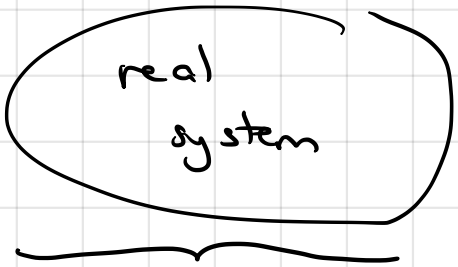
Modelling MDPs Compositionally

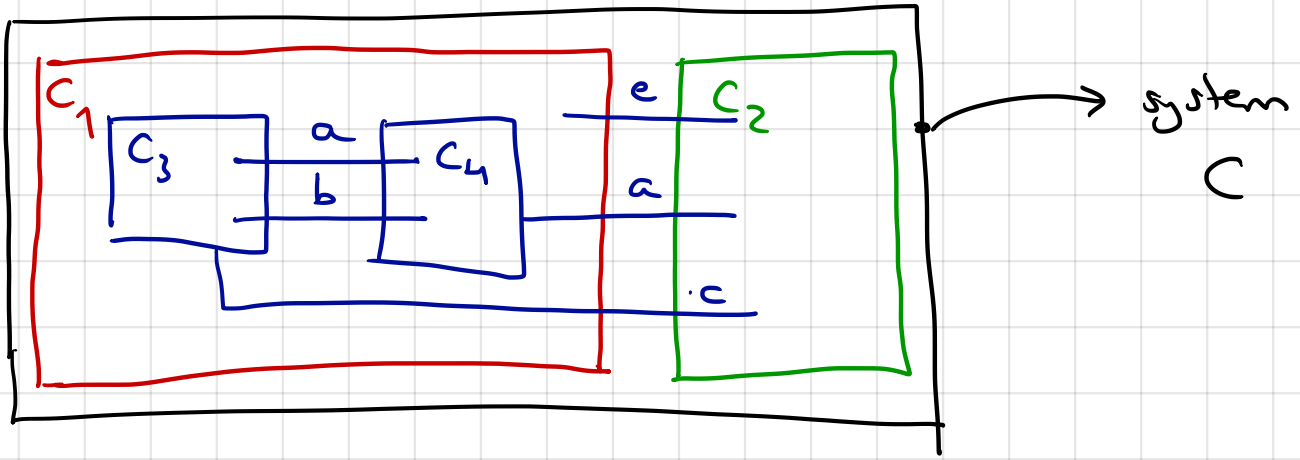
DTMCs / MDPs allow a monolithic modeling of systems



model ⟹ (big) single MDP / DTMC

- complex
- many components
- huge

Complexity of real systems requires a compositional approach: model directly reflects the system architecture (aka: structure)



$C_1 = C_3 \parallel_A C_4$ $\quad A = \{a, b\}$

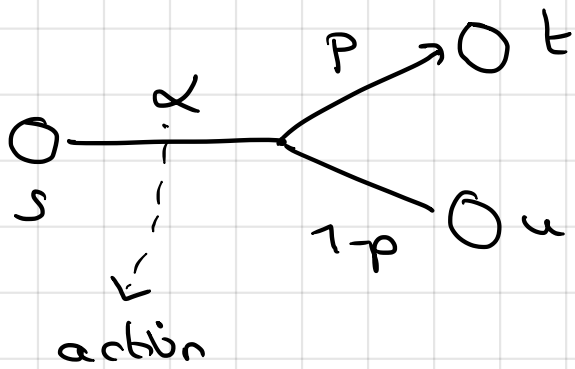
actions along which C_3 & C_4 "communicate"

$C = C_1 \parallel_B C_2$ $\quad B = \{a, c\}$

Needed: a way to combine MDPs. key:

Segala's Probabilistic Automata

- transitions



- actions will be used to "glue together" PAs
  = synchronisation

PA is a tple $(S, s_0, A, \longrightarrow)$ with

S is a set of states, $s_0 \in S$ initial state

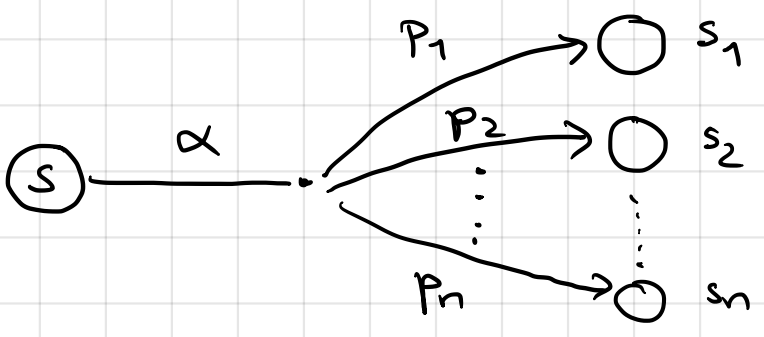
A is a set of actions

$\longrightarrow \subseteq S \times A \times Distr(S)$

Notation $(s, \alpha, \mu) \in \longrightarrow$ is denoted as

$$s \xrightarrow{\alpha} \mu$$

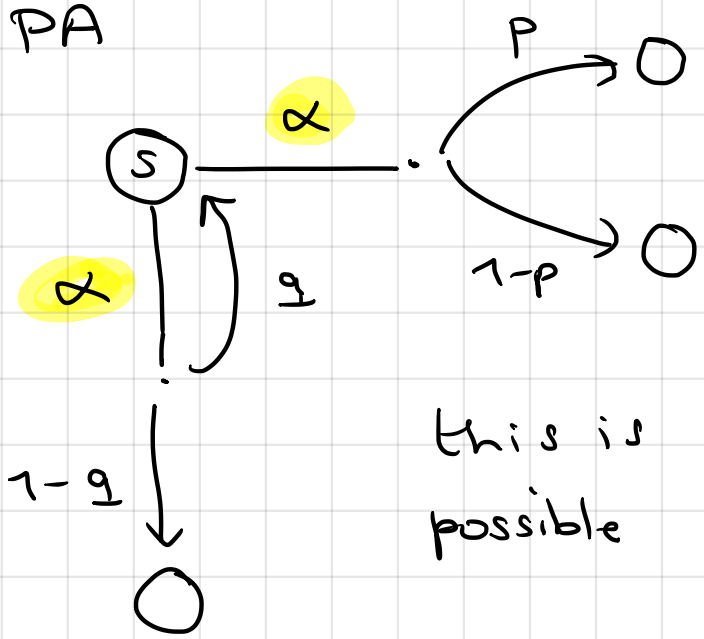
$s \xrightarrow{\alpha} \mu$ is depicted as follows:



$$\sum_{i=1}^{n} p_i = 1$$

Slight difference to MDPs:

