PROBABILISTIC MODELS
LOGICS
&
EQUIVALENCES

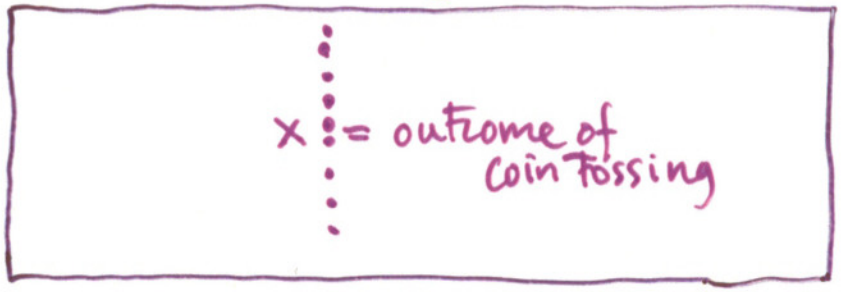
KIM G. LARSEN

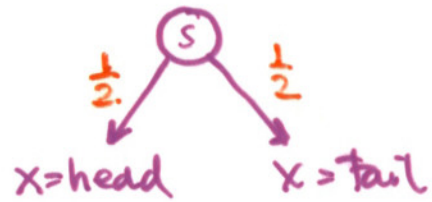
"Probabilistic systems": modelled by extensions of transition systems with probabilistic assumptions for state changes

Discrete Time

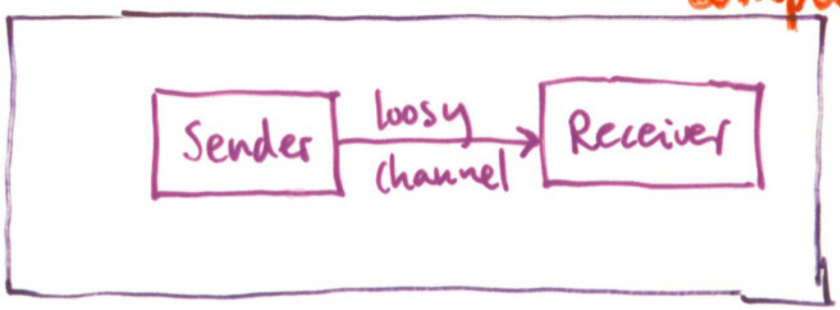
DTMCs or MDPs

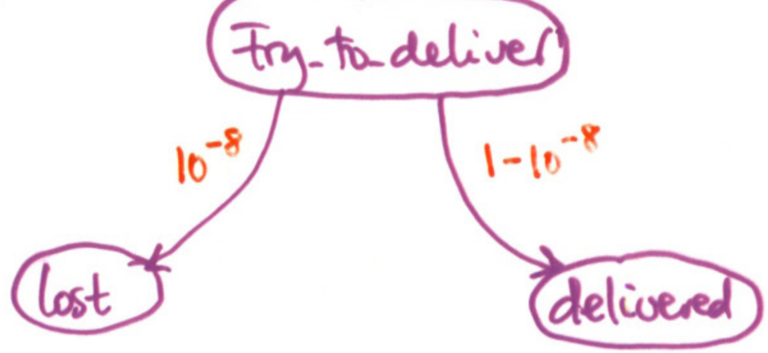
Randomized Algorithms





Parallel Systems w. unreliable media/components





OTHER APPLICATION AREA'S

Symmetry breakers in distributed algorithms:

"leader election is eventually resolved with probability 1"

Modelling of failures

"The chance of shutdown occuring is at most 1%"

Modelling Soft Deadlines

"The change of a frame being delivered within 5ms is at least 89%"

