Polynomial Time Algrotihms for Testing Probabilistic Bisimulation and Simulation

Presenteret af Robert Jørgensgaard Engdahl

Christel Baier

Den 2. November 2007

Artiklen i store træk

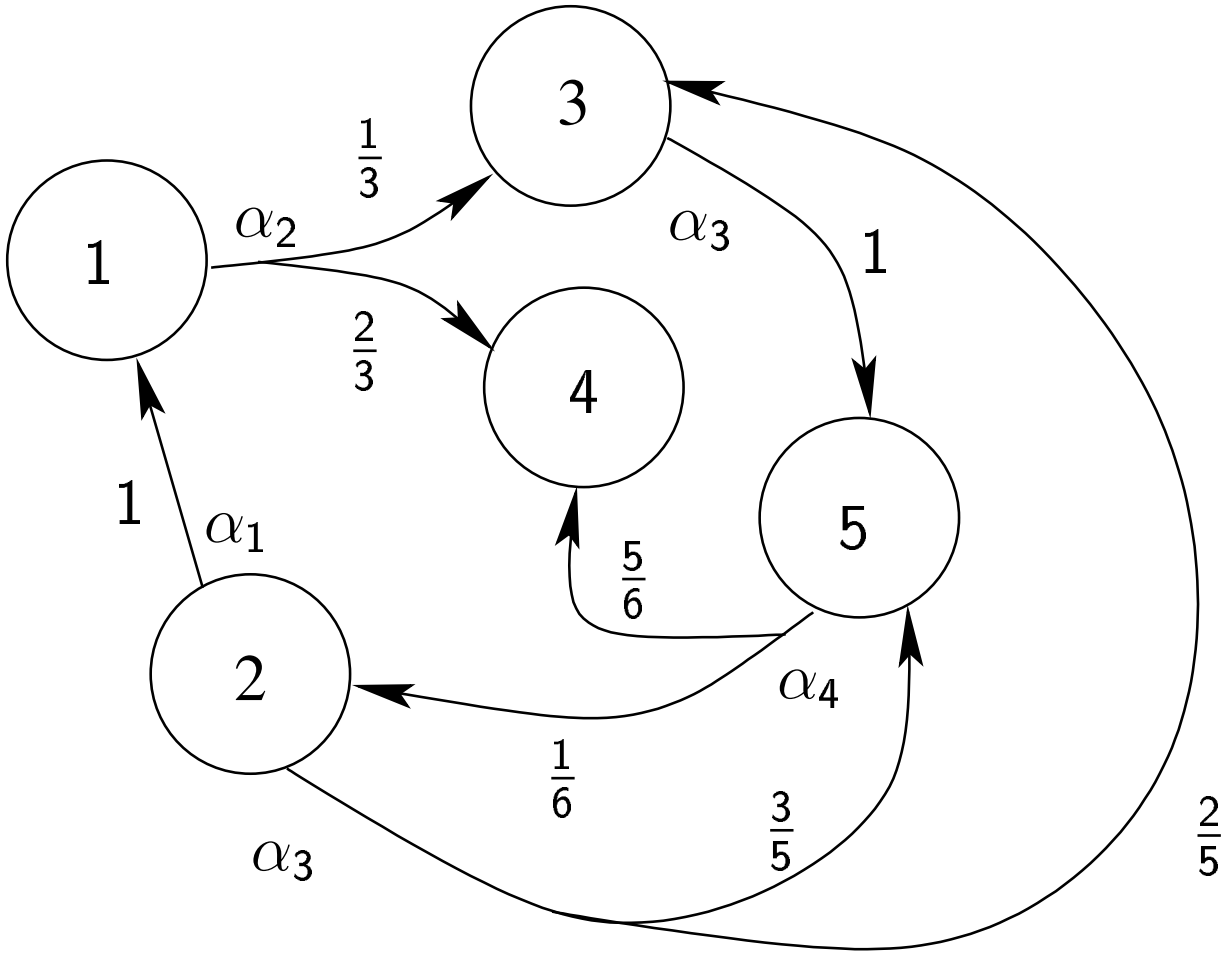
- Vi beskæftiger os med simularitet og bisimularitet for probabilistiske overgangssystemer.
- Gennemstrømnings-maksimeringsproblemet har en kendt løsning, som vi bruger til at konstruere en $\mathcal{O}(n^7 m^2)$-fikspunktsalgoritme for test af (bi)simularitet.
- Bisimularitet kan vi dog også beregne med en $\mathcal{O}(n^2 m)$-fikspunktsalgoritme.