in PA



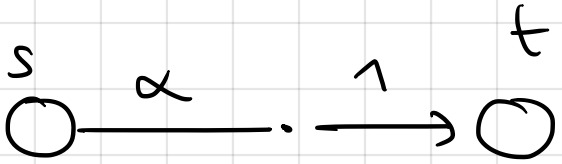
this is possible

In MDPs, this is not possible

---

if $|supp(\mu)| = 1$

then



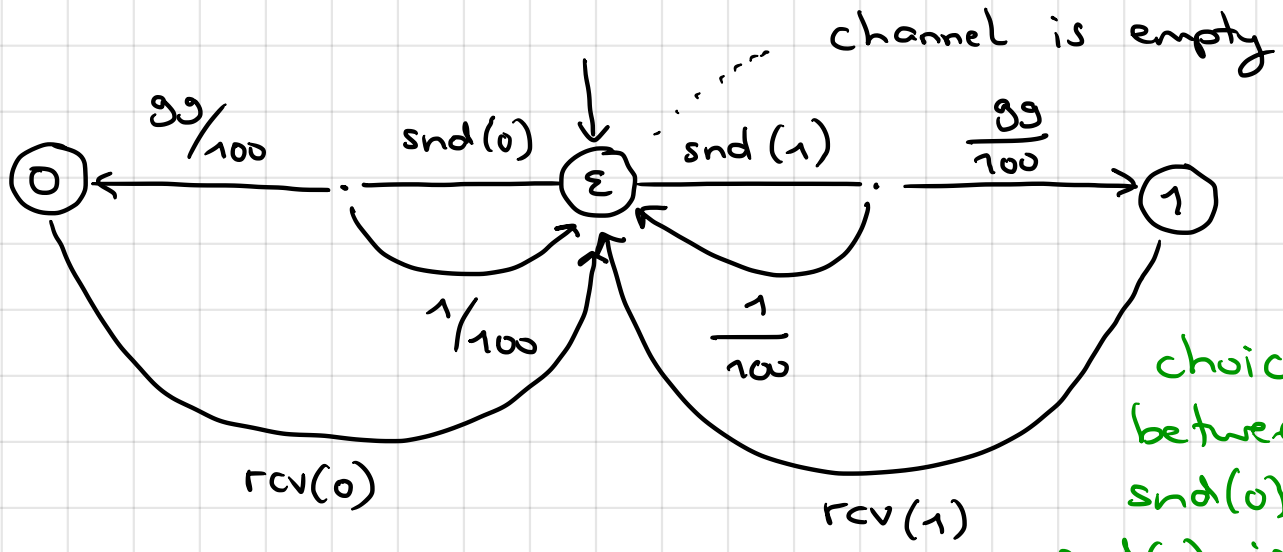
abbreviated by

Example lossy communication channel (capacity is 1)

carries bits

A.

loss rate $= \frac{1}{100}$

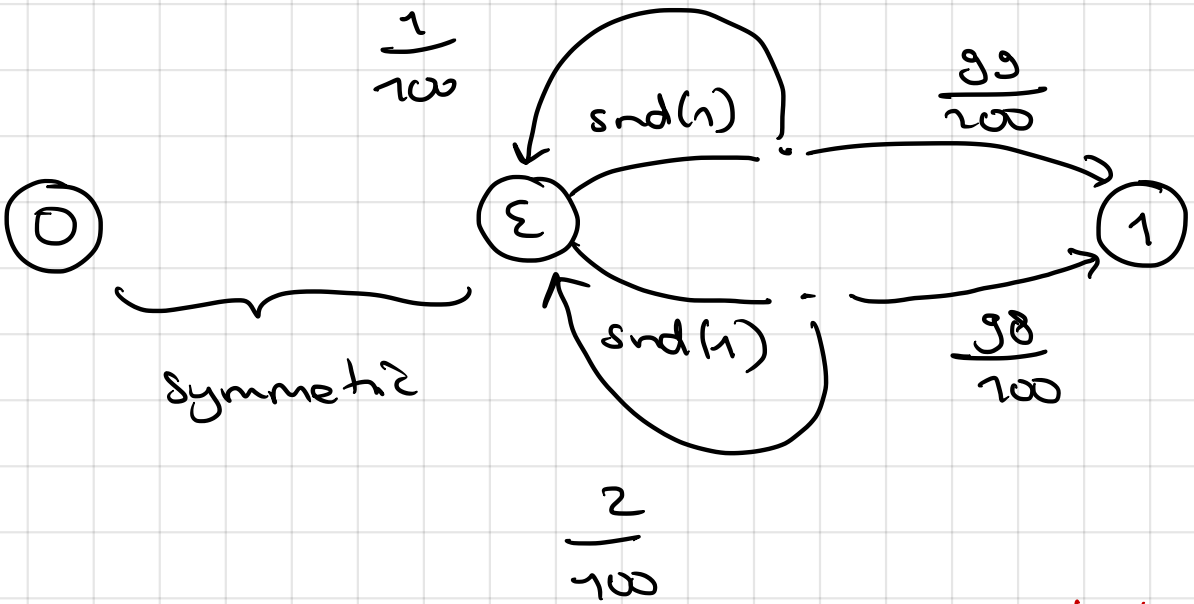


choice between snd(0) & snd(1) is "external"

B. a variant with partially unknown loss rate:

$$\text{rate} \in \left\{ \frac{1}{100}, \frac{2}{100} \right\}$$

can be resolved by environment



cannot be resolved by environment

choice between the two snd(1) branches is internal

Remark: every labelled transition system is a PA.

$s \xrightarrow{\alpha} s'$ by $s \xrightarrow{\alpha} \mu$

$\in$ LTS

$\mu(s') = 1$

Dirac distribution

Parallel composition of PA.

- essential to construct PA in a modular way = compositional
- state space of PA_1 & PA_2 is Cartesian product of S_1 and S_2
- assume a partial function

$$\gamma : A_1 \times A_2 \nrightarrow A$$

e.g. $\gamma(\alpha, \beta) = \delta$

α and β may synchronise and then are named δ

if $(\alpha, \beta) \in \text{dom}(\gamma)$ then PA_1 can also perform α autonomously (independent of PA_2)

similarly PA_2 can perform β autonomously

$PA_1 = (S_1, s_{0,1}, A_1, \longrightarrow_1)$

$PA_2 = (S_2, s_{0,2}, A_2, \longrightarrow_2)$

$PA_1 \parallel PA_2 = (S, s_0, A, \longrightarrow)$ with

$S = S_1 \times S_2 \quad , \quad s_0 = (s_{0,1}, s_{0,2})$

$A = A_1 \cup A_2$

$$\frac{s_1 \xrightarrow{\alpha}_1 \mu_1 \qquad s_2 \xrightarrow{\beta}_2 \mu_2}{(s_1, s_2) \xrightarrow{c} \mu_1 \times \mu_2} \quad \text{if } \gamma(\alpha, \beta) = c$$

$\mu_1 \times \mu_2$ product of distributions

$\mu_1 \times \mu_2 (s_1', s_2') = \mu_1(s_1') \cdot \mu_2(s_2')$

$$\frac{s_1 \xrightarrow{\alpha}_1 \mu_1}{(s_1, s_2) \xrightarrow{\alpha} \mu_1 \times \{s_2 \mapsto 1\}}$$