System Performance

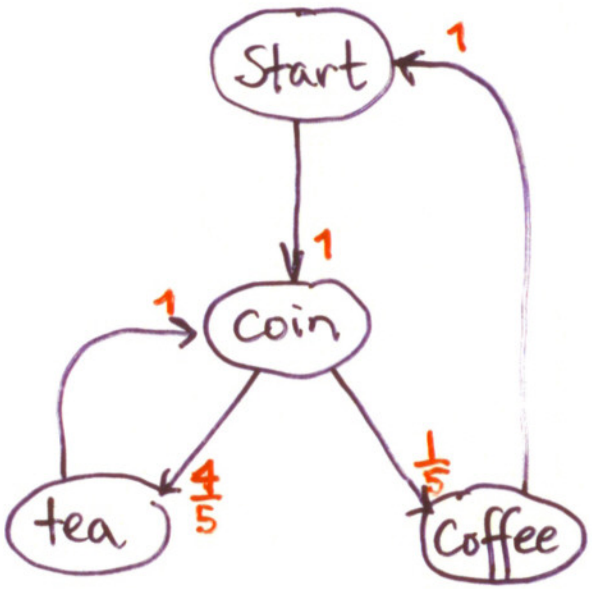
"In the long run mean waiting in a lift queue is 30sec"

QUESTIONS

- How to model stochastic/probabilistic systems (compositionally)? DTMC, CTMC, MDP, ..
- How to formulate correctness properties of systems? (hard → soft deadlines) PCTL, CSL, ..
- Relating properties of components to properties of systems?
- Notions of correct implementation.
- Algorithmic Support. PRISM, ETMCC, RAPTURE, ..

DTMC

Discrete Time Markov Chains



Markov Chain

(S, s_0, p, L)

sets of states

initial state

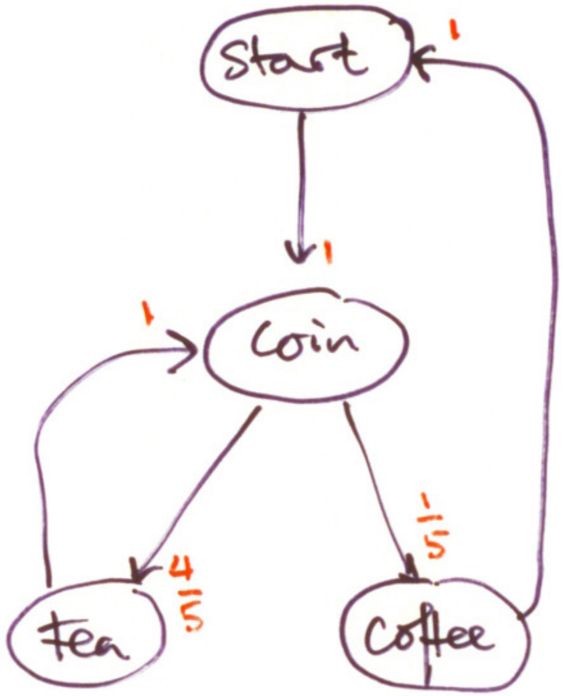
$L : S \to 2^{AP}$

$p : S \times S \to [0,1]$

s.t

$\forall s. \sum_{s'} p(s,s') = 1$

DTMC (cont.)



Path

$\sigma = s_0 \to s_1 \to s_2 \to \cdots \to s_n \to \cdots$

$\sigma[n] = s_n$

$\sigma\uparrow n = s_0 \to s_1 \to s_2 \to \cdots \to s_n$

Probability Measure on sets of path σ^*: from s_0

$$\mathrm{Prob}_{s_0}(\{\sigma : \sigma\uparrow n = s_0 \to s_1 \to \ldots \to s_n\})$$
$$= p(s_0, s_1) \cdot p(s_1, s_2) \cdot \ldots \cdot p(s_{n-1}, s_n)$$

Prob(start → coin → tea → coin → cof → ....)

$= 1 \cdot \frac{4}{5} \cdot 1 \cdot \frac{1}{5} = \frac{4}{25}$

* Prob defined on sigma-algebra generated by sets $\{\sigma : \sigma\uparrow n = s_0 \to s_1 \ldots \to s_n\}$.