Program

1. Grundlæggende definitioner
   - Probabilistisk overgangssystem
   - Bisimulering
   - Simulering
2. (Bi)simularitetstest
   - Invariant for (bi)simularitetstestsalgoritme
   - Gennemstrømnings-maksimeringsproblemet
   - Simularitetstestsalgoritmen
3. Hurtigere bisimularitetstest
   - Partitioneringsfunktionen $\mathcal{J}$
   - Den hurtige bisimularitetstestalgoritme

Næste afsnit

Eksempel - et probabilistisk overgangssystem



Probabilistisk overgangssystem

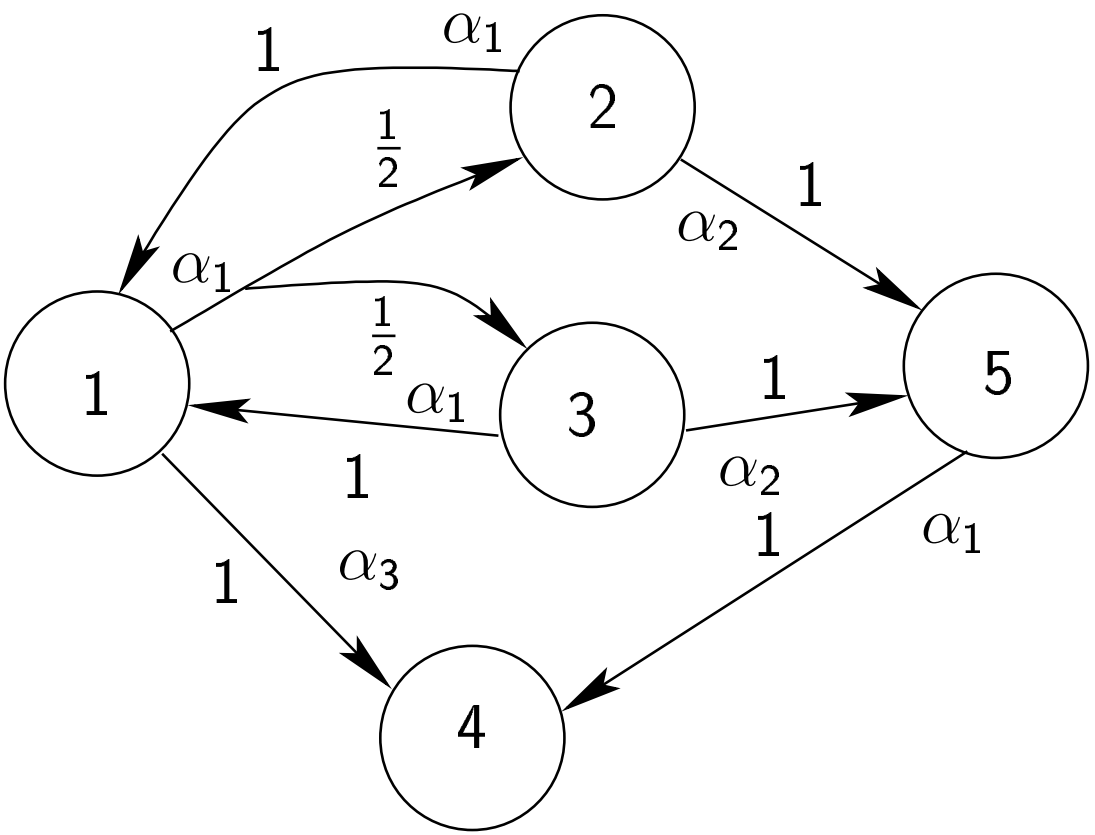
Definition

Et probabilistisk overgangssystem er et par $\mathcal{S} = (S, \rightarrow)$, hvor

