Silvia S. Pelozo
Becaria doctoral de CONICET (Tipo I)
Licenciada en Sistemas (UNNE)

Inicio del doctorado Abril de 2010

Grupo de Sistemas Dependibles

Tema Model checking probabilista para el análisis de propiedades del estado de régimen

Comisión de doctorado

- Pedro R. D'Argenio [Director]
- Ricardo J. Corin
- Laura Alonso i Alemany
- Héctor L. Gramaglia [Suplente]

Reasoning about security on distributed probabilistic systems through bounded-reachability

Silvia S. Pelozo

SUPERVISOR: PEDRO R. D'ARGENIO

Córdoba, 2010-12-06

UNC Universidad Nacional de Córdoba

CONICET

Our problem

$$\left.\begin{array}{l}\text{Distributed systems}\\ +\ \text{random behavior}\\ +\ \text{privacy of components}\end{array}\right\} \xrightarrow{\text{model checking}} \left[\begin{array}{l} P\left(\Diamond\mathrm{GOOD}\right)\\ P\left(\Diamond\mathrm{BAD}\right)\end{array}\right.$$

Our problem

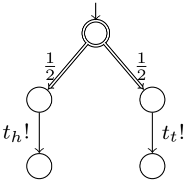
$$\left.\begin{array}{l}\text{Distributed systems}\\ +\ \text{random behavior}\\ +\ \text{privacy of components}\end{array}\right\} \xrightarrow{\text{model checking}} \left[\begin{array}{l}P\left(\Diamond\textsc{good}\right)\\ P\left(\Diamond\textsc{bad}\right)\end{array}\right.$$

Example

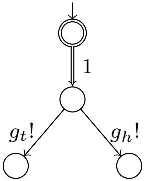
Player T tosses a coin

Player G tries to guess

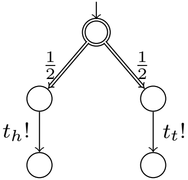
Player T



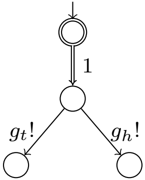
Player G

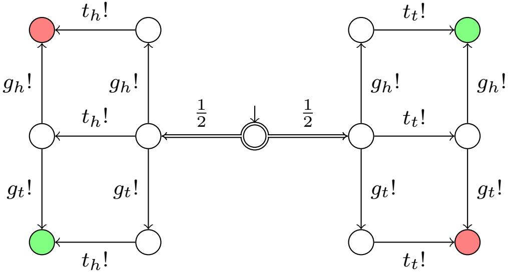


Player T



Player G





Formal model

$$\langle S, \quad \hat{s}, \ A, \ \rightarrow, \ \Rightarrow \rangle$$

Formal model

$$\langle S,\ \ \hat{s},\ \ A,\ \ \rightarrow,\ \ \Rightarrow \rangle$$

finite set of states

$\in S$ initial state

finite set of actions partitioned in inputs A_I and outputs A_O

$\subseteq S \times A \times S$ set of interactive transitions

Formal model

$$\langle S,\ \ \hat{s},\ \ A,\ \ \rightarrow,\ \ \Rightarrow \rangle$$

finite set
of states

$\in S$ initial
state

finite set of actions
partitioned in inputs
A_I and outputs A_O

$\subseteq S \times A \times S$ set
of interactive
transitions

$S \rightharpoonup Dist(S)$ set
of probabilistic
transitions

We require:

$$Dom\,(\rightarrow) \cap Dom\,(\Rightarrow) = \emptyset$$

Input enabledness:

$$\forall s \in S, a \in A_I : \exists s' \in S : s \xrightarrow{a} s'$$

Input determinism:

$$\forall s \in S, a \in A_I : \exists!\; s' \in S : s \xrightarrow{a} s'$$

Output isolation:

$$\forall s \in S, a', a'' \in A_O : s \xrightarrow{a'} s' \wedge s \xrightarrow{a''} s'' \\ \implies a' = a'' \wedge s' = s''$$