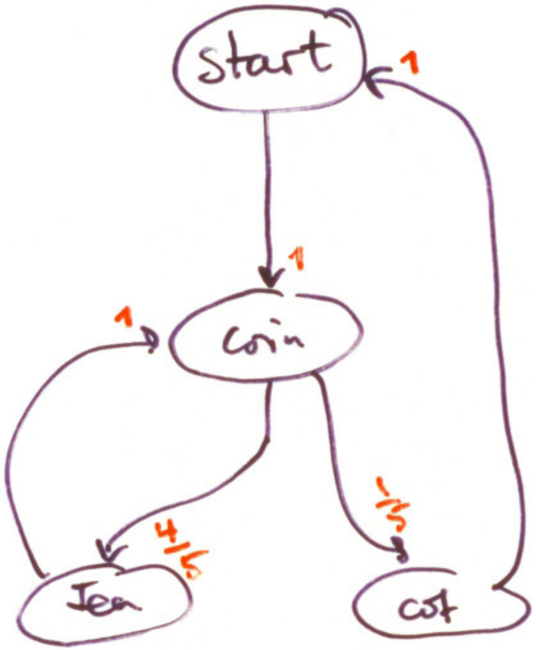
DTMC (cont)

Hitting Probabilities / Probabilistic Reachability.

Let $s \in S$ and $T \subseteq S$.

Then

$$\mathrm{Prob}(s, \Diamond T) = \mathrm{Prob}\left(\{\sigma \mid \sigma[0]=s \wedge \exists n.\ \sigma[n] \in T\}\right).$$



FACT

The values $\mathrm{Prob}(s, \Diamond T)$ $(s \in S)$ are the least solution (in $[0,1]$) of:

$$\mathrm{Prob}(s, \Diamond T) = \begin{cases} \sum_{s'} p(s,s') \cdot \mathrm{Prob}(s', \Diamond T) & ; s \notin T \\ 1 & ; s \in T \end{cases}$$

Ex.: $\mathrm{Prob}(\mathrm{start}, \Diamond \mathrm{cof})$

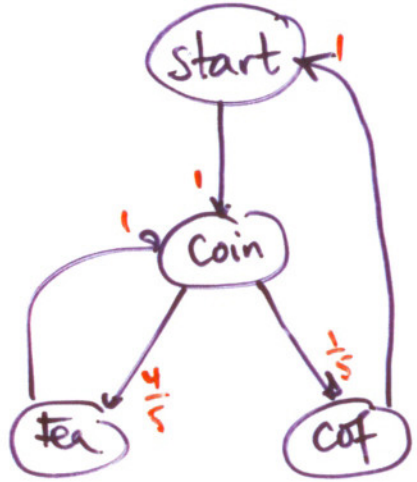
$x_{st} = 1 \cdot x_{coin}$

$x_{coin} = \frac{4}{5} \cdot x_{tea} + \frac{1}{5} \cdot x_{cof}$

$x_{cof} = 1$

$x_{tea} = 1 \cdot x_{coin}$

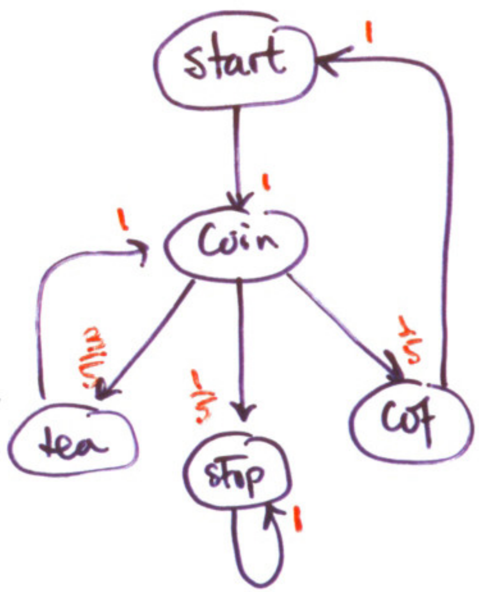
COMPUTATION of $Prob(s, \Diamond T)$



A: Computation by iteration.