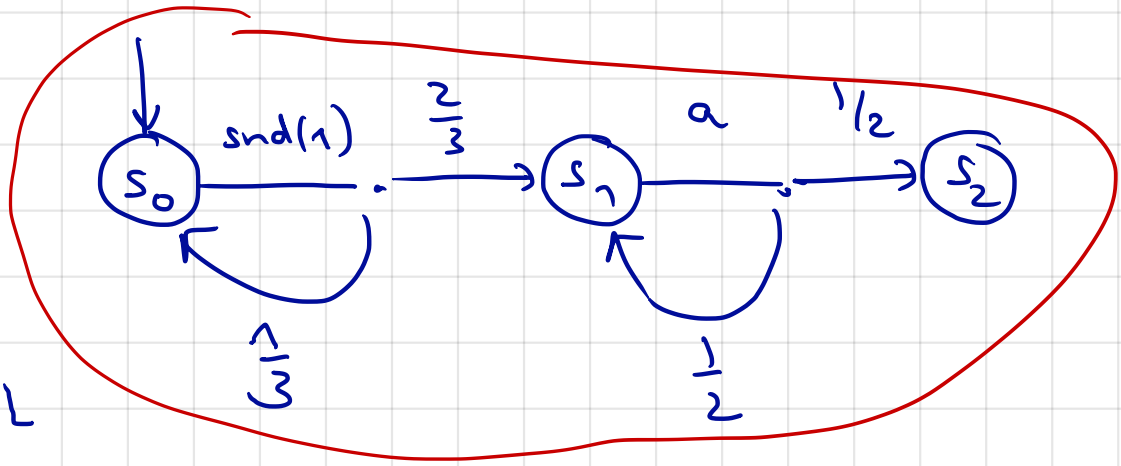
PA_2 stays in s_2 with prob. one

symmetrically

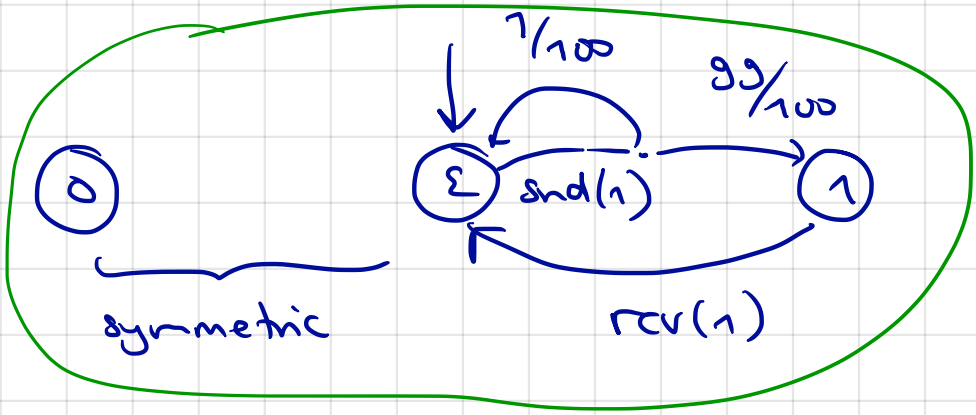
$$\frac{s_2 \xrightarrow{\alpha}_2 \mu_2}{(s_1, s_2) \xrightarrow{\alpha} \{s_1 \mapsto 1\} \times \mu_2}$$

Example

Sender



lossy channel

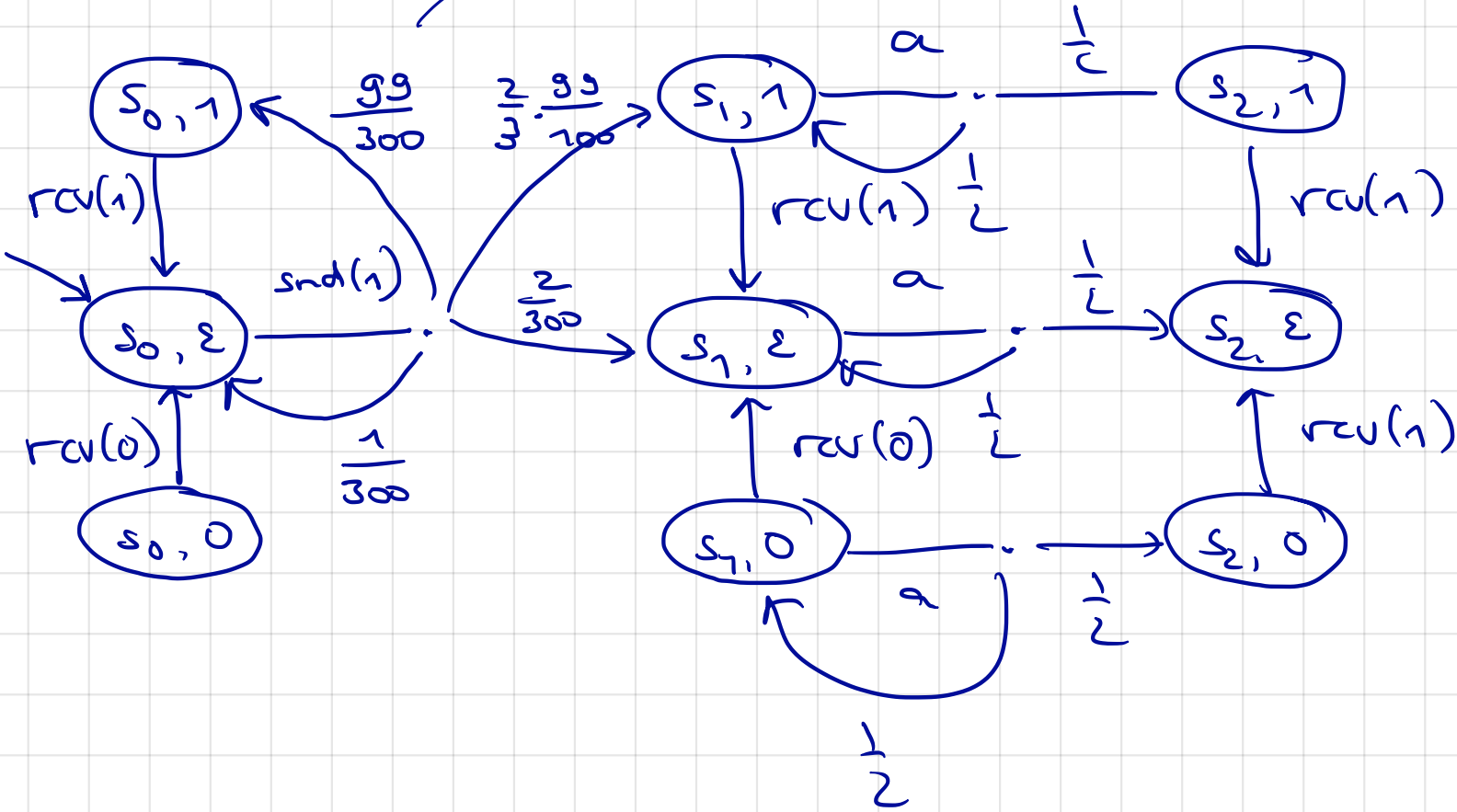


$f(snd(1), snd(1)) = snd(1)$

$f(a,b)$ is undefined for all other pairs

$\frac{1}{3} \cdot \frac{99}{100}$

Sender || Lossy Channel



Described in the syntax for PA:

$$Sender = snd(1).\left(Sender \oplus_{\frac{1}{3}} Sender_2\right)$$

$$Sender_2 = a.\left(Sender_2 \oplus_{\frac{1}{2}} \underline{0}\right)$$

$$LC = snd(0).\left(LC \oplus_{\frac{1}{100}} rcv(0).LC\right) + snd(1).\left(LC \oplus_{\frac{1}{100}} rcv(1).LC\right)$$

$$Sys = LC \parallel Sender \qquad \vdash (snd(1), snd(1)) = snd(1)$$

Parallel composition facilitates compositional modeling of (discrete) probabilistic systems

Assume $Sys = ((P_1 \,||\, \_) \,||\, \_) \,||\, \ldots \,||\, P_N)$

Now: we wat to minimise the underlying state space of Sys.

Approach 1 determine Sys' s.t. $|Sys'| \ll |Sys|$

and $Sys \sim_p Sys'$

↳ probabilistic bisimilar

then check e.g. for PCTL formula Φ whether $Sys' \models \Phi$

Then conclude $Sys \models \Phi$

⇒ not using the compositional definition of Sys

Approach 2 : use compositional minimisation.

$P_1 \,||\, P_2 \,||\, \ldots\ldots\ldots\ldots \,||\, P_N$

$\underbrace{\quad}_{\downarrow} \quad \underbrace{\quad}_{\downarrow}$

$\underbrace{P_1' \,||\, P_2'}_{} \,||\, \ldots\ldots\ldots \,||\, P_N'$ $\qquad P_i' \sim_p P_i$

First: probabilistic bisimulation on PA.

As for DTMCs, for states $(s,t) \in R$, we consider the probability to move from s to some eq. class under (and t) R.

Def. (lifting of an equivalence on S).

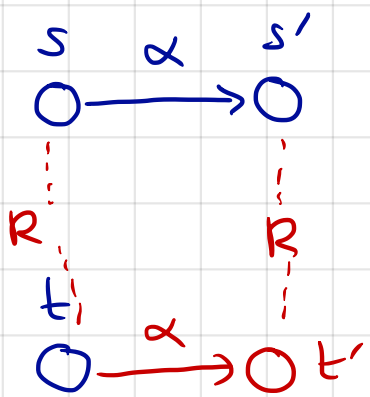
Let R be an equivalence on $S \times S$.

