *Expansion* $(M/B)' \backslash B = (((V', E'), g'), a')$ das wie folgt definierte Modell:

- $V' = V$ und $a' = a$.
- $(v, w) \in E' \Leftrightarrow (v, w) \in E \wedge (v/B, w/B) \in (E/B)' \wedge \exists \ell : \ell \in (g/B)'(v/B, w/B) \wedge \ell \in g(v, w)$
- $\ell \in g'(v, w) \Leftrightarrow \ell \in g(v, w) \wedge \ell \in (g/B)'(v/B, w/B)$

Allgemeiner Ansatz

$$\begin{tikzcd}
M \arrow[r, "\text{Verfeinerung}"] \arrow[d, "\text{Quotientenbildung}"'] & M' \\
M/B \arrow[r, "\text{Verfeinerung}"] & (M/B)' \arrow[u, "\text{Expansion}"']
\end{tikzcd}$$

Definition des Omegaautomaten

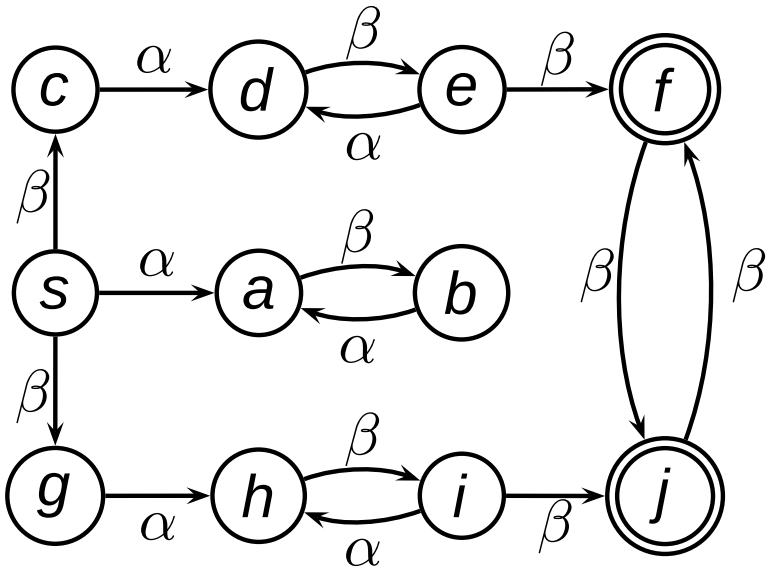
Definition

Ein *Omegaautomat* ist ein Modell $M = (((V, E), g), a)$ mit $a : V \to \mathcal{P}(\{\text{init}, \text{F}\})$ und genau einem init-Knoten. Ein *Kontroller C* für einen Omegaautomat ist eine Abbildung $C : V \to 2^{lm(g)}$. Der von einem Kontroller C kontrollierte Omegaautomat lässt an jedem Knoten genau die Übergänge mit den entsprechenden Kantenlabels zu.