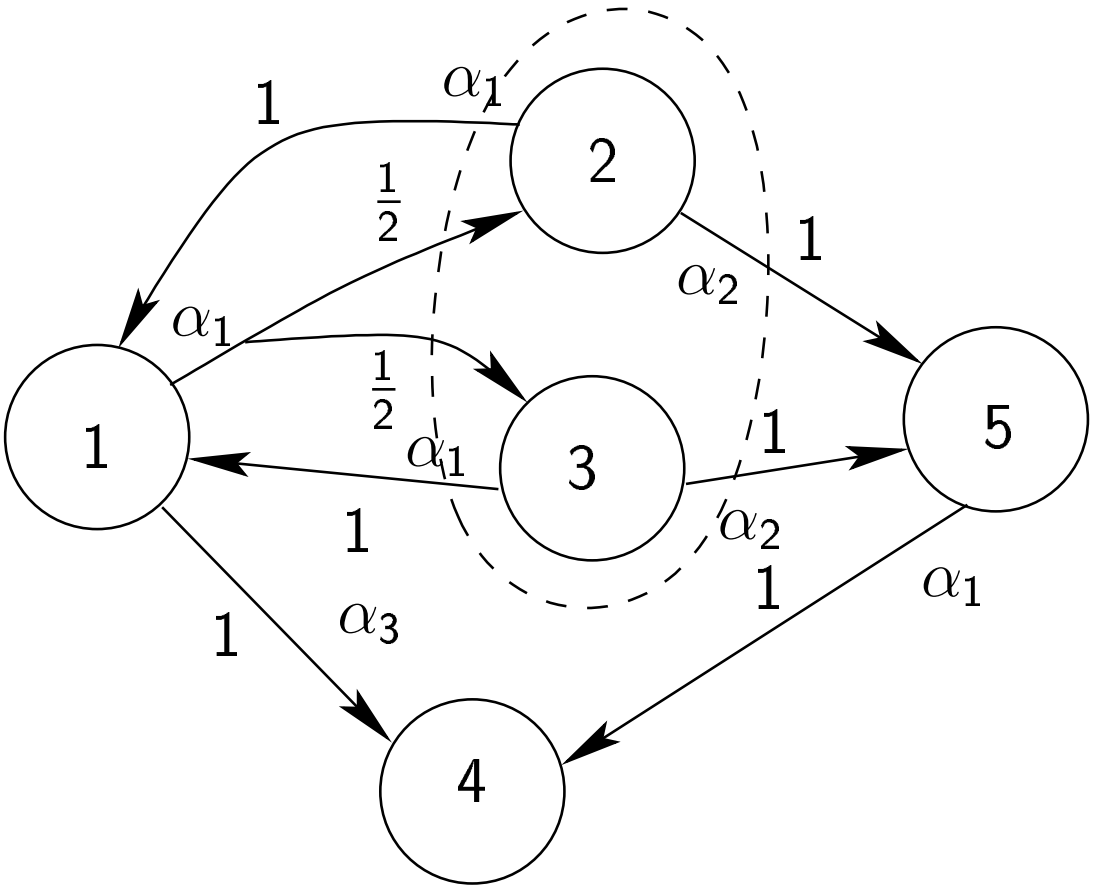
- S er en endelig mængde af tilstande, og
- $\rightarrow \subseteq S \times Act \times \mathcal{D}(S)$ er en endelig probabilistisk overgangsrelation, hvor Act er en mængde af *actions* og $\mathcal{D}(S)$ er mængden af sandsynlighedsfordelinger på S.

$s \xrightarrow{\alpha} \mu$ bruges som notation for $(s, \alpha, \mu) \in \rightarrow$

Eksempel - et probabilistisk overgangssystem



Eksempel - . . . med bisimulære tilstande



Bisimulering

Definition

Lad $(S, \rightarrow)$ være et probabilistisk overgangssystem. En bisimulering på S er en ækvivalensrelation R på S, således at for alle $(s, s') \in R$ gælder det at $s \xrightarrow{\alpha} \mu$ medfører $s' \xrightarrow{\alpha} \mu'$, hvor $\mu(A) = \mu'(A)$ for alle $A \in S/R$.

S/R er mængden af ækvivalensklasser (Kvotienten) af S m.h.t. R

Definition

To tilstande s og s' kaldes bisimulære ($s \sim s'$), hvis der findes en bisimulering indeholdende (s, s').