Parallel Composition

$$\mathcal{P} \text{ and } \mathcal{Q} \text{ are composable if } A_O^{\mathcal{P}} \cap A_O^{\mathcal{Q}} = \emptyset$$

$\mathcal{C} := \mathcal{P} \parallel \mathcal{Q}$ will be:

$$\left\langle S^{\mathcal{P}} \times S^{\mathcal{Q}}, (\hat{s}_{\mathcal{P}}, \hat{s}_{\mathcal{Q}}), A_I^{\mathcal{C}} \cup A_O^{\mathcal{C}}, \rightarrow_{\mathcal{C}}, \Rightarrow_{\mathcal{C}} \right\rangle$$

where:

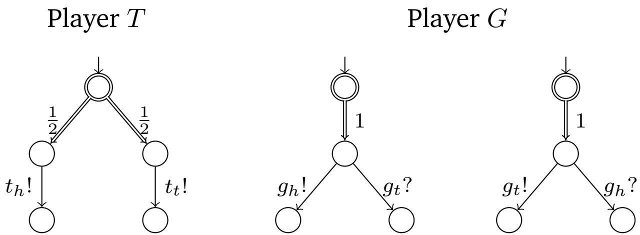
$$A_O^{\mathcal{C}} := A_O^{\mathcal{P}} \cup A_O^{\mathcal{Q}} \quad ; \quad A_I^{\mathcal{C}} := \left(A_I^{\mathcal{P}} \cup A_I^{\mathcal{Q}}\right) \setminus A_O^{\mathcal{C}}$$

and:

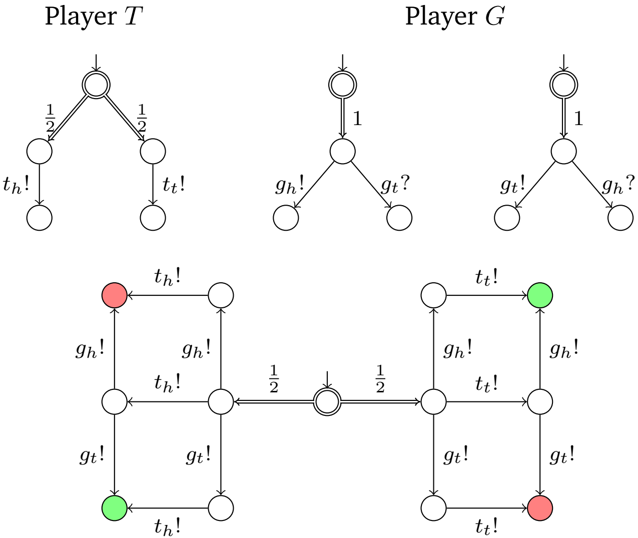
$$\frac{s \xrightarrow{a}_{\mathcal{P}} s'}{(s,t) \xrightarrow{a}_{\mathcal{C}} (s',t)} \quad a \notin A^{\mathcal{Q}} \qquad\qquad \frac{t \xrightarrow{a}_{\mathcal{Q}} t'}{(s,t) \xrightarrow{a}_{\mathcal{C}} (s,t')} \quad a \notin A^{\mathcal{P}}$$

$$\frac{s \xrightarrow{a}_{\mathcal{P}} s' \qquad t \xrightarrow{a}_{\mathcal{Q}} t'}{(s,t) \xrightarrow{a}_{\mathcal{C}} (s',t')} \qquad\qquad \frac{s \Rightarrow_{\mathcal{P}} \mu_s \qquad t \Rightarrow_{\mathcal{Q}} \mu_t}{(s,t) \Rightarrow_{\mathcal{C}} \mu_s \times \mu_t}$$