B: Precompute $S^{No} = \{ s \mid Prob(s, \Diamond T) \overset{=}{>} 0 \}$ (without probabilities).

Find the unique solution of the linear equation system for states $s \in S \setminus (S^{No} \cup T)$ (e.g. Guass elimination)



MEAN HITTING TIMES

$H^T : \Sigma_s \longrightarrow \{0,1,2,\ldots\} \cup \{\infty\}$ $\qquad H^T(\sigma) = \inf\{n \geq 0 : \sigma[n] \in T\}$

w. sequences

We want to compute $\mathbb{E}_s(H^T)$ expected no of steps to hit T from s.

"FACT"

$$\boxed{\mathbb{E}_s(H^T) = \begin{cases} 0 & ; \ s \in T \\ 1 + \sum_{s'} p(s,s') \cdot \mathbb{E}_{s'}(H^T) & s \notin T \end{cases}}$$

Expected cost of hitting T from s:

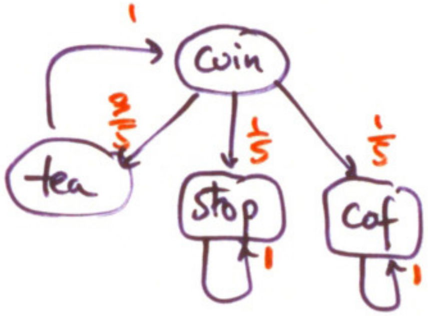
"FACT"

$$\boxed{\mathbb{E}_s(H_c^T) = \begin{cases} 0 & ; \ s \in T \\ c(s) + \sum_{s'} p(s,s') \cdot \mathbb{E}_{s'}(H_c^T) & s \notin T \end{cases}}$$

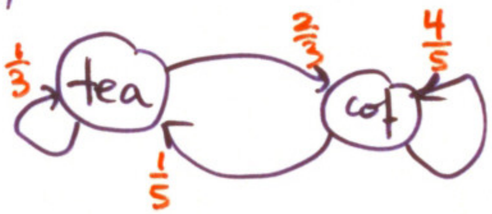
STATIONÆR FORDELING

Equilibrium:

1)



2)



3)

We want distribution $D : S \to [0,1]$
s.t.

$$D_s = \sum_{s'} p(s',s) \cdot D_{s'}$$

With $\sum_s D_s = 1$

$\frac{1}{D_s}$ = Expected time between two cons. s. (in limit!) (for connected DTMC

Only well defined for aperiodic DTMCs !!

LOGICAL PROPERTIES

CTL

(state-form)

$$\varphi ::= p \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \forall f \mid \exists f$$

(path-form)

$$f ::= \varphi_1 \, \mathsf{U} \, \varphi_2 \mid \varphi_1 \, \mathcal{U} \, \varphi_2 \mid X\varphi$$

$s \models p$ iff $p \in L(s)$

$s \models \forall f$ iff $\forall \sigma.\ \sigma[0]=s.\ \sigma \models f$

$\sigma \models X\varphi$ iff $\sigma[1] \models \varphi$

$\sigma \models \varphi_1 \mathsf{U} \varphi_2$ iff

$\exists i\ .\ \sigma[i] \models \varphi_2 \wedge \forall j<i.\ \sigma[j] \models \varphi$

$\sigma \models \varphi_1 \mathcal{U} \varphi_2$ iff

$\sigma \models \varphi_1 \mathsf{U} \varphi_2$ or $\forall j\ .\ \sigma[j] \models \varphi_1$

LOGICAL PROPERTIES

PCTL [Hansson/Jonsson ~90]

(state-form)

$$\varphi ::= p \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \cancel{\forall f} \mid \cancel{\exists f}$$

$$[f]_I$$

(path-form)

$$f ::= \varphi_1 \, U^{\le t} \varphi_2 \mid \varphi_1 \, \mathcal{U}^{\le t} \varphi_2 \mid \cancel{X\varphi}$$