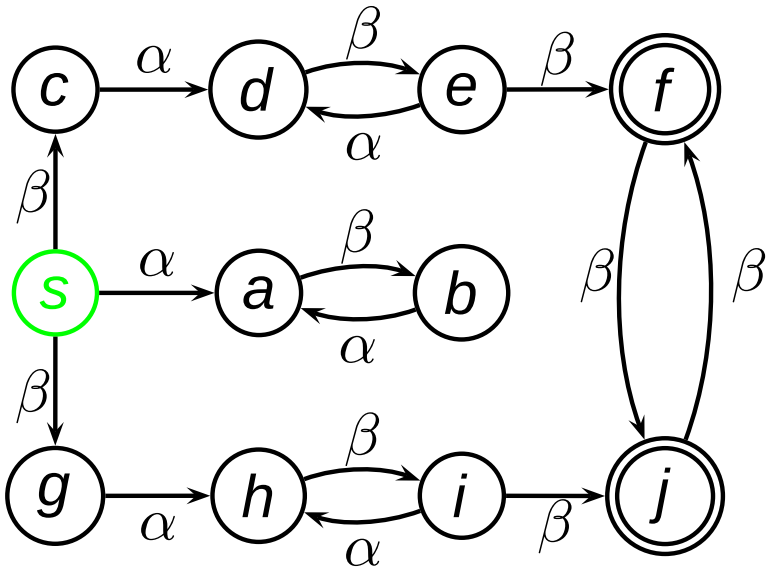
Kontrolle eines Omegaautomaten

- Knoten mit Label F sind ‚gute' Knoten.
- Ziel: Garantiere Sicherheits- und Lebendigkeitseigenschaften der Form $\Box F$, $\Diamond F$, $\Box\Diamond F$ und $\Diamond\Box F$ für alle Wege, die im init-Knoten starten.
- Ansatz über Quotienten korrekt

