Why Probability and Nondeterminism? Concurrency Theory

- Nondeterminism
  - Scheduling within parallel composition
  - Unknown behavior of the environment
  - Underspecification
- Probability
  - Environment may be stochastic
  - Processes may flip coins

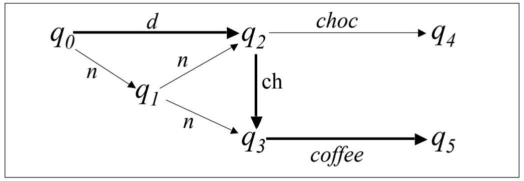
Automata

$A = (Q, q_0, E, H, D)$

- Transition relation $D \subseteq Q \times (E \cup H) \times Q$
- Internal (hidden) actions
- External actions: $E \cap H = \emptyset$
- Initial state: $q_0 \in Q$
- States

Example: Automata

$A = (Q, q_0, E, H, D)$



Execution: $q_0\ n\ q_1\ n\ q_2\ ch\ q_3\ coffee\ q_5$

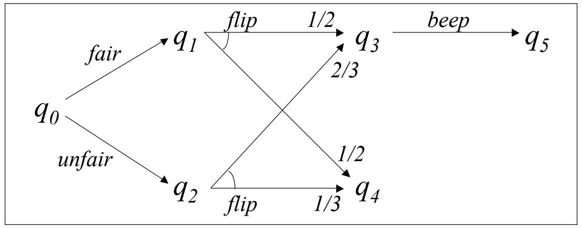
Trace: $n\ n\ coffee$

Probabilistic Automata

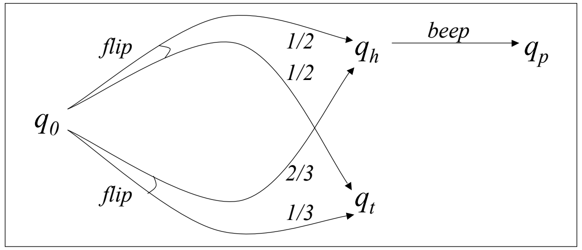
$PA = (Q, q_0, E, H, D)$

- Transition relation $D \subseteq Q \times (E \cup H) \times \mathrm{Disc}(Q)$
- Internal (hidden) actions
- External actions: $E \cap H = \emptyset$
- Initial state: $q_0 \in Q$
- States

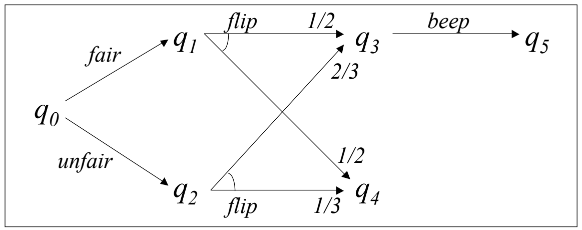
Example: Probabilistic Automata



Example: Probabilistic Automata

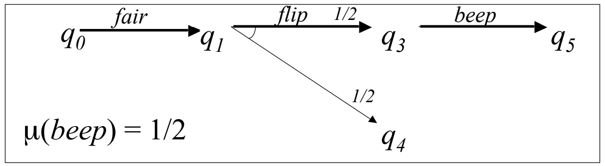


Example: Probabilistic Automata

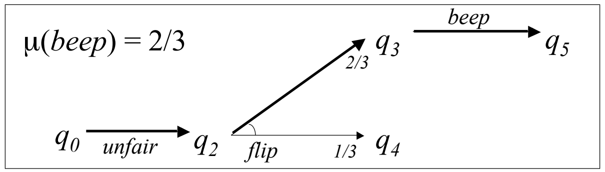


What is the probability of beeping?

Example: Probabilistic Executions

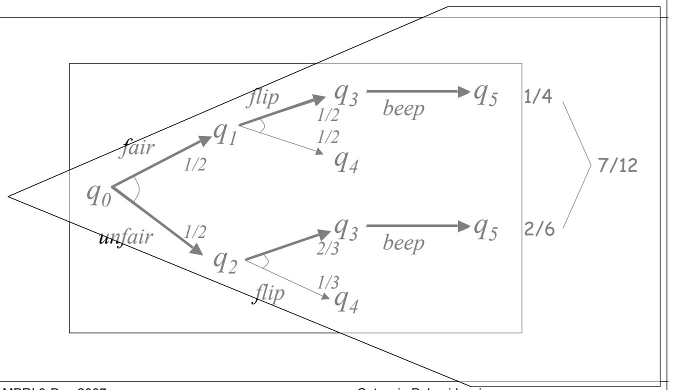


1/2



2/3

Example: Probabilistic Executions



Measure Theory

- Sample set
  - Set of objects Ω
- Sigma-field (σ-field)
  - Subset F of 2^Ω satisfying
    - Inclusion of Ω
    - Closure under complement
    - Closure under countable union
    - Closure under countable intersection
- Measure on (Ω, F)
  - Function μ from F to $\Re^{\geq 0}$
    - For each countable collection $\{X_i\}_I$ of pairwise disjoint sets of F, $\mu(\cup_I X_i) = \Sigma_I \mu(X_i)$
- (Sub-)probability measure
  - Measure μ such that $\mu(\Omega) = 1$ ($\mu(\Omega) \leq 1$)
- Sigma-field generated by $C \subseteq 2^\Omega$
  - Smallest σ-field that includes C

Example: set of executions

Study probabilities of sets of executions
which sets can I measure?