$I \subseteq [0,1]$

$s \models p$ iff $p \in L(s)$

~~$s \models \forall f$ iff $\forall \sigma.\ \sigma[0]=s.\ \sigma \models f$~~

$\sigma \models X\varphi$ iff $\sigma[1] \models \varphi$

$\sigma \models \varphi_1 U^{\le t} \varphi_2$ iff

$\exists i \le t.\ \sigma[i] \models \varphi_2 \wedge \forall j < i.\ \sigma[j] \models \varphi_1$

$\sigma \models \varphi_1 \mathcal{U}^{\le t} \varphi_2$ iff

$\sigma \models \varphi_1 U^{\le t} \varphi_2$ or $\forall j \le t.\ \sigma[j] \models \varphi_1$

$s \models [f]_I$ iff

$\mathrm{Prob}(\{\sigma \mid \sigma[0]=s \wedge \sigma \models f\}) \in I$

MODEL CHECKING PCTL

Labelling Alg.

INPUT A (finite) DTMC ; A PCTL state formula φ

OUTPUT $Sat(\varphi) = \{ s \mid s \models \varphi \}$

IF $\varphi = p$ then ret $\{ s \mid p \in L(s) \}$

IF $\varphi = \varphi_1 \wedge \varphi_2$ then ret $Sat(\varphi_1) \cap Sat(\varphi_2)$

IF $\varphi = \neg \varphi_1$ then ret $S \setminus Sat(\varphi_1)$

IF $\varphi = [f]_I$ then

IF $f \equiv \varphi_1 \, U^{\leq t} \varphi_2$ $(t \neq +\infty)$ THEN

$P(t,s) =$ $Prob(\sigma : \sigma[0] = s \wedge \sigma \models \varphi_1 U^{\leq t} \varphi_2)$

Let
$$P(t,s) = \begin{cases} 0 & ; t < 0 \\ 1 & ; s \in Sat(\varphi_2), t \geq 0 \\ 0 & ; s \notin Sat(\varphi_2), s \notin Sat(\varphi_1), t \geq 0 \\ \sum_{s'} p(s,s') \cdot P(t-1, s') & ; \text{o/w} \end{cases}$$

RETURN $\{ s \mid P(t,s) \in I \}$

SPECIAL CASES

(allowing prob. to be ignored)

$$\varphi_1 \, U^{\leq t}_{>0} \, \varphi_2 = X^{\leq t}_{>0} \qquad X^{\leq t}_{>0} = \varphi_2 \vee (\varphi_1 \wedge \Diamond X^{\leq t-1}_{>0})$$

$$\varphi_1 \, U^{\leq \infty}_{>0} \, \varphi_2 = X_{>0} \qquad X_{>0} \underset{\min}{=} \varphi_2 \vee (\varphi_1 \wedge \Diamond X_{>0})$$

$$\varphi_1 \, U^{\leq t}_{\geq 1} \, \varphi_2 = X^{\leq t}_{\geq 1} \qquad X^{\leq t}_{\geq 1} \underset{n}{=} \varphi_2 \vee (\varphi_1 \wedge \Box X^{\leq t-1}_{\geq 1})$$

$$\varphi_1 \, U^{\leq \infty}_{\geq 1} \, \varphi_2 = X_{\geq 1} \qquad X_{\geq 1} \underset{\min}{=} \varphi_2 \vee (\varphi_1 \wedge \Box X_{\geq 1})$$

Denote $s \longrightarrow s'$ iff $p(s,s') > 0$

$\Diamond \varphi \equiv U^{\leq 1}_{>0} \varphi$ *
Almost

Write $\Diamond \varphi$ for the formula s.t.