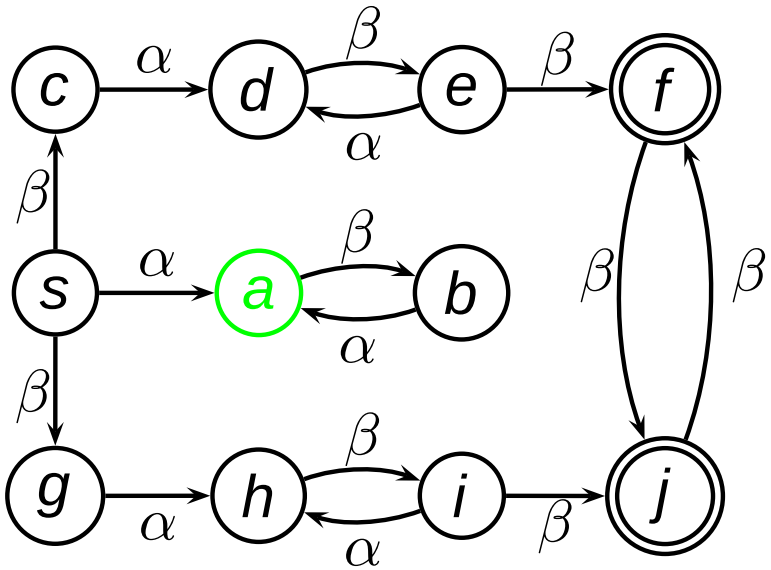
Ein Omegaautomat



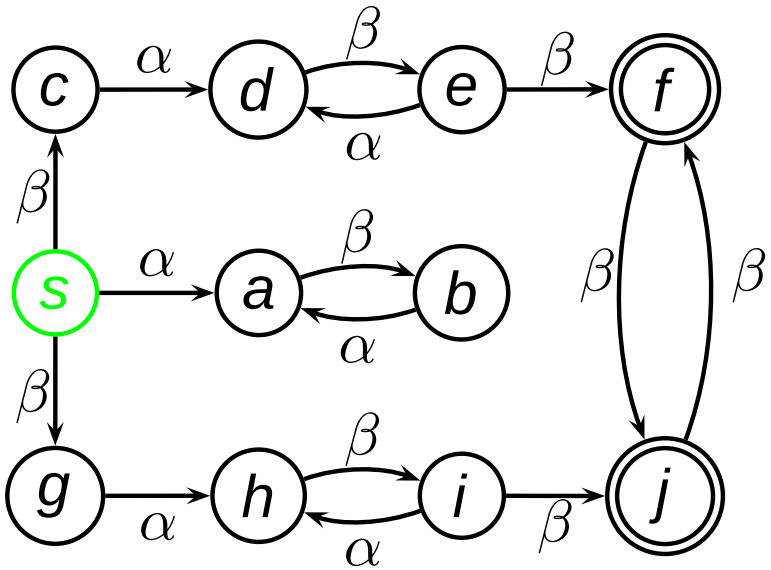
1. Beispiellauf



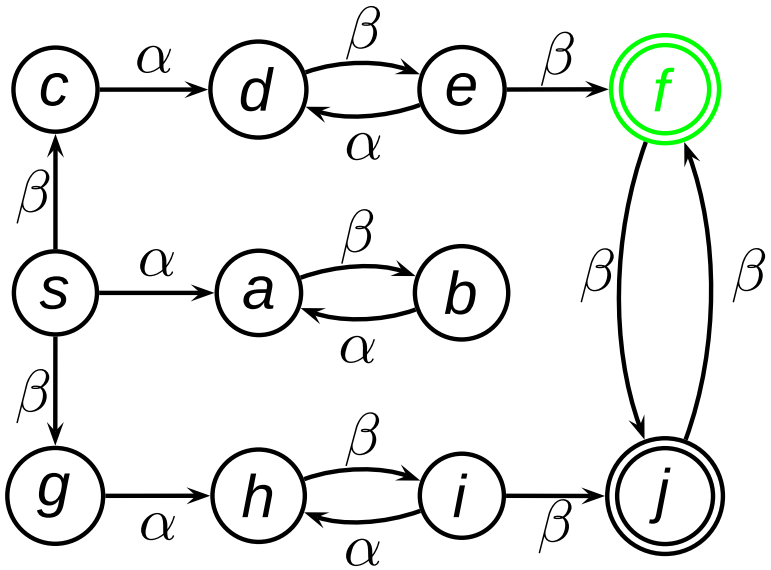
