MPRI C.2.3 - Concurrency

Probabilistic models and applications
Lecture 2

Kostas Chatzikokolakis

Dec 20, 2012

Outline of the lectures

- Dec 13
- Dec 20
- Jan 10 *
- Jan 17 *
- Jan 24 *

* not guaranteed

What would you talk about if the world was going to end tomorrow?

- The need for randomization
- Probabilistic automata
- Probabilistic bisimulation
- Probabilistic calculi
- Encoding of the pi-calculus into the asynchronous fragment
- Introduction to probabilistic model checking and PRISM
- Verification of anonymity protocols: Dining Cryptographers, Crowds

Exercises from the last lecture

Exercise 1: The algorithm of Lehmann and Rabin assumes a fair scheduler.

- Why?
- Is it possible to have a probabilistic solution to the dininig philosophers problem that does not depend on scheduler fairness?

Exercises from the last lecture

Exercise 2: Give a solution of the dining philosophers problem (satisfying all constraints) in the π-calculus (or CCS). Hint: use mixed choice

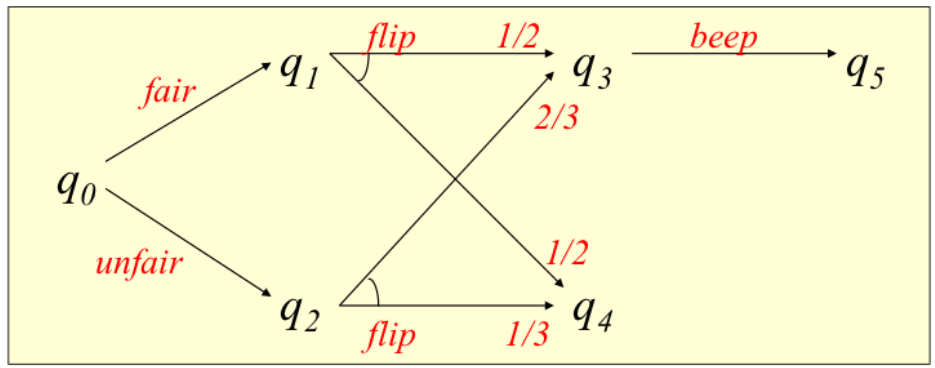
And a probabilistic puzzle

- I select two real numbers in some arbitrary way
- I put them in two envelopes, you select one of them (in any way you want)
- You see the number and you have 2 options: keep it, or exchange it with the other envelope
- Your goal is to select the bigger number
- Is there any strategy that guarantees winning this game with pb higher than 1/2?

Probabilistic automata

$A = (S, q, A, D)$

- S: set of states (countable)
- $q \in S$: initial state (or distribution on states)
- A: set of actions
- $D \subseteq S \times A \times Disc(S)$: transition relation
- we write $s \xrightarrow{a} \mu$ for $(s, a, \mu) \in D$



Probability space of executions

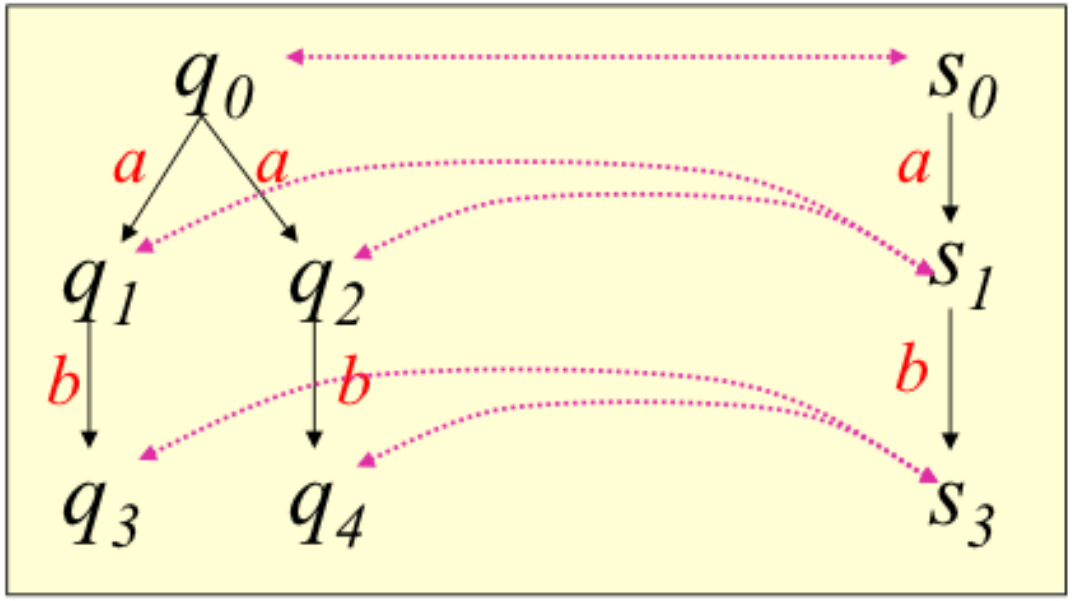
- Execution: $\alpha = s_0 a_1 s_1 a_2 s_2 \ldots$
  such that for each i: $s_i \xrightarrow{a_{i+1}} \mu_i$ and $\mu_i(s_{i+1}) > 0$
- $exec^*(A)$, $exec(A)$: set of finite/all executions
- Scheduler: $\sigma : exec^*(A) \to D$
  such that $\sigma(\alpha) = (s, a, \mu)$ implies $lstate(\alpha) = s$
- Measure μ_σ induced by a scheduler σ:

$$\mu_\sigma(C_{s_0 a_1 s_1 \ldots a_n s_n}) = \prod_{i=1}^{n} \mu_i(s_i)$$

  where $\sigma(s_0 \ldots a_i s_i) = (s_i, a_{i+1}, \mu_{i+1})$, and zero for all other cones

Probabilistic automata

When can we say that two automata have the same behaviour?



Lifting relations to distributions

- Let $\sim \subseteq S \times T$ be a relation between the sets S, T
- Define $\sim_p \subseteq \mathit{Disc}(S) \times \mathit{Disc}(T)$
- $\pi \sim_p \rho$ iff there exists $\alpha \in \mathit{Disc}(S \times T)$ such that:
  - $\alpha(s, T) = \pi(s)$ for each $s \in S$
  - $\alpha(S, t) = \rho(t)$ for each $t \in T$
  - $\alpha(s, t) = 0$ if $s \not\sim t$

Lifting equivalence relations to distributions

Let $\sim \subseteq S \times S$ be an equivalence relation on S.

Then $\pi \sim_p \rho$ iff $\pi([s]) = \rho([s])$ for all equivalence classes $[s]$ of $\sim$.

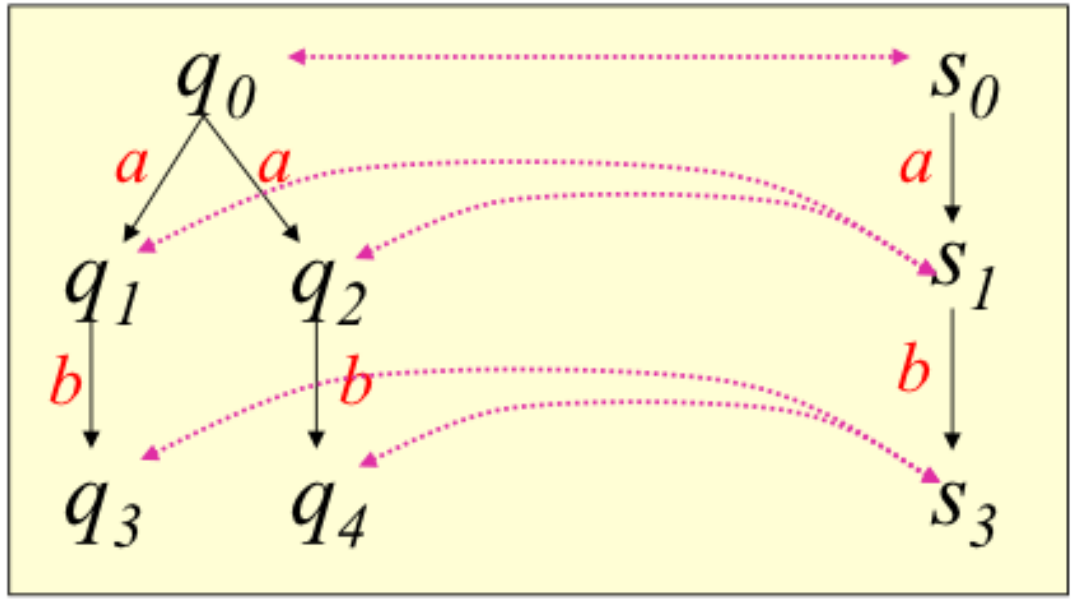
Probabilistic bisimulation

A relation $\mathcal{R} \subseteq S \times S$ is a *strong probabilistic bisimulation* iff for all $s_1, s_2 \in \mathcal{R}$ and for all $a \in A$