Measure Theory

Why not $F = 2^\Omega$?

Flip a fair coin infinitely many times

$\Omega = \{h,t\}^\infty$

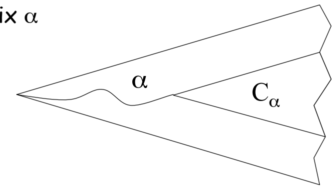
$\mu(\omega) = 0$ for each $\omega \in \Omega$

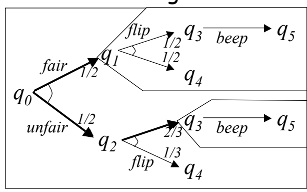
$\mu(\text{first coin } h) = 1/2$

Theorem: there is no probability measure on 2^Ω such that $\mu(\omega) = 0$ for each $\omega \in \Omega$.

Cones and Measures

- Cone of α
  - Set of executions with prefix α
  - Represent event "α occurs"
- Measure of a cone
  - Product edges of α





...xtends uniquely
...-field generated by cones

Examples of Events

- Eventually action a <u>occurs</u>
  - Union of cones where action a occurs once
- Action a <u>occurs at least</u> n times
  - Union of cones where action a occurs n times
- Action a <u>occurs at most</u> n times
  - Complement of action a occurs at least n+1 times
- Action a <u>occurs exactly</u> n times
  - Intersection of previous two events
- Action a <u>occurs infinitely</u> many times
  - Intersection of action a occurs at least n times for all n
- Execution α occurs and <u>nothing is scheduled after</u>
  - Set consisting of α only
  - C_α intersected complement of cones that extend α

Schedulers - Resolution of nondeterminism

<u>Scheduler</u>

Function $\sigma : exec^*(A) \rightarrow Q \times (E \cup H) \times Disc(Q)$

if $\sigma(\alpha) = (q,a,\nu)$ then $q = lstate(\alpha)$

<u>Probabilistic execution</u> generated by σ from state r

Measure $\mu_{\sigma,r}$

$\mu_{\sigma,r}(C_s) = 0$ if $r \neq s$

$\mu_{\sigma,r}(C_r) = 1$

$\mu_{\sigma,r}(C_{\alpha a q}) = \mu_{\sigma,r}(C_\alpha) \bullet \nu(q)$ if $\sigma(\alpha) = (q,a,\nu)$

Probabilistic CCS

$$P ::= 0 \mid P|P \mid \alpha.P \mid P+P \mid (\upsilon\alpha)P \mid X \mid \text{let } X = P \text{ in } X \mid P \oplus_p P$$

Prefix

$$\frac{}{\alpha.P \xrightarrow{\alpha} \delta(P)}$$

Nondeterministic process

$$\frac{P \xrightarrow{\alpha} \mu}{P + Q \xrightarrow{\alpha} \mu}$$

Probabilistic processes

$$\frac{}{P_1 \oplus_p P_2 \xrightarrow{\tau} p\mu_1 + (1-p)\mu_2}$$

Probabilistic CCS

Interleaving

$$\frac{P \xrightarrow{\alpha} \mu}{P|Q \xrightarrow{\alpha} \mu|Q}$$

Hiding

$$\frac{P \xrightarrow{\alpha} \mu}{(\nu a)\, P \xrightarrow{\tau} (\nu a)\, \mu} \quad \alpha \neq a, \hat{a}$$

Communication

$$\frac{P_1 \xrightarrow{a} \delta(P'_2) \qquad P_2 \xrightarrow{\hat{a}} \delta(P'_2)}{P_1 | P_2 \xrightarrow{\tau} \delta(P'_2 | P'_2)}$$

Recursion

$$\frac{P[\text{ let } X = P \text{ in } X / X\,] \xrightarrow{\alpha} \mu}{\text{let } X = P \text{ in } X \xrightarrow{\alpha} \mu}$$

Bisimulation Relations

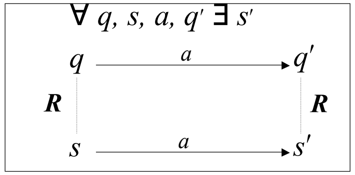
We have the following objectives

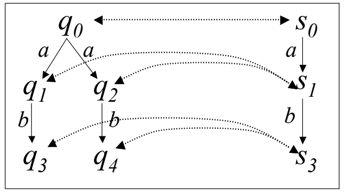
- They should extend the corresponding relations in the non probabilistic case
- Keep definitions simple
- Where are the key differences?