Then: the lifting of R to $Distr(S)$, denoted $\equiv_R$, is defined by:

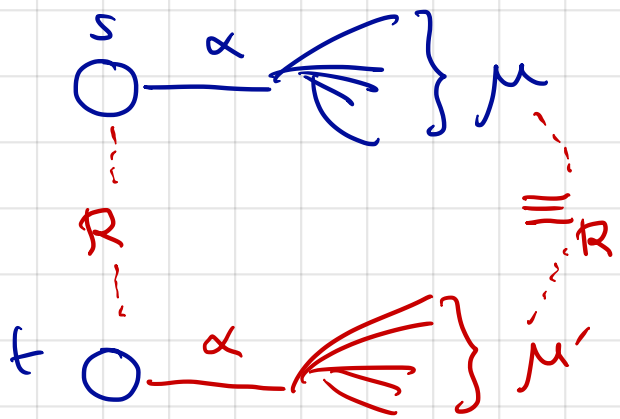
$$\mu \equiv_R \mu' \text{ iff } \forall C \in S/_R \cdot \mu(C) = \mu'(C)$$

$$\sum_{s \in C} \mu(s)$$

Intuition $(s,t) \in R$



now:



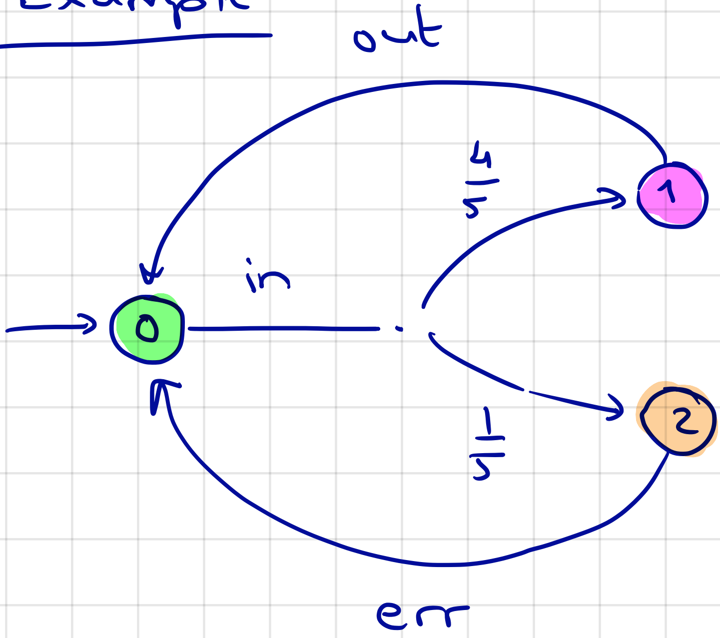
Def (strong bisimulation on PA)

Let $P = (S, s_0, A, \rightarrow)$ be a PA, and $R \subseteq S \times S$ an equivalence. Then: R is a strong bisimulation on P iff $\forall (s,t) \in R$ it holds

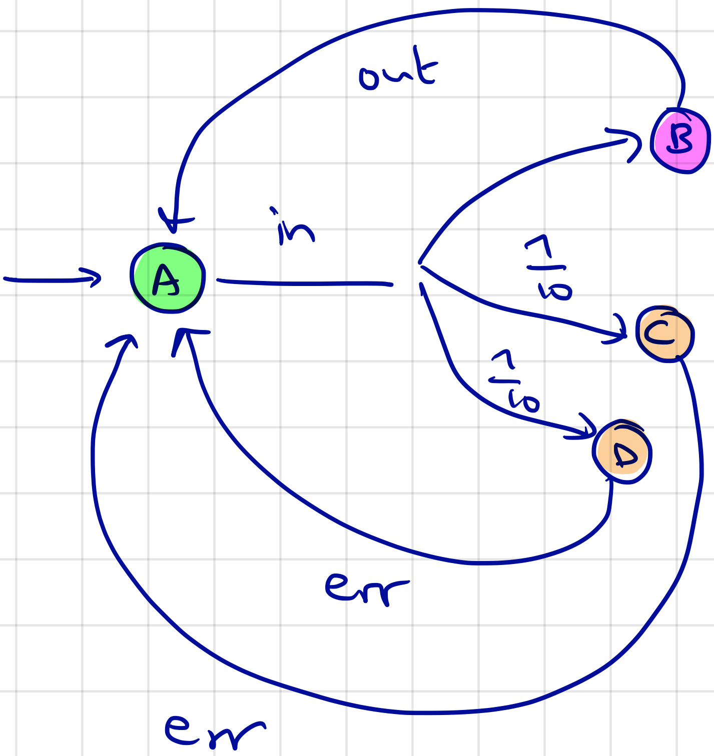
if $s \xrightarrow{\alpha} \mu$ then there exists $t \xrightarrow{\alpha} \nu$ such that $\mu \equiv_R \nu$.

States s and t are bisimilar, denoted $s \sim_P t$, if for some strong bisimulation R, $(s,t) \in R$.

Example



relation R, indicated by the colors is a strong bisimulation



e.g.