- if $s_1 \xrightarrow{a} \mu_1$ then $\exists \mu_2$ such that $s_2 \xrightarrow{a} \mu_2$ and $\mu_1 \,\mathcal{R}\, \mu_2$,
- if $s_2 \xrightarrow{a} \mu_2$ then $\exists \mu_1$ such that $s_1 \xrightarrow{a} \mu_1$ and $\mu_1 \,\mathcal{R}\, \mu_2$.

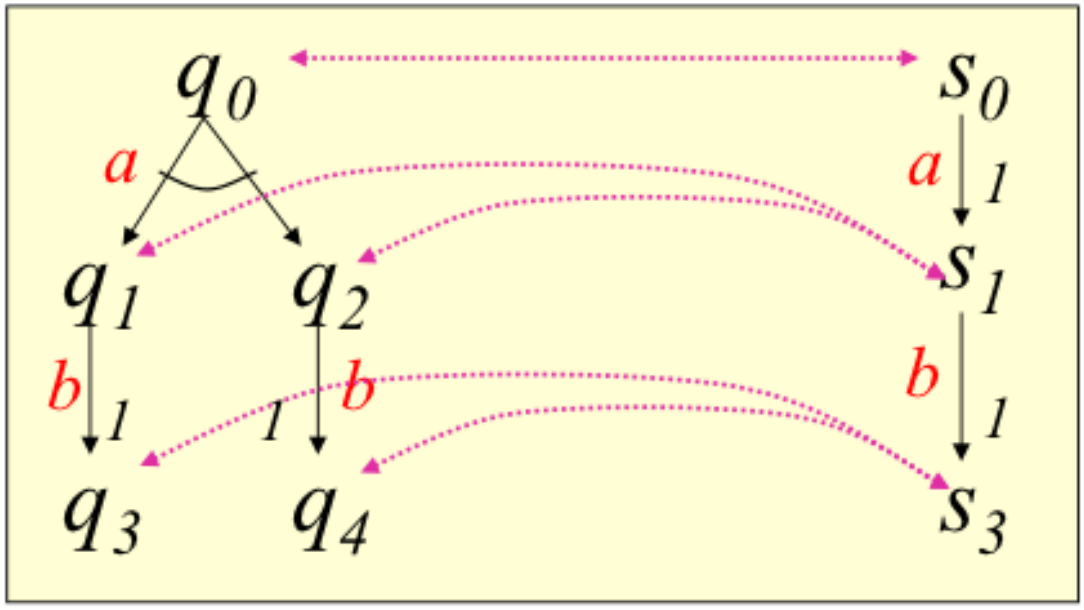
We write $s_1 \sim s_2$ if there is a strong bisimulation that relates them.