Vægtfunktion

Definition

Lad S være en endelig mængde af tilstande, $R \subseteq S \times S$ og $\mu, \mu' \in \mathcal{D}(S)$. En *vægtfunktion* for (μ, μ') m.h.t. R er en funktion $\delta : S \times S \to [0, 1]$ der opfylder:

1. For alle $s, s' \in S$ er marginalerne af δ netop μ og μ', d.v.s.:

$$\sum_{s' \in S} \delta(s, s') = \mu(s) \text{ og } \sum_{s \in S} \delta(s, s') = \mu'(s')$$

2. Hvis $\delta(s, s') > 0$ så $(s, s') \in R$.

Alternativ definition af bisimulering

Sætning

Lad $(S, \rightarrow)$ være et probabilistisk overgangssystem og R være en ækvivalensrelation på S. R er en bisimulering hvis det for alle $(s, s') \in R$ gælder at $s \xrightarrow{\alpha} \mu$ medfører at der findes en overgang $s' \xrightarrow{\alpha} \mu'$ og en vægtfunktion for (μ, μ') m.h.t. R.

Bevis.

$$\begin{aligned}\mu'(A) &= \sum_{s' \in A} \mu'(s) = \sum_{s \in S} \sum_{s' \in A} \delta(s, s') = \sum_{s \in A} \sum_{s' \in A} \delta(s, s') \\ &= \sum_{s \in A} \sum_{s' \in S} \delta(s, s') = \sum_{s \in A} \mu(s) = \mu(A)\end{aligned}$$

□

Simulering

Definition

Lad $(S, \rightarrow)$ være et probabilistisk overgangssystem. En simulering for $(S, \rightarrow)$ er en delmængde R af $S \times S$ således, at for alle $(s, s') \in R$ gælder, at $s \xrightarrow{\alpha} \mu$ medfører, at der findes en overgang $s' \xrightarrow{\alpha} \mu'$ og en vægtfunktion δ for (μ, μ') m.h.t. R.

Definition

s implementerer s' ($s \sqsubseteq s'$) hvis der findes en simulering indeholdende (s, s').

Næste afsnit

Hjælpedefintioner

Definition

Lad $(S, \rightarrow)$ være et probabilistisk overgangssystem. Ækvivalensrelationen endelig bisimulering $\sim_n$ defineres rekursivt som:

$\sim_0$: $\sim_0 = S \times S$.

$\sim_{n+1}$: $s \sim_{n+1} s'$, hvis $s \xrightarrow{\alpha} \mu$ medfører at der findes en overgang $s' \xrightarrow{\alpha} \mu'$ hvor $\mu(A) = \mu'(A)$ for alle $A \in S/\sim_n$, og omvendt.

Endelig simulering $\sqsubseteq_n$ defineres rekursivt som:

$\sqsubseteq_0$: $\sqsubseteq_0 = S \times S$.

$\sqsubseteq_{n+1}$: $s \sqsubseteq_{n+1} s'$, hvis $s \xrightarrow{\alpha} \mu$ medfører at der findes en overgang $s' \xrightarrow{\alpha} \mu'$ og en vægtfunktion δ for μ, μ' m.h.t. $\sqsubseteq_n$.

Grænserne for endelig (bi)simulering

Lemma (Lemma 5)

Lad $(S, \rightarrow)$ være et probabilistisk overgangssystem og $s, s' \in S$. Da gælder det, at

1. *$s \sqsubseteq s'$, hvis og kun hvis $s \sqsubseteq_n s'$ for alle $n \geq 0$.*
2. *$s \sim s'$, hvis og kun hvis $s \sim_n s'$ for alle $n \geq 0$.*

Bemærk, at vi har ruserne

$$\sqsubseteq_0 \supseteq \sqsubseteq_1 \supseteq \ldots \text{ og } \sim_0 \supseteq \sim_1 \supseteq \ldots,$$

hvoraf det følger, at

$$\lim_{n\to\infty} \sqsubseteq_n = \sqsubseteq \text{ og } \lim_{n\to\infty} \sim_n = \sim.$$

Polynomiel konvergens

Lemma (Lemma 6)

Lad $(S, \rightarrow)$ være et probabilistisk overgangssystem, n være antallet af tilstande i S og $N = n^2$. Det gælder da, at $\sim = \sim_N$ og $\sqsubseteq = \sqsubseteq_N$.

Bevis.