$0 \xrightarrow{\text{in}} \mu$

$\mu(\bullet) = \frac{4}{5}$

$\mu(\bullet) = \frac{1}{5}$

$A \xrightarrow{\text{in}} \nu$

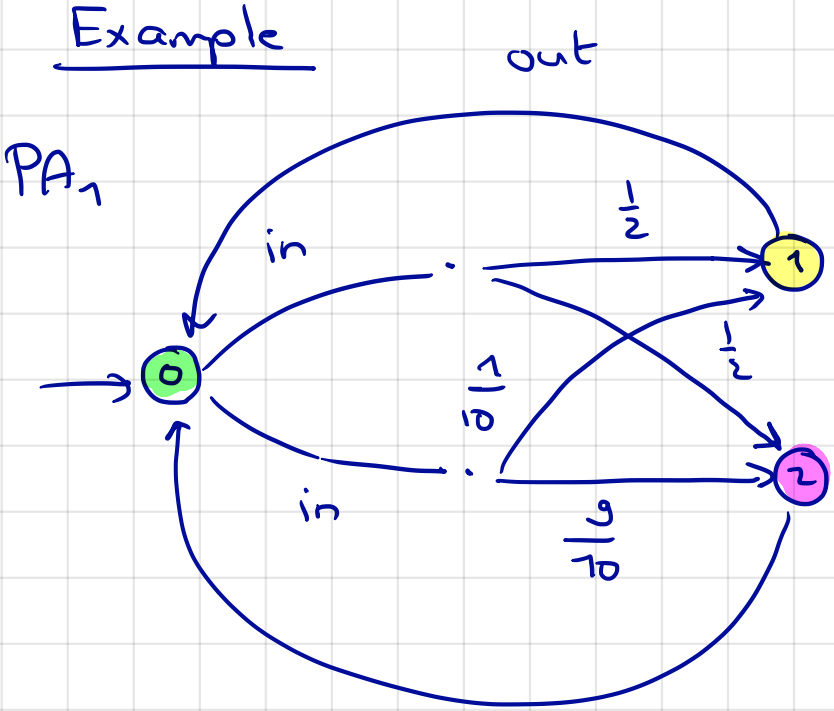
$\nu(\bullet) = \frac{4}{5}$

$\nu(\bullet) = \frac{1}{10} + \frac{1}{10}$

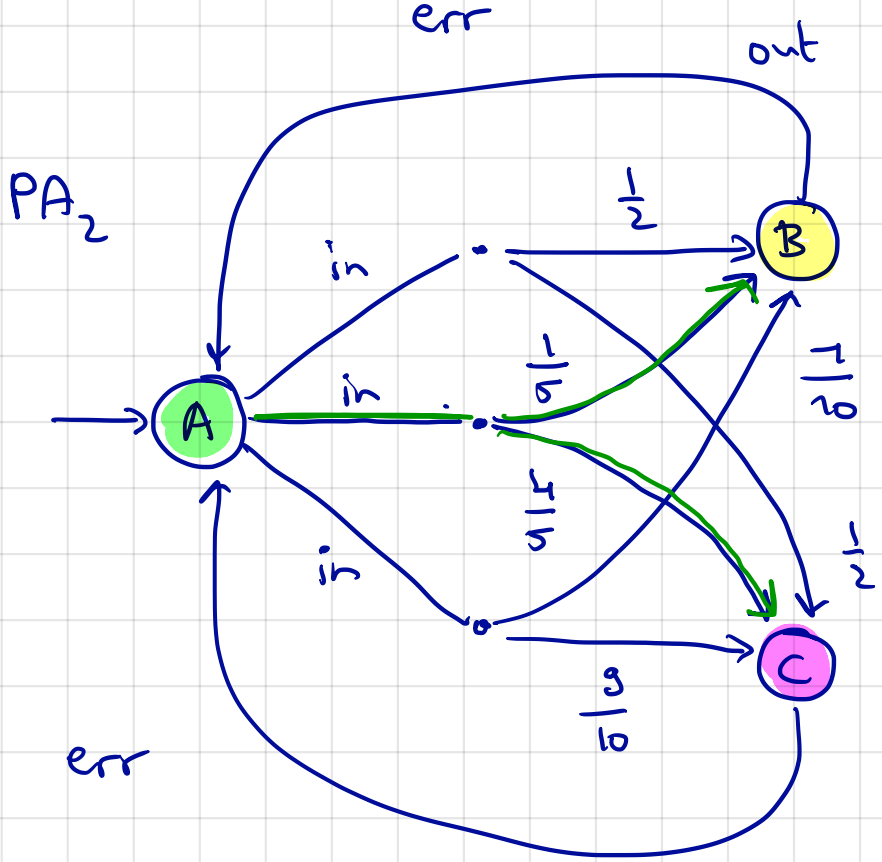
$= \frac{1}{5}$

$\mu \equiv_R \nu$

Example



err



$$\mu_1 = \{ 1 \mapsto \tfrac{1}{2},\ 2 \mapsto \tfrac{1}{2} \}$$

$$\mu_2 = \{ 1 \mapsto \tfrac{1}{10},\ 2 \mapsto \tfrac{9}{10} \}$$

$PA_1 \not\sim_p PA_2$

but they are (in some way) similar as the — option is in fact a convex combination of the two possible distributions

$$\mu = \frac{1}{4}\mu_1 + \frac{3}{4}\mu_2$$

but

$PA_1 \sim_{qp} PA_2$

This motivates the notion of

"combined" bisimulation

Notation: $s \xrightarrow{\alpha} \mu$ iff there is a family of transitions $s \xrightarrow{\alpha} \mu_i$ such that μ is a convex combination of μ_i's, i.e $\mu = \sum c_i \cdot \mu_i$

$0 \leq c_i \leq 1$ with $\sum c_i = 1$

Strong combined bisimulation

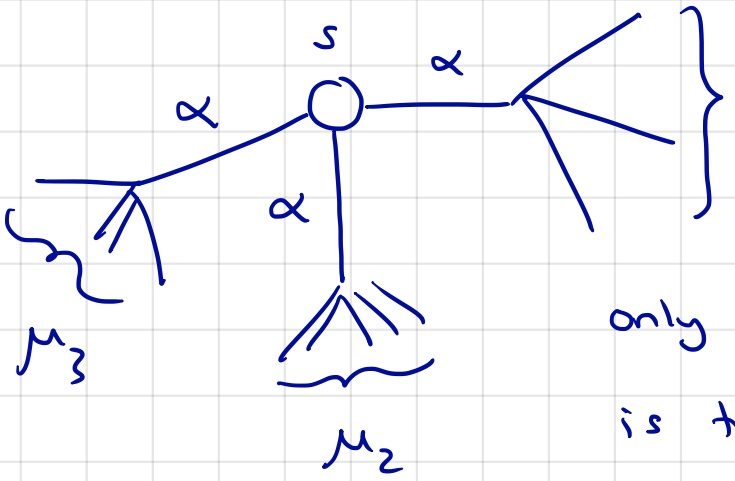
Equivalence $R \subseteq S \times S$ is a strong combined bisimulation iff $\forall (s,t) \in R$ it holds:

$s \xrightarrow{\alpha} \mu$ then there exists a combined transition $t \xrightarrow{\alpha} \nu$

and $\mu \equiv_R \nu$

$s \sim_{cp} t$ iff $(s,t) \in R$ for some strong combined bisimulation.

Probabilistic automata almost an MDP



only purpose of the actions is to compose PA so as to build larger PAs

$$Sys = (((PA_1 \parallel PA_2) \parallel PA_3) \ldots\ldots) \parallel PA_N$$

defined as follows:

$$\frac{s_1 \xrightarrow{\alpha}_1 \mu_1 \qquad s_2 \xrightarrow{\beta}_2 \mu_2}{(s_1, s_2) \xrightarrow{c} \mu_1 \times \mu_2} \; f(\alpha, \beta) = c$$

(s_1, s_2) a state in $PA_1 \parallel PA_2$

$$\mu_1 \times \mu_2 (s_1', s_2') = \mu_1(s_1') \cdot \mu_2(s_2')$$

$\mu_1 \times \mu_2 (s_1', s_2') = \frac{1}{3}$

$\mu_1(s_1') = \frac{1}{2}$ $\quad \mu_2(s_2') = \frac{2}{3}$

$\mu_1(t_1') = \frac{1}{2}$ $\quad \mu_2(t_2') = \frac{1}{6}$

$\mu_2(u_2') = \frac{1}{6}$

Analyse

$Sys = \underbrace{((PA_1 \,||\, PA_2) \,||\, \ldots\ldots)}\, ||\, PA_N$?

state space of Sys is exponential in N

① Minimise Sys wrt probabilistic bisimulation $\sim_p$.

Idea: if $s \xrightarrow{\alpha} \mu$ then $\exists\, t \xrightarrow{\alpha} \nu$ and $\mu \equiv_R \nu$

$R \subseteq S \times S$ equivalence

② Avoid constructing the entire (exponential) state space of Sys.

Compositional minimisation:

e.g. $Sys = PA_1 \,||\, PA_2$

$\sim_p$ ↓ ↓

$\widehat{Sys} = \widehat{PA_1} \,||\, \widehat{PA_2}$

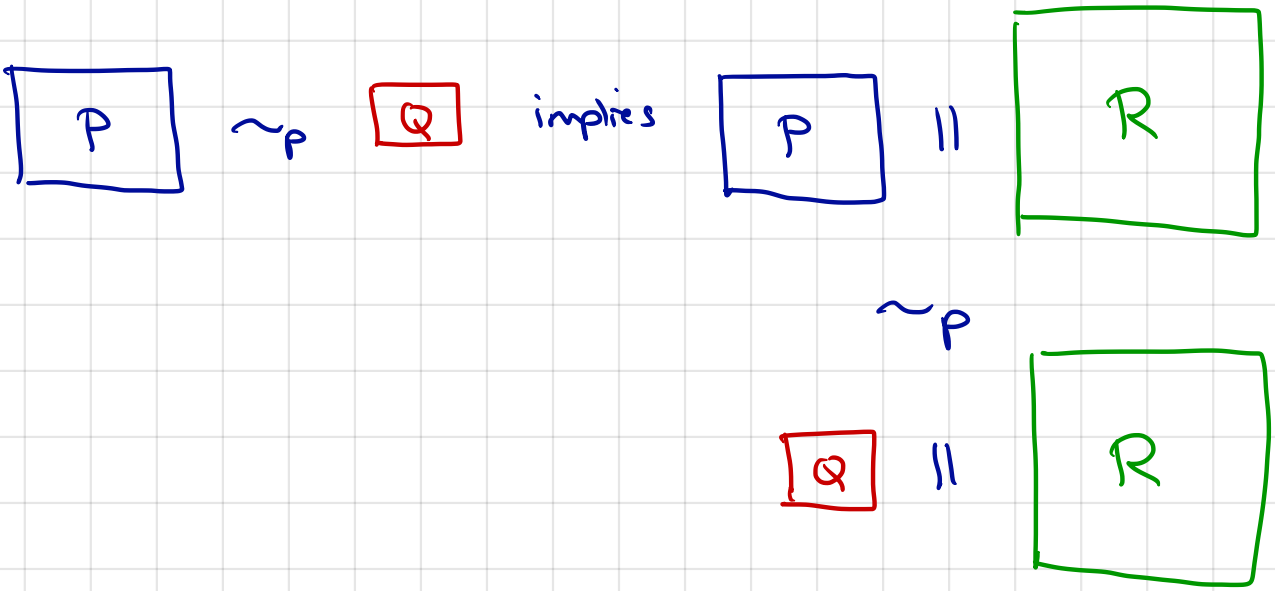
Congruence property

$\widehat{PA_1} \sim_p PA_1$ $\quad$ $\widehat{PA_2} \sim_p PA_2$

Theorem (Congruence theorem for PA)