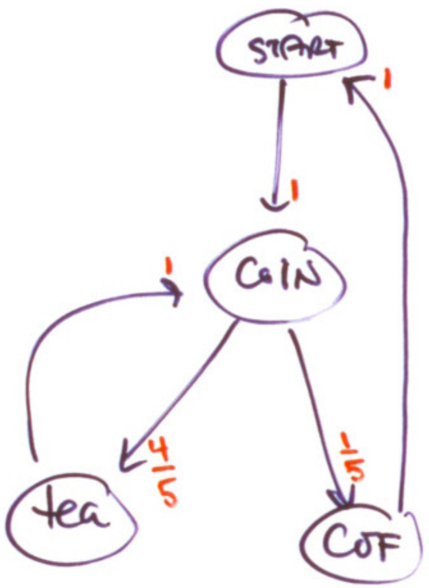
$s \models \Diamond \varphi$ iff $\exists s' . \, s \longrightarrow s' \wedge s' \models \varphi$

$\Box \varphi$: $s \models \Box \varphi$ iff $\forall s' . \, s \longrightarrow s' \Rightarrow s' \models \varphi$

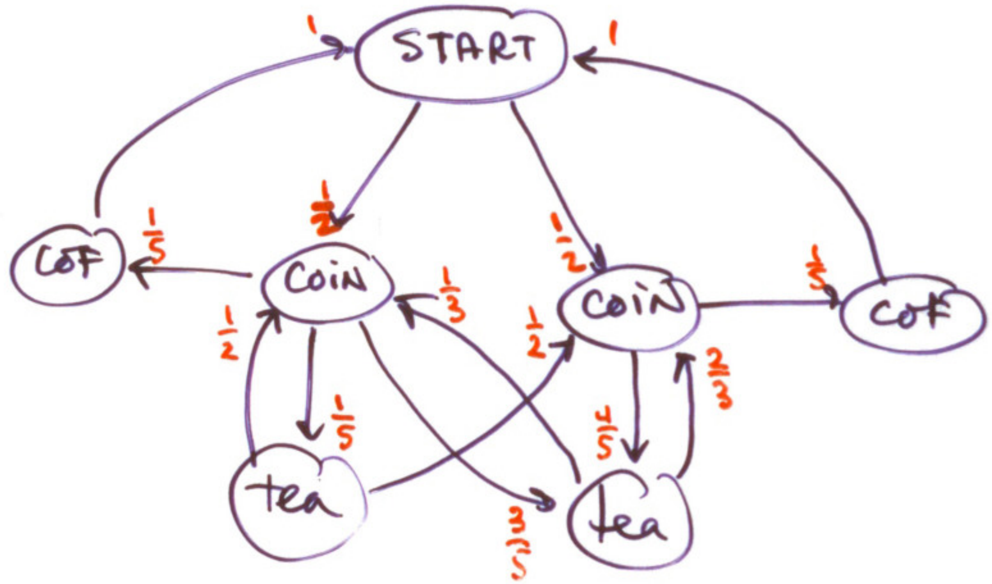
PROBABILISTIC BISIMULATION

Larsen & Skou 89

A simple machine



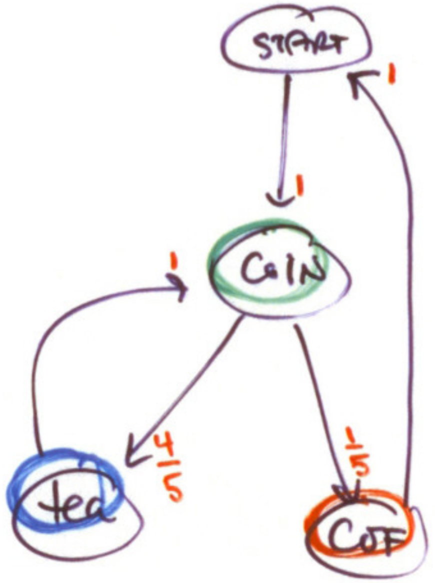
A complicated machine



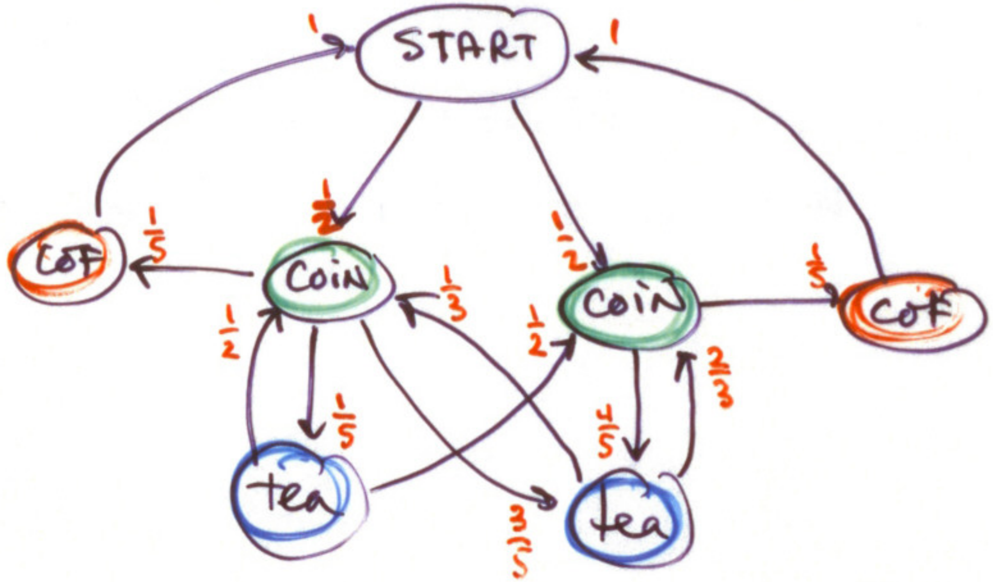