Ad $\sqsubseteq = \sqsubseteq_N$: *Da $\sqsubseteq_0 = S \times S$ indeholder N elementer findes der et $j < N$ der opfylder at $\sqsubseteq_{j+1} = \sqsubseteq_j$. $\sqsubseteq_j$ er således et fikspunkt da $\sqsubseteq_n$ er defineret rekursivt (d.v.s $\sqsubseteq_j = \sqsubseteq_i$ for alle $i \geq j$, særligt for $i = N$).*

Ad $\sim = \sim_N$: *Da $\sim_0 = S \times S$ indeholder N elementer findes der et $j < N$ der opfylder at $\sim_{j+1} = \sim_j$. $\sim_j$ er således et fikspunkt da $\sim_n$ er defineret rekursivt (d.v.s $\sim_j = \sim_i$ for alle $i \geq j$, særligt for $i = N$).*

□

Netværk

Definition

Et netværk er en tuppel $\mathcal{N} = (N, E, \bot, \top, c)$, hvor

- (N, E) er en endelig orienteret graf; N mængden af knuder og $E \subseteq N \times N$ mængden af kanter.
- $\bot, \top \in N$ kaldes, henholdsvis, kilde og dræn.
- $c : E \to \mathbf{R}^+$ er en kapacitetsfunktion der beskriver den maksimalt tilladte gennemstrømning gennem en kant.

Gennemstrømningsfunktion for et netværk

Definition

Lad $f : E \to \mathbf{R}$. f kaldes en gennemstrømningsfunktion hvis

1. $0 \leq f(e) \leq c(e)$ for alle kanter $e \in E$.
2. (Kirchhoffs første lov:) Lad $in(v)$ være mængden af indgående kanter til knuden v og $out(v)$ være mængden af udgående. For hver knude $v \in N$ skal det gælde, at

$$\sum_{e \in in(v)} f(e) = \sum_{e \in out(v)} f(e).$$

Vi definerer gennemstrømningen $\mathcal{F}(f)$ for f som

$$\mathcal{F}(f) = \sum_{e \in out(\perp)} f(e) - \sum_{e \in in(\perp)} f(e).$$

Konstruktion af netværk

Definition

Givet en endelig mængde S, $R \subseteq S \times S$ og $\mu, \mu' \in \mathcal{D}(S)$. Lad $S' = \{t' \mid t \in S\}$ $(t' \notin S)$. Lad $\bot \neq \top \notin S \cup S'$. Lad $N = S \cup S' \cup \{\bot\} \cup \{\top\}$. Lad

$$E = \{(s, t') \mid (s, t) \in R\} \cup \{(\bot, s) \mid s \in S\} \cup \{(t', \top) \mid t' \in S'\},$$

og endelig, lad $c(\bot, s) = \mu(s)$, $c(t', \top) = \mu'(t)$ og $c(s, t') = 1$. *Netværket* $\mathcal{N}(\mu, \mu', R)$ defineres nu som $\mathcal{N}(\mu, \mu', R) = (N, E, \bot, \top, c)$.

Hvad skal vi med netværk (1/2)?

Lemma (Lemma 7)

Der findes en vægtfunktion δ for (μ, μ') m.h.t. R hvis og kun hvis den maximale gennemstrømning i $\mathcal{N}(\mu, \mu', R)$ er 1.

Bevis.

Ad maksimum: Antag, at der findes en vægtfunktion δ for (μ, μ') m.h.t. R. Gennemstrømningen i $\mathcal{N}(\mu, \mu', R)$ er opadtil begrænset af 1 da

$$\mathcal{F}(f) = \sum_{s \in S} f(\bot, s) \leq \sum_{s \in S} c(\bot, s) = \sum_{s \in S} \mu(s) = 1,$$

for alle f. Vælg nu f således at $f(\bot, s) = \mu(s)$, $f(t', \top) = \mu'(t)$, $f(s, t') = \delta(s, t)$. Da μ er en sandsynlighedsfordeling og $in(\bot) = \emptyset$ haves $\mathcal{F}(f) = 1$, hvilket er optimalt, som skulle vises. □

Hvad skal vi med netværk (2/2)?

Lemma (Lemma 7)

Der findes en vægtfunktion δ for (μ, μ') m.h.t. R hvis og kun hvis den maximale gennemstrømning i $\mathcal{N}(\mu, \mu', R)$ er 1.

Bevis.