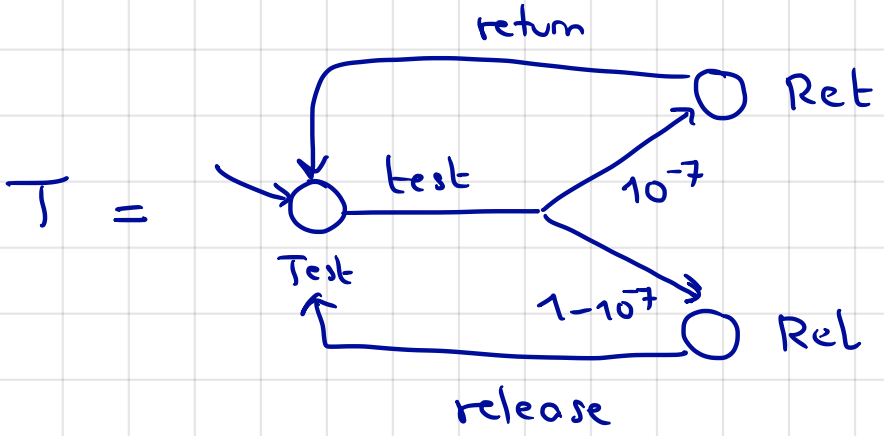
For every PA P, Q

1. $P \sim_p Q$ implies $\forall R \in PA.\ P \| R \sim_p Q \| R$



2. $P \sim_p Q$ implies $\forall R \in PA:\ R \| P \sim_p R \| Q$

Example (compositional minimisation)



$$P_N = \underbrace{T \,||\, T \,||\, \ldots \,||\, T}_{N \text{ times}}$$

size of $P_N = \mathcal{O}(3^N)$

Counting abstraction: keep track of how many Test processes are in state Test, Rel, Ret

$P(m, k, l)$

- m: # Test process in state "Test"
- k: state "Ret"
- l: state "Rel"

$P(m,k,\ell)$ = Test (m,k,ℓ) +

Return (m,k,ℓ) +

Release (m,k,ℓ)

Test (m,k,ℓ) = test, then $P(m-1,k+1,\ell)$ with prob 10^{-7}

else $P(m-1,k,\ell+1)$ with prob $1-10^{-7}$

Return (m,k,ℓ) = after a return, move to state

Return $(m+1,k-1,\ell)$ if $k>0$

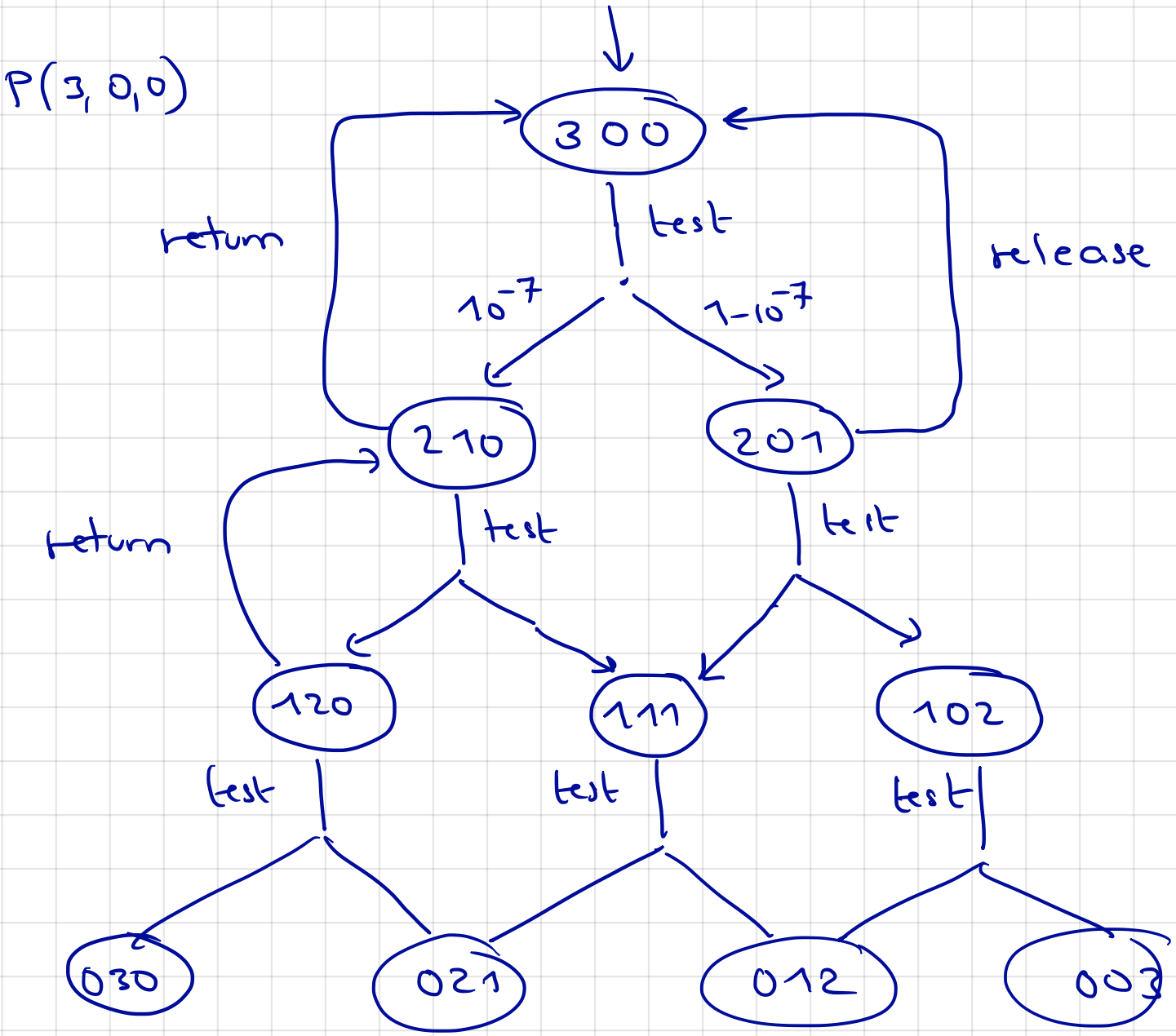
similarly for Test.

It follows that

$$P_N = \underbrace{T \,||\, \ldots \,||\, T}_{N \text{ times}} \sim_p P(N,0,0)$$