Example



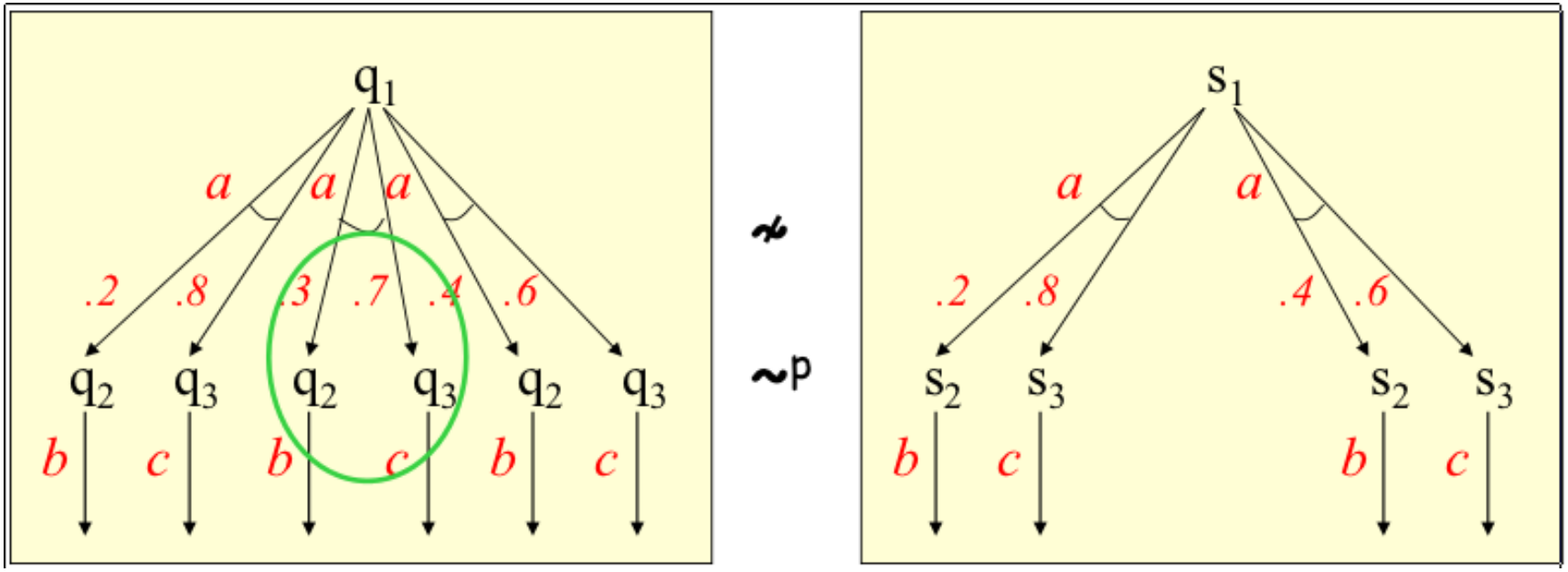
Example

With a probabilistic choice:



Exercise: show that this is a generalization of traditional bisimulation

Example



These processes can be made bisimilar if we allow "composed" transitions.

Exercise: define such a notion of bisimulation

Weak probabilistic bisimulation

- We include a silent action τ
- $s \stackrel{a}{\Longrightarrow} \mu \quad \mu \in Disc(S)$ iff
  - there exits a scheduler σ s.t.
  - s.t. $\mu(t) = \mu_\sigma(\tau^* a \tau^* t)$
  - where $\tau^* a \tau^* t$ is the union of all cones of the form $s\tau s_1 \tau \ldots s_n a \tau \ldots t$

Weak probabilistic bisimulation

A relation $\mathcal{R} \subseteq S \times S$ is a *weak probabilistic bisimulation* iff for all $s_1, s_2 \in \mathcal{R}$ and for all $a \in A$

- if $s_1 \xrightarrow{a} \mu_1$ then $\exists \mu_2$ such that $s_2 \stackrel{a}{\Longrightarrow} \mu_2$ and $\mu_1 \,\mathcal{R}\, \mu_2$,
- if $s_2 \xrightarrow{a} \mu_2$ then $\exists \mu_1$ such that $s_1 \stackrel{a}{\Longrightarrow} \mu_1$ and $\mu_1 \,\mathcal{R}\, \mu_2$.

We write $s_1 \approx s_2$ if there is a weak prob bisimulation that relates them.

CCS with internal probabilistic choice

$\alpha ::= a \mid \bar{a} \mid \tau$	**prefixes**
$P, Q ::=$	**processes**
$\alpha.P$	prefix
$\mid P \mid Q$	parallel
$\mid P + Q$	nondeterministic choice
$\mid \sum_i p_i P_i$	internal probabilistic choice
$\mid (\nu a)P$	restriction
$\mid\ !P$	replication
$\mid 0$	nil