Ad eksistens: Lad f være en gennemstrømningsfunktion med $\mathcal{F}(f) = 1$. Lad $\delta(s,t) = f(s,t')$ for $(s,t) \in R$ og $\delta(s,t) = 0$ ellers.

$$\sum_{t \in S} \delta(s,t) = \sum_{t \in S} f(s,t') = f(\bot, s) = \mu(s), \text{ da}$$

$$\left.\begin{array}{r} f(\bot,s) \leq c(\bot,s) = \mu(s) \\ \sum_{s \in S} f(\bot,s) = \mathcal{F}(f) = 1 = \sum_{s \in S} \mu(s) \end{array}\right\} \Rightarrow \begin{array}{l} f(\bot,s) = \mu(s) \\ \text{for alle } s \in S. \end{array}$$

Samme fremgangsmåde for μ'. □

Bemærk konstruktivt bevis!

Bevis.

Ad eksistens: Lad f være en gennemstrømningsfunktion med $\mathcal{F}(f) = 1$. Lad $\delta(s,t) = f(s,t')$ for $(s,t) \in R$ og $\delta(s,t) = 0$ ellers.

$$\sum_{t \in S} \delta(s,t) = \sum_{t \in S} f(s,t') = f(\bot, s) = \mu(s), \text{ da}$$

$$\left.\begin{array}{r} f(\bot,s) \leq c(\bot,s) = \mu(s) \\ \sum_{s \in S} f(\bot,s) = \mathcal{F}(f) = 1 = \sum_{s \in S} \mu(s) \end{array}\right\} \Rightarrow \begin{array}{l} f(\bot,s) = \mu(s) \\ \text{for alle } s \in S. \end{array}$$

Samme fremgangsmåde for μ'. □

Kompleksitet og beregnlighed for gennemstrømnings-maksimeringsproblemet

V. Malhotra, M. Pramodh Kumar and S. Maheshwari beskriver i "An $\mathcal{O}(|V|^3)$ Algorithm for Finding Maximum Flows in Networks" hvordan gennemstrømnings-maksimeringsproblemet kan løses i $\mathcal{O}(n^3)$ tid.

Algoritme 1 (Eksistens af vægtfunktion

Inddata: En endelig mængde S, fordelinger $\mu, \mu' \in \mathcal{D}(S)$ og $R \subseteq S \times S$.

Uddata: En vægtfunktion δ for (μ, mu') m.h.t. R eller "Nej".

Metode: Løs gennemstrømnings-maksimeringsproblemet for $\mathcal{N}(\mu, \mu', R)$ og få herved gennemstrømningen F og gennemstrømningsfunktionen f. Hvis $F < 1$ returneres "Nej", ellers returneres δ som konstrueret i Lemma 7.

Tidskompleksitet: $\mathcal{O}(n^3)$.

Algoritme 2 (Simularitetstest)

Inddata: Et probabilistisk overgangssystem $(S, \rightarrow)$.

Uddata: Den fuldstændige simuleringsrelation $R = \{(s,t) \in S \times S \mid s \sqsubseteq t\}$.

Metode: Lad $N = n^2$, $R_0 = S \times S$, hvor $n = |S|$.

- For $j = 1, \ldots, N$
  - $R_j := R_{j-1}$
  - For alle $(s,t) \in R_{j-1}$
    - For alle overgange $s \xrightarrow{\alpha} \mu$: Hvis ikke der findes en overgang $t \xrightarrow{\alpha} \mu'$, således at Algoritme 1 giver en vægtfunktion for (μ, μ') m.h.t. R_{j-1} så $R_j := R_j \backslash \{(s,t)\}$
- Returner $R := R_N$.

Tidskompleksitet: $\mathcal{O}(n^7 \cdot m^2)$, $m = |E|$ og $n = |S|$ ($\mathcal{O}(n^5 \cdot m^2)$ i artiklen?).

Algoritme 2 (Bisimularitetstest)

Inddata: Et probabilistisk overgangssystem $(S, \rightarrow)$.

Uddata: Den fuldstændige bisimuleringsækvivalensrelation $R = \{(s,t) \in S \times S \mid s \sim t\}$.

Metode: Lad $N = n^2$, $R_0 = S \times S$, hvor $n = |S|$.