Strong Bisimulation on Automata

Strong bisimulation between A_1 and A_2

Relation $\boldsymbol{R} \subseteq Q \times Q$, $Q = Q_1 \cup Q_2$, such that

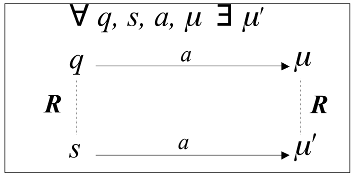


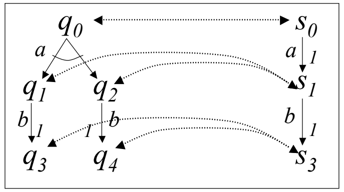


Strong Bisimulation on Probabilistic Automata

Strong bisimulation between A_1 and A_2

Relation $\boldsymbol{R} \subseteq Q \times Q$, $Q = Q_1 \cup Q_2$, such that





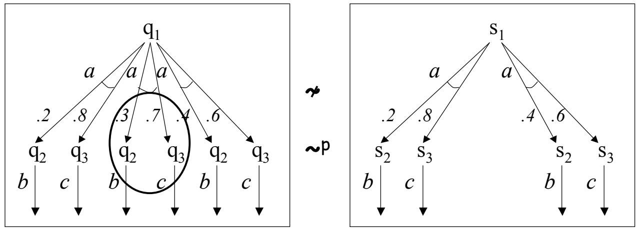
$\mu \, \boldsymbol{R} \, \mu'$ [LS89]

$$\Leftrightarrow$$

$$\forall C \in Q/\boldsymbol{R} \, . \; \mu(C) = \mu'(C)$$

Probabilistic Bisimulations

- These two Probabilistic Automata are not bisimilar



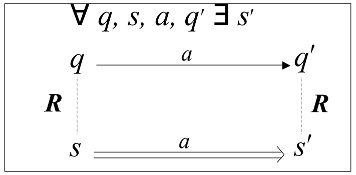
- Yet they satisfy the same formulas of a logic PCTL
  - The logic observes probability bounds on reachability properties
- Bisimilar if we match transitions with convex combinations of transitions

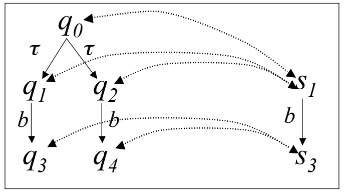
Weak Bisimulation on Automata

Weak bisimulation between A_1 and A_2

Relation $\boldsymbol{R} \subseteq Q \times Q$,

$Q = Q_1 \cup Q_2$, such that





$s \xRightarrow{a} s'$

$\Leftrightarrow$

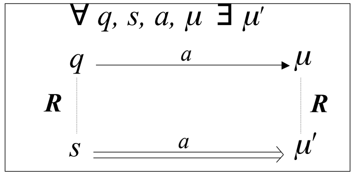
$\exists \alpha$: $trace(\alpha)=a$, $fstate(\alpha)=s$, $lstate(\alpha)=s'$

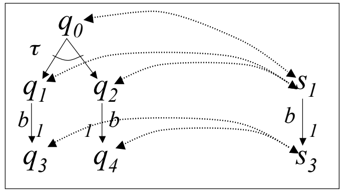
Weak bisimulation on Probabilistic Automata

Weak bisimulation between A_1 and A_2

Relation $\boldsymbol{R} \subseteq Q \times Q$,

$Q = Q_1 \cup Q_2$, such that





$\mu \, \boldsymbol{R} \, \mu'$ [LS89]

$\Leftrightarrow$

$\forall C \in Q/\boldsymbol{R} \,.\, \mu(C) = \mu'(C)$

Weak Transition

$$q \xRightarrow{a} \rho$$

There is a probabilistic execution μ such that

- $\mu(exec^*) = 1$ (it is finite)
- $trace(\mu) = \delta(a)$ (its trace is a)
- $fstate(\mu) = \delta(q)$ (it starts from q)
- $lstate(\mu) = \rho$ (it leads to ρ)

$q \xRightarrow{a} s$ iff $\exists \alpha$: $trace(\alpha)=a$, $fstate(\alpha)=q$, $lstate(\alpha)=s$

Exercises

- Prove that the probabilistic CCS is an extension of CCS (to define what this means is part of the exercise)
- Prove that probabilistic bisimulation is an extension of bisimulation
- Write the Lehmann-Rabin algorithm in probabilistic CCS (without using guarded choice)