1. Beispiellauf



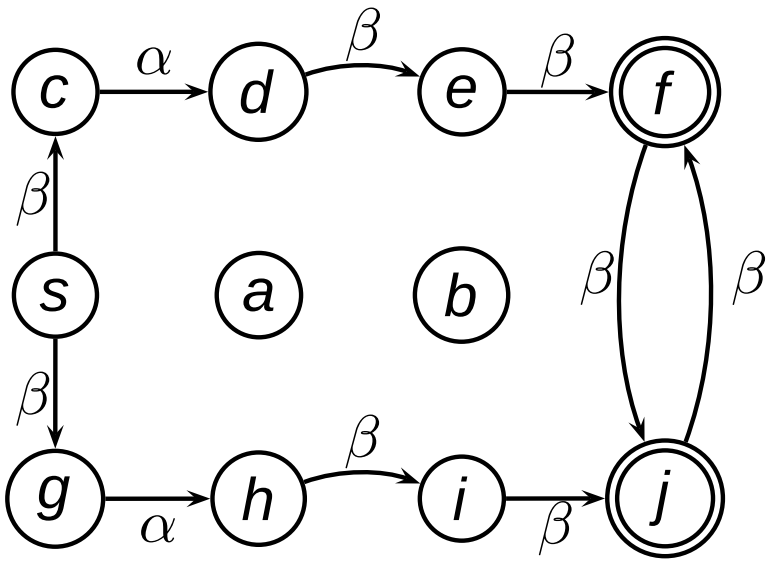
2. Beispiellauf



2. Beispiellauf

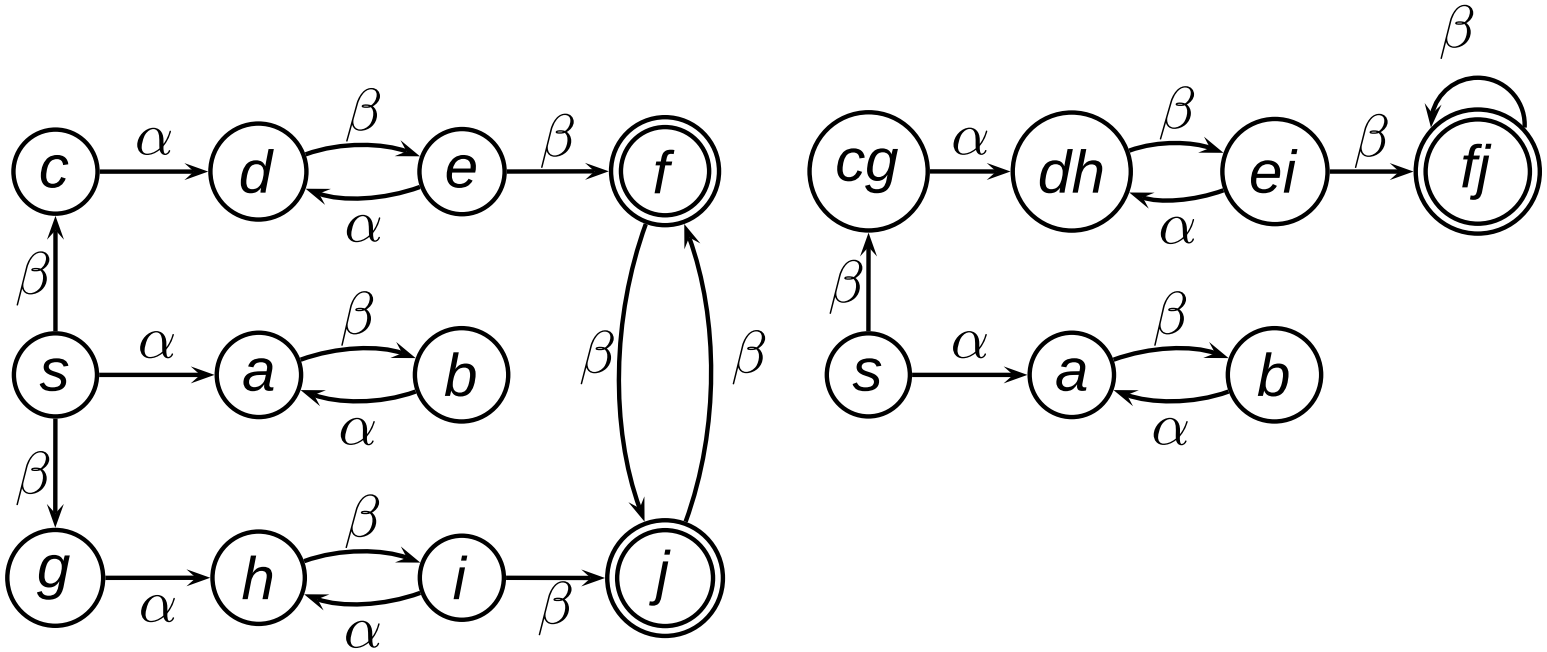


Ein kontrollierter Omegaautomat