- For $j = 1, \ldots, N$
  - $R_j := R_{j-1}$
  - For alle $(s,t) \in R_{j-1}$
    - For alle overgange $s \xrightarrow{\alpha} \mu$: Hvis ikke der findes en overgang $t \xrightarrow{\alpha} \mu'$, således at Algoritme 1 giver en vægtfunktion for (μ, μ') m.h.t. R_{j-1} så $R_j := R_j \backslash \{(s,t),(t,s)\}$
    - For alle overgange $t \xrightarrow{\alpha} \mu$: Hvis ikke der findes en overgang $s \xrightarrow{\alpha} \mu'$, således at Algoritme 1 giver en vægtfunktion for (μ, μ') m.h.t. R_{j-1} så $R_j := R_j \backslash \{(s,t),(t,s)\}$
- Returner $R := R_N$.

Næste afsnit

Partitioneringsfunktionen

Definition

En partitionering af et probabilistisk overgangssystem $(S, \rightarrow)$ er en mængde X af disjunkte delmængder af S, således at

1. $\bigcup_{B \in X} B = S$.
2. for alle $[s] \in S/\sim$ findes et $B \in X$ således at $[s] \subseteq B$.

Definition

Lad $X(s) = \{(\alpha, \mu(X)) \mid s \xrightarrow{\alpha} \mu\}$ (En slags ækvivalensovergangsrelation). Lad $\equiv_X$ være ækvivalensrelationen der opfylder $s \equiv_X s'$ hvis og kun hvis $X(s) = X(s')$. Definer nu $\mathcal{J}(X)$ som

$$\mathcal{J}(X) = \bigcup_{B \in X} B/\equiv_X .$$

$S/\sim$ er et fikspunkt for $\mathcal{J}$

$$\mathcal{J}(X) = \bigcup_{B \in X} B/\equiv_X .$$

Lemma

Lad $S, \rightarrow)$ være et probabilistisk overgangssystem og X en partitionering af $(S, \rightarrow)$.

1. *$S/\sim$ er en partition med $\mathcal{J}(S/\sim) = S/\sim$.*
2. *$\mathcal{J}(X)$ er en partitionering af $(S, \rightarrow)$.*
3. *$\mathcal{J}(X) = X$ medfører at $X = S/\sim$.*

Kompleksitivitet for $\mathcal{J}$ (1/2)

Lemma

Lad $(S, \rightarrow)$ være et probabilistisk overgangssystem med n tilstande og m overgange. Lad endvidere X være en partitionering af $(S, \rightarrow)$. Så gælder det at $\mathcal{J}(X)$ kan beregnes i $\mathcal{O}(n \cdot m)$ tid og $\mathcal{O}(n \cdot m)$ plads.

Kompleksitivitet for $\mathcal{J}$ (2/2)