CCS with internal probabilistic choice

Operational semantics given by a probabilistic automaton

$$\text{ACT} \quad \frac{}{\alpha.P \xrightarrow{\alpha} \delta(P)} \qquad \text{RES} \quad \frac{P \xrightarrow{\alpha} \mu \qquad \alpha \neq a, \overline{a}}{(\nu a)P \xrightarrow{\alpha} (\nu a)\mu}$$

$$\text{SUM1} \quad \frac{P \xrightarrow{\alpha} \mu}{P + Q \xrightarrow{\alpha} \mu} \qquad \text{SUM2} \quad \frac{Q \xrightarrow{\alpha} \mu}{P + Q \xrightarrow{\alpha} \mu}$$

$$\text{PAR1} \quad \frac{P \xrightarrow{\alpha} \mu}{P \mid Q \xrightarrow{\alpha} \mu \mid Q} \qquad \text{PAR2} \quad \frac{Q \xrightarrow{\alpha} \mu}{P \mid Q \xrightarrow{\alpha} P \mid \mu}$$

CCS with internal probabilistic choice

$$\text{COM} \quad \frac{P \xrightarrow{a} \delta(P') \quad Q \xrightarrow{\overline{a}} \delta(Q')}{P \mid Q \xrightarrow{\tau} \delta(P' \mid Q')}$$

$$\text{PROB} \quad \frac{}{\sum_i p_i P_i \xrightarrow{\tau} \sum_i p_i \, \delta(P_i)}$$

CCS with internal probabilistic choice

$$\text{REP1} \quad \frac{P \xrightarrow{\alpha} \mu}{!P \xrightarrow{\alpha} \mu \mid !P}$$

$$\text{REP2} \quad \frac{P \xrightarrow{a} \delta(P_1) \quad P \xrightarrow{\overline{a}} \delta(P_2)}{!P \xrightarrow{\tau} \delta(P_1 \mid P_2 \mid !P)}$$

Asynchronous π-calculus

π-calculus without output prefix (replaced by output action) and without choice ($+$)

$$\pi ::= x(y) \mid \tau$$

action prefixes (input, silent)

x, y are channel names

$$\begin{array}{rcll} P & ::= & O & \text{inaction} \\ & \mid & \pi.P & \text{prefix} \\ & \mid & \bar{x}y & \text{output action} \\ & \mid & P \mid P & \text{parallel} \\ & \mid & (\nu x)P & \text{restriction, new name} \\ & \mid & !\,P & \text{replication} \end{array}$$

Probabilistic asynchronous π-calculus

The input guarded choice is probabilistic.

The prefixes

$$\alpha \ ::= \ x(y) \mid \tau$$

input | silent action

The processes

$$\begin{array}{rcll} P & ::= & 0 & \text{inaction} \\ & \mid & \Sigma_i p_i \alpha_i . P_i & \text{probabilistic choice} \\ & \mid & \bar{x} y & \text{output} \\ & \mid & P \mid P & \text{parallel} \\ & \mid & (\nu x) P & \text{new name} \\ & \mid & ! \, P & \text{replication} \end{array}$$

where $\Sigma_i p_i = 1$

Probabilistic asynchronous π-calculus

- To give semantics to this calculus we need generalized automata
- Transition relation: $D \subseteq S \times Disc(A \times S)$
- We write $s\{\xrightarrow[p_i]{\alpha_i} s_i \mid i \in I\}$ for

  $(s, \mu) \in D$ with $\mu(\alpha_i, s_i) = p_i$

Operational semantics

Sum $\quad \sum_i p_i \alpha_i.P_i \; \{\xrightarrow[p_i]{\alpha_i} P_i\}_i$

Out $\quad \bar{x}y \; \{\xrightarrow[1]{\bar{x}y} \mathbf{0}\}$

Res $\quad \dfrac{P \; \{\xrightarrow[p_i]{\mu_i} P_i\}_i}{\nu y P \; \{\xrightarrow[p'_i]{\mu_i} \nu y P_i\}_{i:y \notin fn(\mu_i)}}$

$\exists i.\ y \notin fn(\mu_i)$ and
$\forall i.\ p'_i = p_i / \sum_{j:y \notin fn(\mu_j)} p_j$

Operational semantics

$$\text{Open}\quad \frac{P \{\xrightarrow[1]{\bar{x}y} P'\}}{\nu y P \{\xrightarrow[1]{\bar{x}(y)} P'\}}\ x \neq y \qquad \text{Par}\quad \frac{P \{\xrightarrow[p_i]{\mu_i} P_i\}_i}{P \mid Q \{\xrightarrow[p_i]{\mu_i} P_i \mid Q\}_i}$$

$$\text{Com}\quad \frac{P \{\xrightarrow[1]{\bar{x}y} P'\} \qquad Q \{\xrightarrow[p_i]{\mu_i} Q_i\}_i}{P \mid Q \{\xrightarrow[p_i]{\tau} P' \mid Q_i[y/z_i]\}_{i:\mu_i = x(z_i)} \cup \{\xrightarrow[p_i]{\mu_i} P \mid Q_i\}_{i:\mu_i \neq x(z_i)}}$$