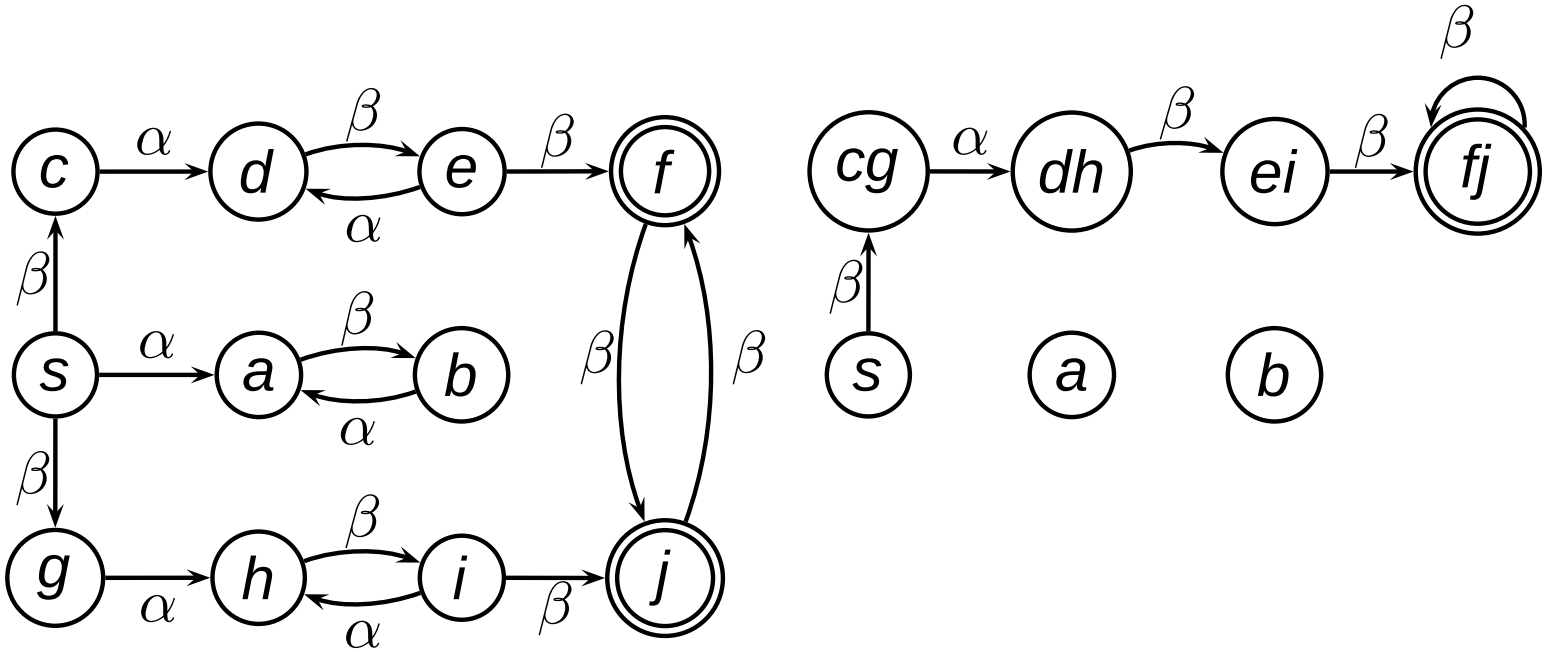


Erfüllt ◊F, □◊F und ◊□F, aber nicht □F.

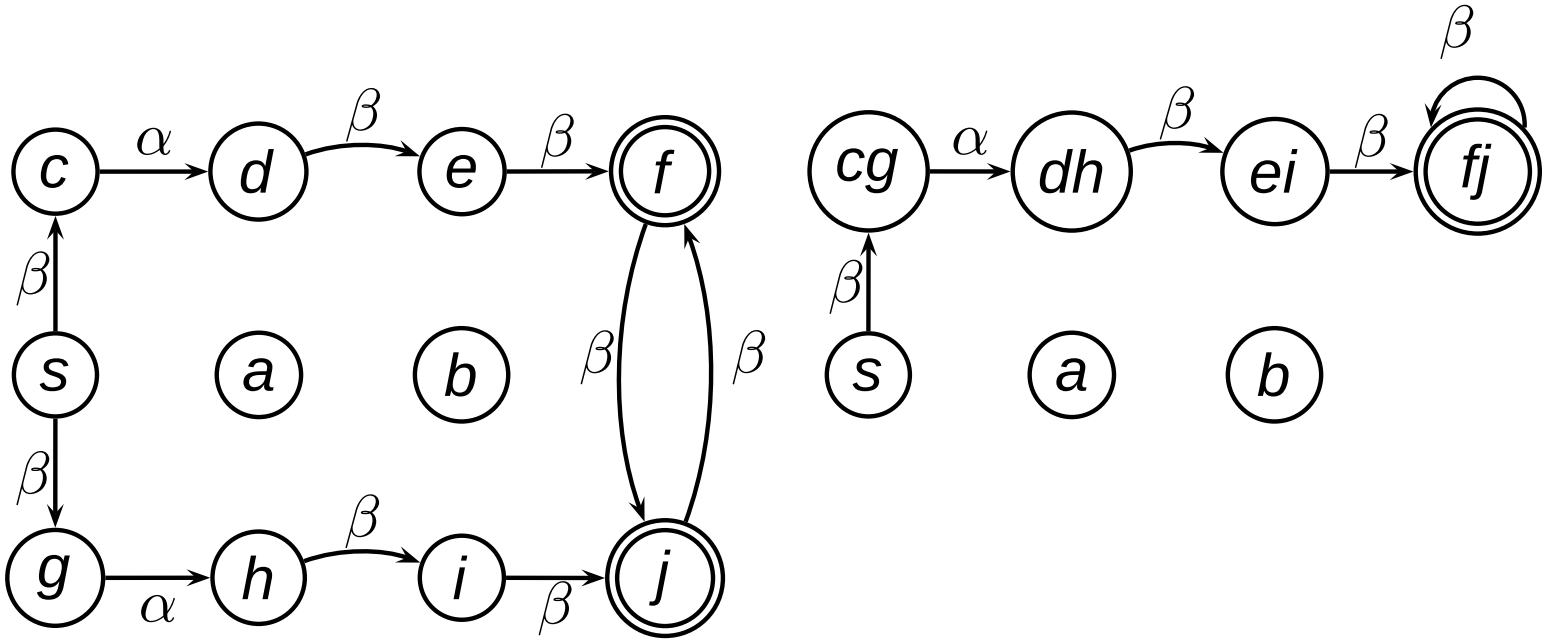
Kontrolle via Quotient (Quotientenbildung)