PROBABILISTIC BISIMULATION

Larsen & Skou 89

A simple machine



A complicated machine



PROBABILISTIC BISIMULATION (cont.)

DEF. A probabilistic bisimulation is an equivalence ($\equiv$) relation on S such that whenever $s_1 \equiv s_2$ then

i) $L(s_1) = L(s_2)$

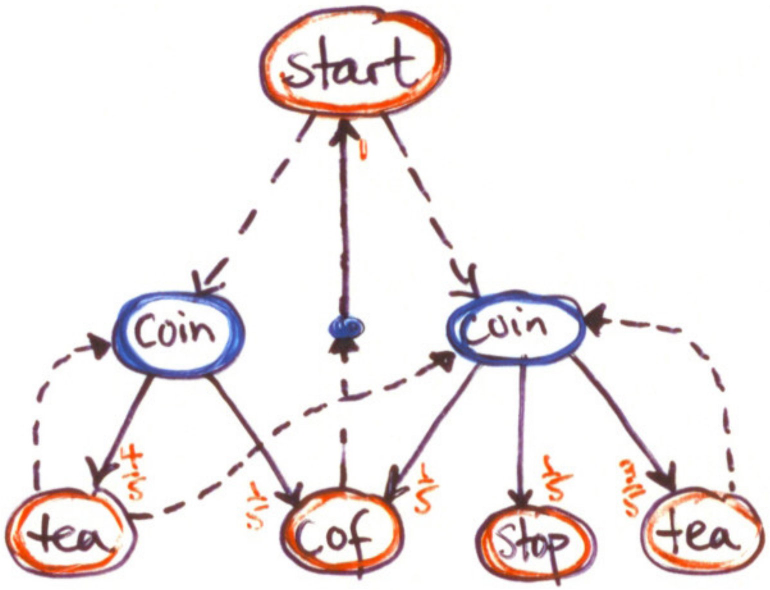
ii) For any $A \in S/\equiv$. $p(s_1, A) = p(s_2, A)$

$s_1 \sim s_2$ iff $s_1 \equiv s_2$ for some prob. bisim. $\equiv$.