Operational semantics

$$\text{Close}\quad \frac{P\ \{\xrightarrow[1]{\bar{x}(y)} P'\} \qquad Q\ \{\xrightarrow[p_i]{\mu_i} Q_i\}_i}{P \mid Q\ \{\xrightarrow[p_i]{\tau} \nu y(P' \mid Q_i[y/z_i])\}_{i:\mu_i = x(z_i)} \cup \{\xrightarrow[p_i]{\mu_i} P \mid Q_i\}_{i:\mu_i \neq x(z_i)}}$$

$$\text{Cong}\quad \frac{P \equiv P' \qquad P'\ \{\xrightarrow[p_i]{\mu_i} Q'_i\}_i \qquad \forall i.\ Q'_i \equiv Q_i}{P\ \{\xrightarrow[p_i]{\mu_i} Q_i\}_i}$$

Operational semantics

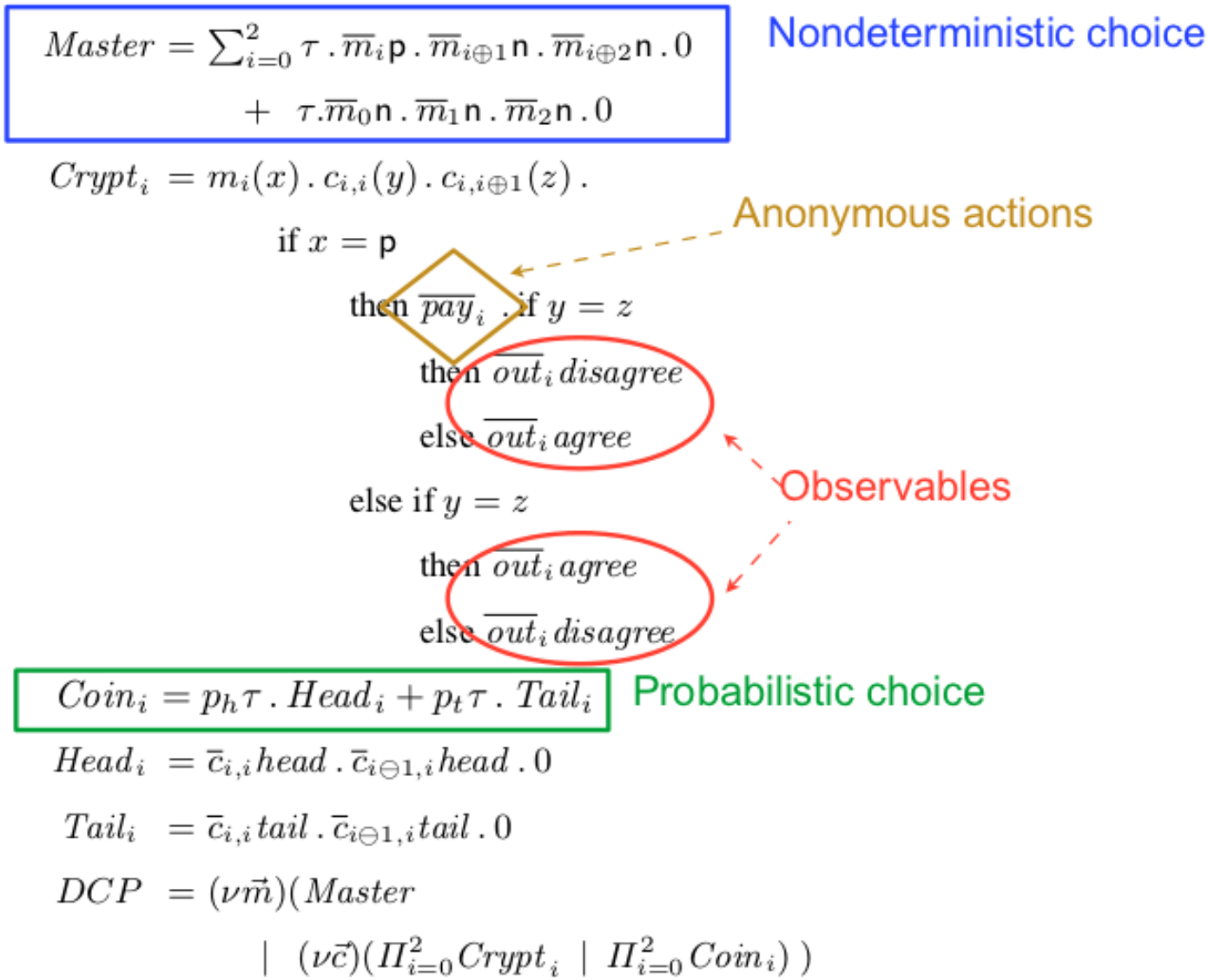
Structural congruence:

We assume that structural congruence satisfies the standard rules: associative monoid rules for $|$, the commutativity of the summands for Σ, the alpha-conversion, and the following:

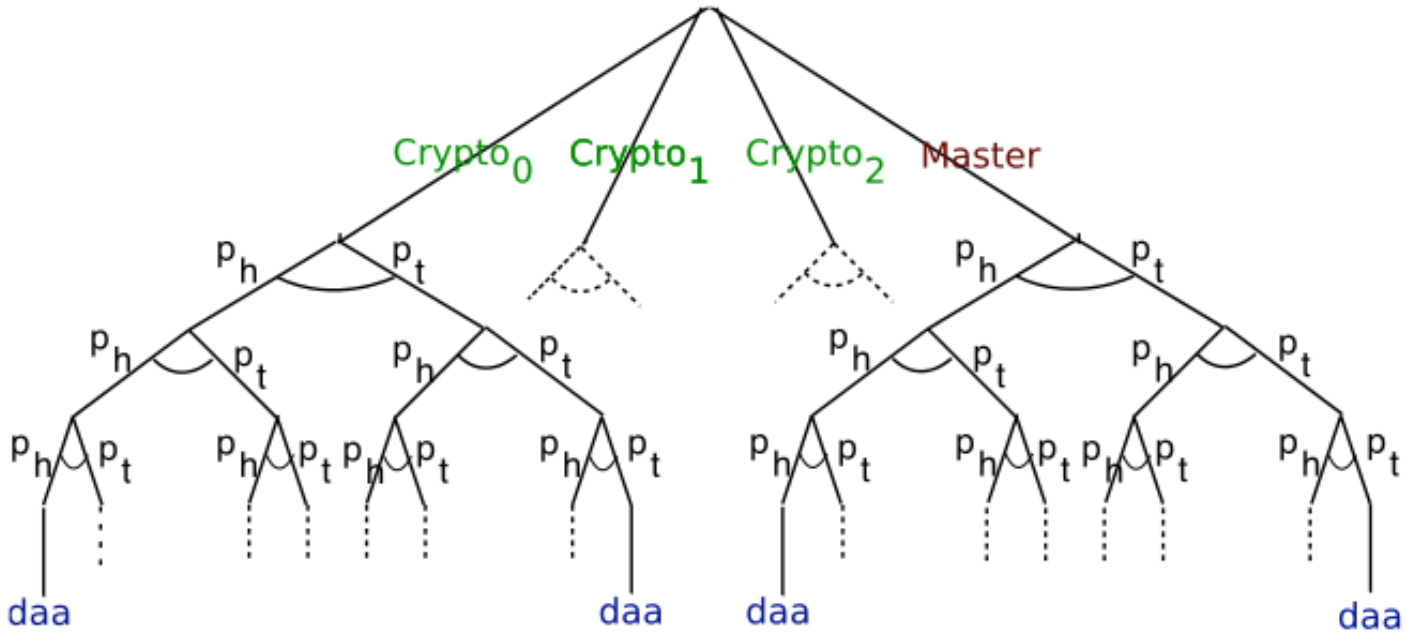
$(\nu x\, P) \mid Q \equiv \nu x\, (P \mid Q)$ if $x \notin fn(Q)$

$!\, P = P \mid !\, P.$

Dining cryptographers in the probabilistic π-calculus



Dining cryptographers in the probabilistic π-calculus



Have a nice holidays!

See you next year (hopefully)