Kontrolle via Quotient (Quotientenkontrolle)



Kontrolle via Quotient (Expansion)



Zielmodelle

Verallgemeinerung des einführenden Beispiels durch:

- allgemeinere Kantenbeschriftung
- allgemeinere Optimalitätskriterien
- analoges Ziel: Optimale Wege in Zielgebiet

Stochastische Spiele

- zuerst untersucht von Shapley (1958)
- hier nur spezielle Form (einfache stochastische Spiele) behandelt
- als Entscheidungsproblem in $\mathbf{NP} \cap \mathbf{coNP}$
- kein polynomieller Algorithmus bekannt

Lineare Fixpunktgleichungen

- kantenbeschriftete Graphen induzieren Adjazenzmatrizen
- Optimalitätsprobleme als Fixpunktgleichungen $x = Ax + b$ darstellbar
- Addition und Multiplikation aus Dioiden
- Beispiel: Bellmann-Gleichungen
- verwandt mit Problemstellung von Zielmodellen

algebraische Eigenschaften von Relationen

Menge der Relationen $\mathrm{Rel}(M)$ über M hat folgende Eigenschaften:

- $R \cup S = S \cup R$
- $(R \cup S) \cup T = R \cup (S \cup T)$
- $R \cup R = R = R \cup \emptyset$
- $(R; S); T = R; (S; T)$
- $R; \emptyset = \emptyset = \emptyset; R$
- $R; \mathrm{Id}_M = R = \mathrm{Id}_M; R$
- $R; (S \cup T) = R; S \cup R; T$ und $(R \cup S); T = R; T \cup S; T$

Definition idempotenter Halbring

Definition

Ein *idempotenter Halbring* ist eine Struktur $(S, +, 0, \cdot, 1)$ mit $0, 1 \in S$ und $+, \cdot : S \times S \to S$ mit folgenden Eigenschaften:

- $x + x = x$
- $x + y = y + x$
- $(x + y) + z = x + (y + z)$
- $x + 0 = x$
- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $x \cdot 1 = x = 1 \cdot x$
- $x \cdot 0 = 0 = 0 \cdot x$
- $x \cdot (y + z) = x \cdot y + x \cdot z$ und $(x + y) \cdot z = x \cdot z + y \cdot z$

Relationenhalbring

Relationen	idempotenter Halbring
$R \cup R = R$	$x + x = x$
$R \cup S = S \cup R$	$x + y = y + x$
$(R \cup S) \cup T = R \cup (S \cup T)$	$(x + y) + z = x + (y + z)$
$R \cup \emptyset = R$	$x + 0 = x$
$(R; S); T = R; (S; T)$	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
$R; \emptyset = \emptyset = \emptyset; R$	$x \cdot 0 = 0 = 0 \cdot x$
$R; \mathrm{Id}_M = R = \mathrm{Id}_M; R$	$x \cdot 1 = x = 1 \cdot x$
$R; (S \cup T) = R; S \cup R; T$	$x \cdot (y + z) = x \cdot y + y \cdot z$
$(R \cup S); T = R; T \cup S; T$	$(x + y) \cdot z = x \cdot z + y \cdot z$

idempotente Halbringe (Fortsetzung)

- $x \sqsubseteq y :\Leftrightarrow x + y = y$ definiert *natürliche Ordnung* (Teilmengenbeziehung im Relationenhalbring)
- *Tests* zur Charakterisierung von Teilmengen (entsprechen Subrelationen von Id_M)
- atomare (minimale nicht-Null) Tests modellieren Elemente
- $|a\rangle p$ und $\langle a|p$ entsprechen (Ur)bild von p unter a
- Konversenbildung modellierbar durch $|a^{\smile}\rangle = \langle a|$