size of $P(N,0,0) \in O(N^2)$

$P(3,0,0) \quad \sim_p \quad T \parallel T \parallel T$



Why is this helpful

$T \parallel \ldots \parallel T$

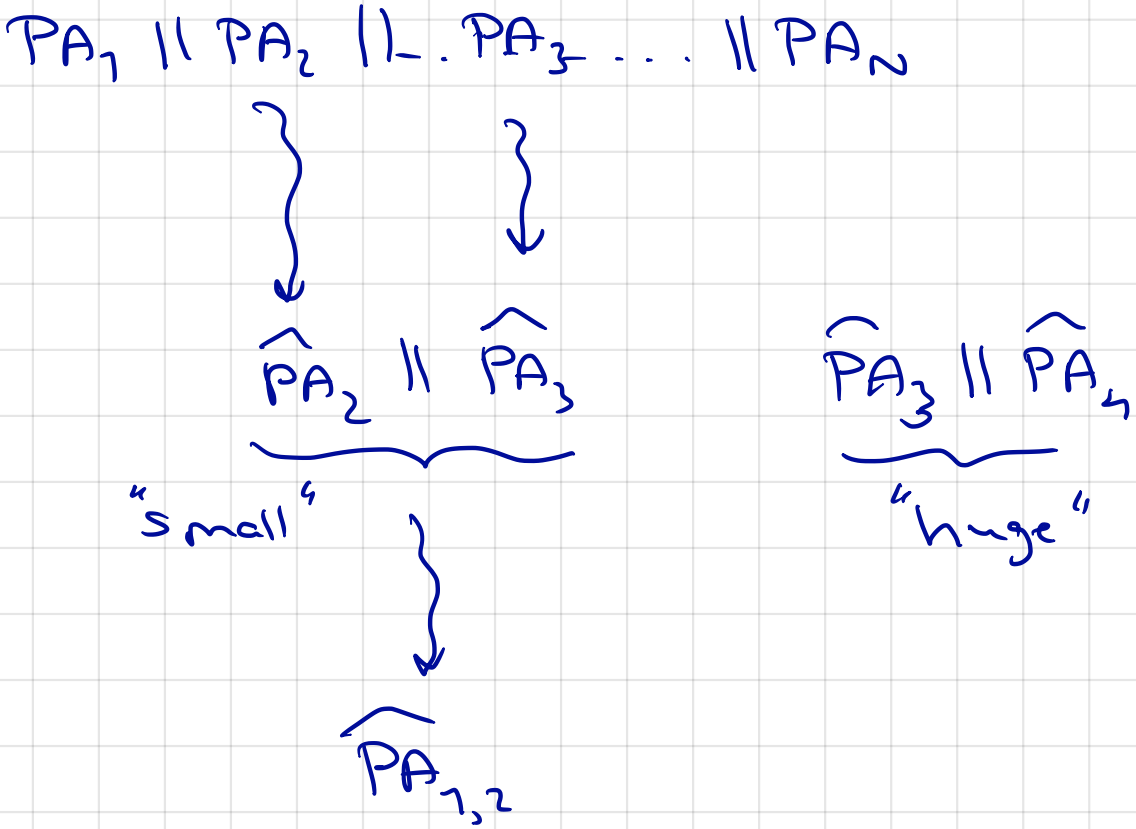
$Sys = \ldots \parallel \ldots \parallel P_N \parallel \ldots$

$\sim_p$

$Sys = \ldots \parallel \ldots \parallel P(N,0,0) \parallel \ldots$

This technique is widely used

- CADP (INRIA France)



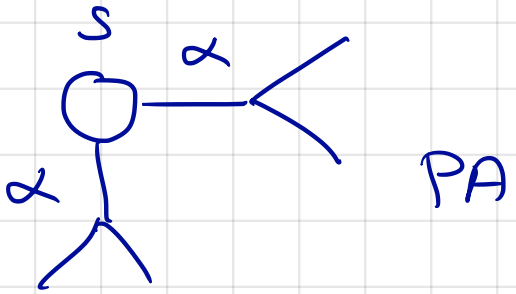
determine the optimal ordering of minimisation by means of a heuristic.

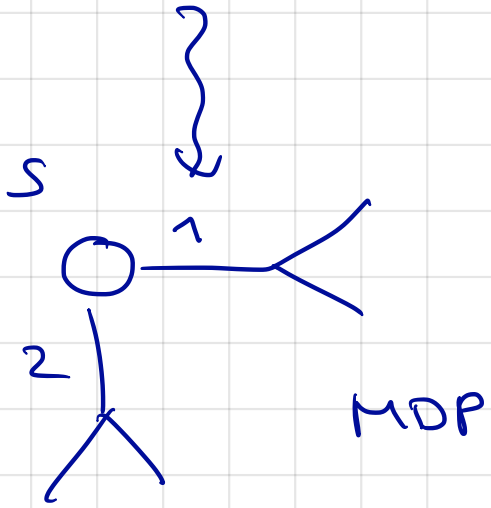
Step (3) Analyse

$\widehat{PA_1} \,||\, \widehat{PA_2} \,||\, \cdots \,||\, \widehat{PA_N}$

one PA

MDP





model checking MDP

For every PA P, Q

$P \sim_p Q$ implies $\mathbb{P}^{max}_{P}(\Diamond G) = \mathbb{P}^{max}_{Q}(\Diamond G)$

All MDP model-checking results are preserved under $\sim_p$.

How to describe PA syntactically ?

Syntax for describing PAs
- Petri nets
- Prob(b) mela
- Process algebra (Modest)

Syntax

$$P ::= \underline{0} \mid P_1 + P_2 \mid \alpha . \sum_{j \in J} [p_j] P_j \mid P_1 \parallel P_2 \mid X$$

$\alpha \in Act$; p_j prob.; J finite index set

where X is a defining equation $X = Q$

Examples

$$X = \alpha . \sum_{j \in \{1,2\}} [p_j] P_j \qquad p_1 = \frac{1}{3} \quad p_2 = \frac{2}{3}$$

$$P_1 = \beta . \underline{0}$$

$$P_2 = \gamma . \underline{0}$$

Shorthand $X = \alpha . (\beta . \underline{0} \oplus_{1/3} \gamma . \underline{0})$

$$X = \alpha.(\beta.\underline{0} \oplus_{\frac{1}{3}} \gamma.\underline{0})$$

$$Y = X + \alpha.(\underline{0} \oplus_{\frac{1}{2}} Y)$$

Semantics the semantics of the syntax term P is the PA $= (S, s_0, A, \rightarrow)$

S = set all sub-terms of P

$s_0 = P$

A = set of actions occurring in P

$\rightarrow$ is defined by the following rules

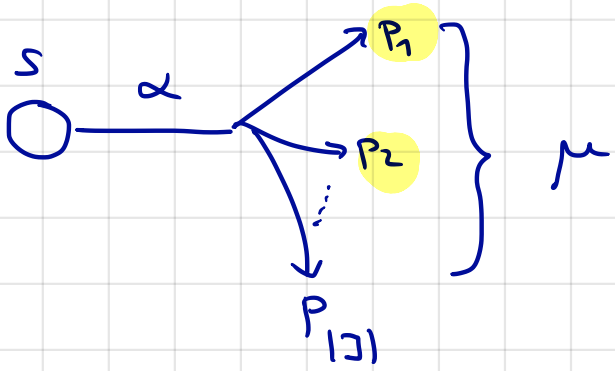
$$\frac{P_1 \xrightarrow{\alpha} \mu}{P_1 + P_2 \xrightarrow{\alpha} \mu} \qquad \frac{P_2 \xrightarrow{\alpha} \mu}{P_1 + P_2 \xrightarrow{\alpha} \mu}$$

$$\frac{P \xrightarrow{\alpha} \mu}{X \xrightarrow{\alpha} \mu} \quad (X = P)$$

true

$$\alpha \sum_{j \in]} [p_j]\, P_j \xrightarrow{\alpha} \mu$$

with



$$\mu(P) = \sum_{\substack{j \in] \\ P_j = P}} p_j$$

Example

$$\alpha.\left(\underbrace{\beta.\underline{0}}_{P_1} \oplus_{\frac{1}{2}} \underbrace{\beta.\underline{0}}_{P_2}\right) \xrightarrow{\alpha} \mu$$

where $\mu(\beta.\underline{0}) = \sum_{\substack{j \in \{1,2\} \\ P_j = \beta.\underline{0}}} p_j$

$= \frac{1}{2} + \frac{1}{2} = 1$

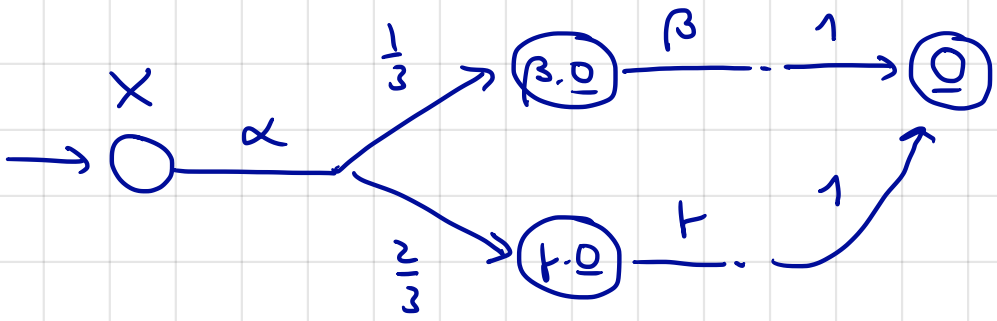
Example $X = \alpha.(\beta.\underline{0} \oplus_{\frac{1}{3}} \tau.\underline{0})$