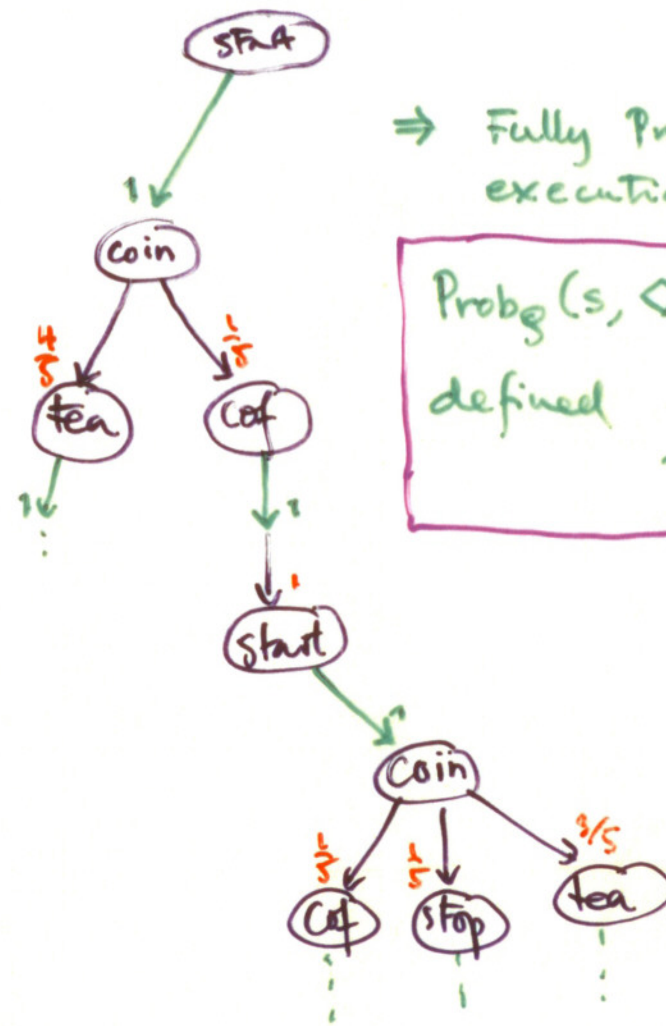
THM $s_1 \sim s_2$ iff $(\forall \varphi \in PCTL.\ s_1 \models \varphi \Leftrightarrow s_2 \models \varphi)$

MARKOV DECISION PROCESS

(Markov Chains with non-determinism)



Scheduler $\mathfrak{S}$: Resolves non-determinism



$\Rightarrow$ Fully Probabilistic execution.

$Prob_{\mathfrak{S}}(s, \Diamond T)$ defined as for DTMC

- probabilistic choice
- non deterministic choice

PROBLEMS:

$$Prob^{inf}(s, \Diamond T) = \inf_{\mathfrak{S}} Prob_{\mathfrak{S}}(s, \Diamond T)$$

$$Prob^{sup}(s, \Diamond T) = \sup_{\mathfrak{S}} Prob_{\mathfrak{S}}(s, \Diamond T)$$

COMPUTING Prob^{inf}:

FACT: For a MDP, the values $\mathrm{Prob}^{inf}(s, \Diamond T)$ are the least solution of:

- If $s \in T$ then $\mathrm{Prob}^{inf}(s, \Diamond T) = 1$
- If $s \notin T$ and s is probabilistic then

$$\mathrm{Prob}^{inf}(s, \Diamond T) = \sum_{s'} p(s,s') \cdot \mathrm{Prob}^{inf}(s', \Diamond T)$$

- If $s \notin T$ and s is non-deterministic then

$$\mathrm{Prob}^{inf}(s, \Diamond T) = \min_{s \to s'} \mathrm{Prob}^{inf}(s', \Diamond T)$$

Also BISIMULATION & SIMULATION

PCTL $s \models [f]_I$ iff

$\forall$ schedulers $\mathcal{S}$. $\mathrm{Prob}_{\mathcal{S}}(\{\sigma \mid \sigma[0] = s \wedge \sigma \models f\}) \in I$.