Bisimulationen in Halbringen

Rückblende:

$$v_1 \xrightarrow{\ell}_{E_1} w_1 \wedge v_1 B v_2 \Rightarrow \exists w_2 : v_2 \xrightarrow{\ell}_{E_2} w_2 \wedge w_1 B w_2$$

Bisimulationen in Halbringen

Rückblende:

$$v_1 \xrightarrow{\ell}_{E_1} w_1 \wedge v_1 B v_2 \Rightarrow \exists w_2 : v_2 \xrightarrow{\ell}_{E_2} w_2 \wedge w_1 B w_2$$

als Autobisimulation für ungelabelte Systeme:

$$v_1 R w_1 \wedge v_1 B v_2 \Rightarrow \exists w_2 : v_2 R w_2 \wedge w_1 B w_2$$

Bisimulationen in Halbringen

Rückblende:

$$v_1 \xrightarrow{\ell}_{E_1} w_1 \wedge v_1 B v_2 \Rightarrow \exists w_2 : v_2 \xrightarrow{\ell}_{E_2} w_2 \wedge w_1 B w_2$$

als Autobisimulation für ungelabelte Systeme:

$$v_1 R w_1 \wedge v_1 B v_2 \Rightarrow \exists w_2 : v_2 R w_2 \wedge w_1 B w_2$$

wird relationenalgebraisch zu:

$$R^{\smile}; B \subseteq B; R^{\smile}$$

Bisimulationen in Halbringen

Rückblende:

$$v_1 \xrightarrow{\ell}_{E_1} w_1 \wedge v_1 B v_2 \Rightarrow \exists w_2 : v_2 \xrightarrow{\ell}_{E_2} w_2 \wedge w_1 B w_2$$

als Autobisimulation für ungelabelte Systeme:

$$v_1 R w_1 \wedge v_1 B v_2 \Rightarrow \exists w_2 : v_2 R w_2 \wedge w_1 B w_2$$

wird relationenalgebraisch zu:

$$R^{\smile}; B \subseteq B; R^{\smile}$$

in Halbringschreibweise:

$$\langle g || b \rangle \sqsubseteq |b\rangle\langle g|$$

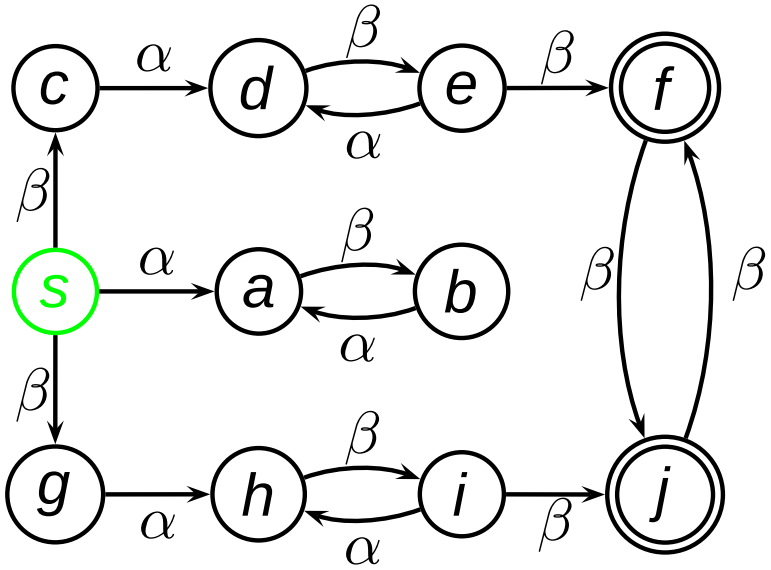
Warum Algebra?

Algebraischer Ansatz bietet

- mathematische Schönheit
- Formulierung in Prädikatenlogik erster Stufe
- Möglichkeit des Einsatzes von Theorembeweisern (hier Prover9)
- automatisches/interaktives Beweisen

Was nun?

- Implementierung
- Praxistest
- Anwendbarkeitskriterium/en
- weitere offene theoretische Fragen


c
d
e
f
s
a
b
g
h
i
j
α
β