$Y = X + \alpha.(\underline{0} \oplus_{\frac{1}{2}} Y)$

PA(X) $\quad \alpha.(\beta.\underline{0} \oplus_{\frac{1}{3}} \tau.\underline{0}) \xrightarrow{\alpha} \mu$

$\mu(\beta.\underline{0}) = \frac{1}{3}$

$\mu(\tau.\underline{0}) = \frac{2}{3}$



$\beta.\underline{0} \xrightarrow{\beta} \nu \quad$ with $\nu(\underline{0}) = 1$

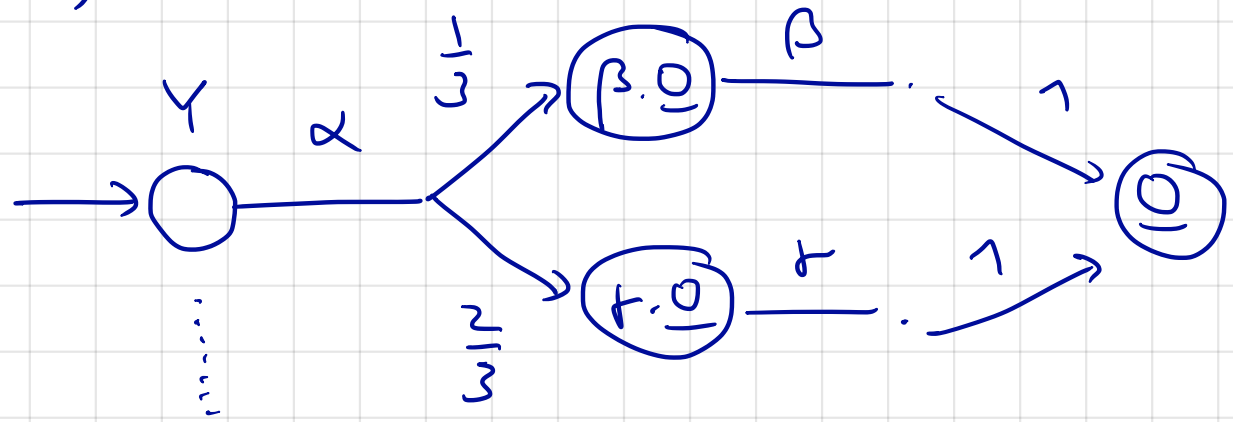
PA(Y)

$\overset{1}{=}$

$$\frac{X \xrightarrow{\alpha} \mu}{X + \alpha.\ldots \xrightarrow{\alpha} \mu} \qquad (Y = X + \alpha..)$$

$$Y \xrightarrow{\alpha} \mu$$

PA(Y)



Derive

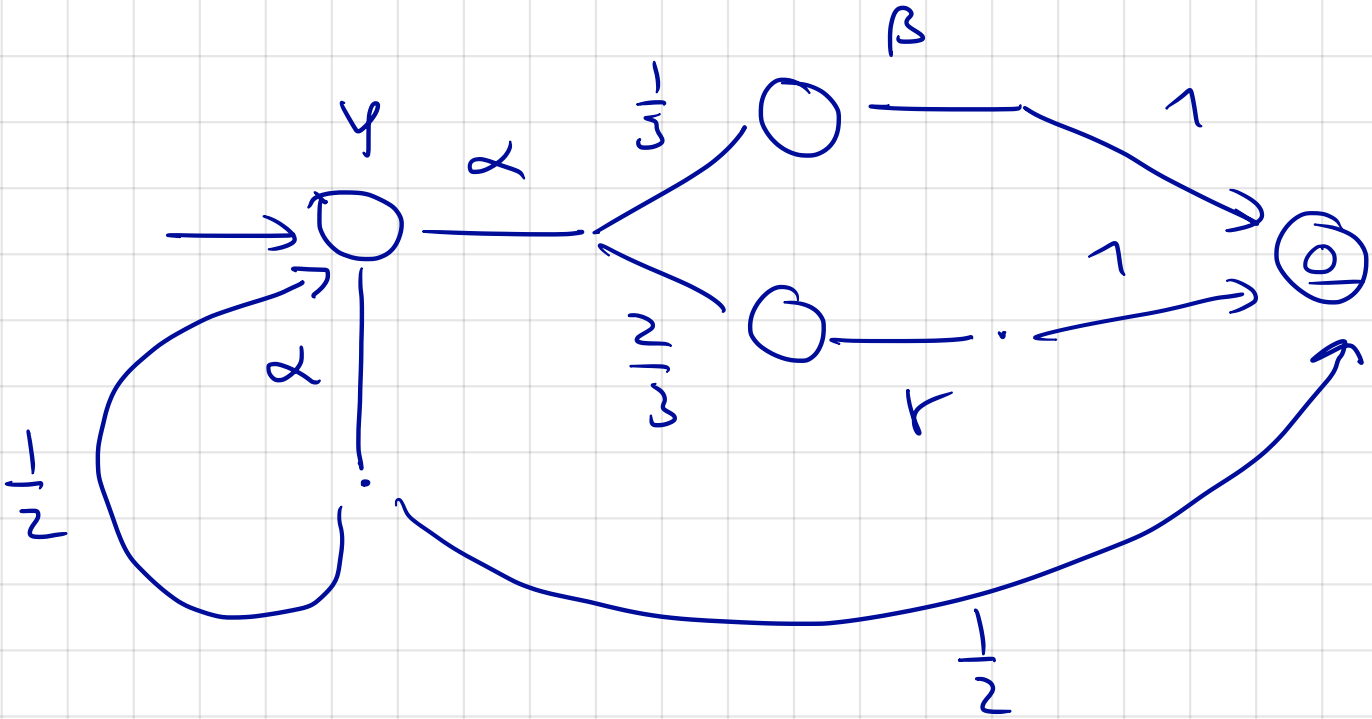
$$\frac{\alpha.(\underline{0} \oplus_{\frac{1}{2}} Y) \xrightarrow{\alpha} V}{X + \alpha.(\underline{0} \oplus_{\frac{1}{2}} Y) \xrightarrow{\alpha} V}$$

$V(\underline{0}) = \frac{1}{2}$

$V(Y) = \frac{1}{2}$

$Y = X + \alpha \ldots$

$$Y \xrightarrow{\alpha} V$$



Expansion law : "parallel composition is syntactic sugar"

let I and J be finite index sets ; and for $i \in I$ let K_i be a finite index set, $j \in J$, M_j be too.

For $$P = \sum_{i \in I} \alpha_i \left(\sum_{k_i \in K_i} [p_{k_i}] P_{k_i} \right)$$

$$Q = \sum_{j \in J} \beta_j \left(\sum_{m_j \in M_j} [q_{m_j}] Q_{m_j} \right)$$

Then $P \parallel Q =$ — synchronisation of α_i and β_j

$$\sum_{(i,j) \in I \times J \,|\, r(\alpha_i, \beta_j) = c_{ij}} c_{ij} \cdot \left(\sum_{k_i, m_j \in K_i \times M_j} \underbrace{[p_{k_i} \cdot q_{m_j}]}_{\text{product distribution}} \left(P_{k_i} \parallel Q_{m_j} \right) \right)$$

$$+ \sum_{i \in I} \alpha_i \left(\sum_{k_i \in K_i} [p_{k_i}] \left(P_{k_i} \parallel Q \right) \right)$$

— P performs α_i autonomously

$$+ \sum_{j \in J} \beta_j \left(\sum_{m_j \in M_j} [q_{m_j}] \left(P \parallel Q_{m_j} \right) \right)$$

— Q performs β_j autonomously