Lemma

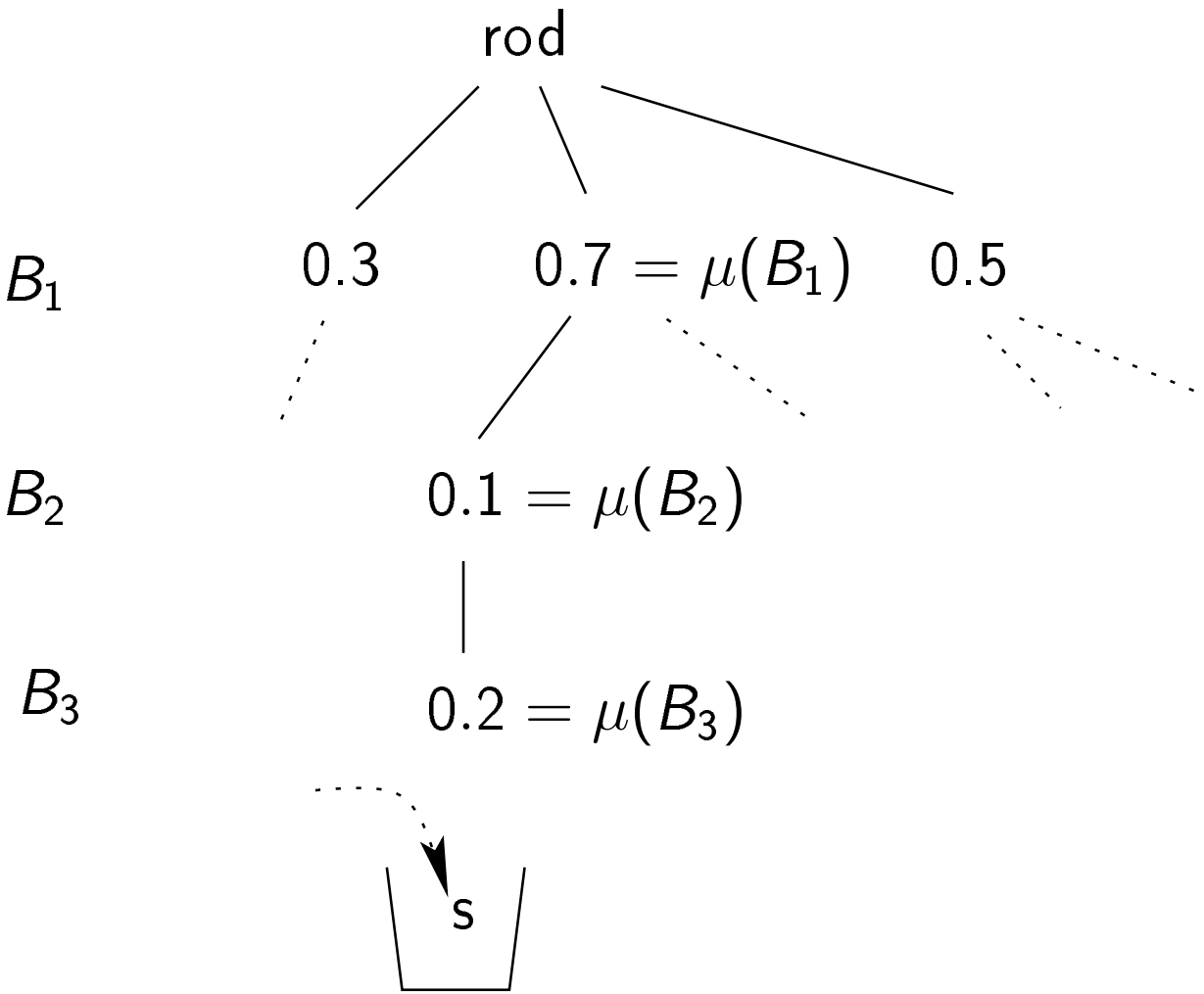
... at $\mathcal{J}(X)$ kan beregnes i $\mathcal{O}(n \cdot m)$ tid og $\mathcal{O}(n \cdot m)$ plads.

Bevis.

Givet $X = \{B_1, \ldots, B_l\}$. For hvert $\alpha \in Act$ og hvert $B \in X$, konstruer et træ $T_{B,\alpha}$ ved at køre alle $s \xrightarrow{\alpha} \mu$ igennem hash-funktionerne $h_k(s \xrightarrow{\alpha} \mu) = \mu(B_k)$ for $k = 1, \ldots, l$ og $s \in B$. Når overgangen $s \xrightarrow{\alpha}$ når til bladet v (d.v.s. dybde l), fyld da s i $L(v)$. For hver overgang $s \xrightarrow{\alpha} \mu$ skal μ beregnes på hver tilstand $s \in S$, deraf $\mathcal{O}(n \cdot m)$. ...
Et binært beslutningstræ T_B bruges nu til at fordele $s \in S$ i $B/\equiv_X$, for hvert B. Tidskompleksiteten er igen $\mathcal{O}(n \cdot m)$. □

Eksempel på $T_{B,\alpha}$-træ

Husk: $h_k(s \xrightarrow{\alpha} \mu) = \mu(B_k)$.



Algoritme 3

Inddata: Et probabilistisk overgangssystem $(S, \rightarrow)$.

Uddata: Mængden af bisimularitetsklasser $R = S/\sim$

Metode: Lad $X := \{S\}$.

- Gentag
  - $Y := X$
  - $X := \mathcal{S}(X)$

  indtil $X = Y$
- Returnér $R := X$.

Tidskompleksitet: $\mathcal{O}(n^2 \cdot m)$.

Pladskompleksitet: $\mathcal{O}(n \cdot m)$.

Artiklens bidrag

- Bisimularitet ($\sim$) kan beregnes i $\mathcal{O}(n^2 \cdot m)$ tid v.h.a. Algoritme 3.
- Simularitet ($\sqsubseteq$) kan beregnes i $\mathcal{O}(n^7 \cdot m^2)$ tid v.h.a. Algoritme 2.

. . . Slut!