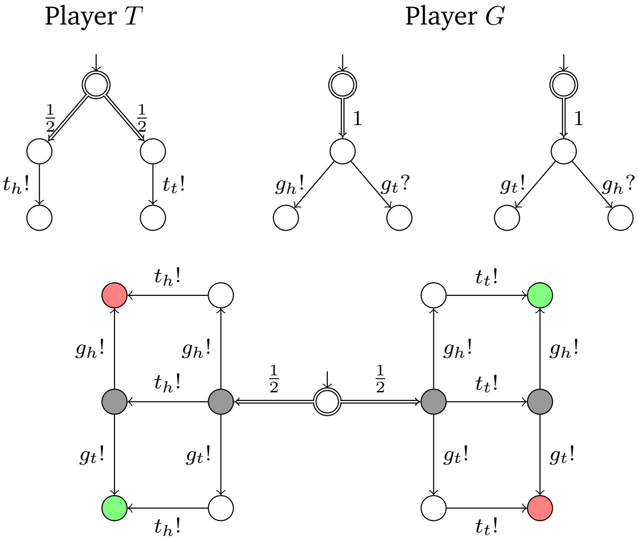
Can be extended to any finite set $\mathcal{C}$.



Player T
Player G
$\frac{1}{2}$
$\frac{1}{2}$
$t_h!$
$t_t!$
1
$g_h!$
$g_t?$
1
$g_t!$
$g_h?$



Player T
Player G
$\frac{1}{2}$
$\frac{1}{2}$
$t_h!$
$t_t!$
1
1
$g_h!$
$g_t?$
$g_t!$
$g_h?$
$t_h!$
$t_t!$
$g_h!$
$g_h!$
$g_h!$
$g_h!$
$t_h!$
$\frac{1}{2}$
$\frac{1}{2}$
$t_t!$
$g_t!$
$g_t!$
$g_t!$
$g_t!$
$t_h!$
$t_t!$


Player T
Player G
1/2
1/2
t_h!
t_t!
1
1
g_h!
g_t?
g_t!
g_h?
t_h!
t_t!
g_h!
g_h!
g_h!
g_h!
t_h!
1/2
1/2
t_t!
g_t!
g_t!
g_t!
g_t!
t_h!
t_t!

Resolution of non-determinism

A *finite path* of $\mathcal{C}$ is a sequence $s_0 a_0 s_1 a_1 \ldots a_{n-1} s_n$ where:

$$a_i \in A \text{ and } s_i \xrightarrow{a_i} s_{i+1}$$

or

$$a_i \in Dist\,(S)\,, s_i \Rightarrow a_i, \text{ and } a_i\,(s_{i+1}) > 0$$

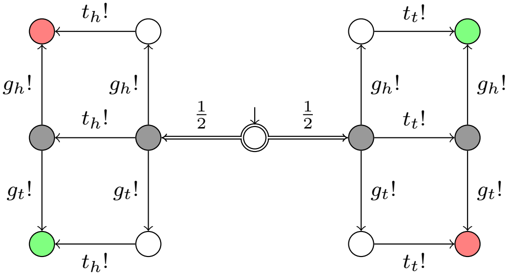
An *interleaving scheduler* is a function

$$\mathcal{I} : Paths\,(\mathcal{C}) \rightarrow Dist\,(\{\mathcal{P}_1, \ldots, \mathcal{P}_n\})$$

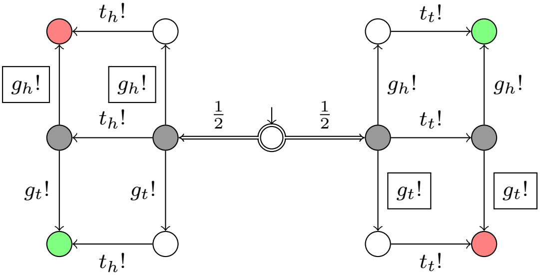
Defined for paths σ such that $last\,(\sigma)$ is vanishing:

$$\mathcal{I}\,(\sigma)\,(\mathcal{P}_i) > 0 \implies A^{en}_{last(\sigma),\mathcal{P}_i} \neq \emptyset$$

Why not all possible schedulers?



Why not all possible schedulers?



$$P\left(\Diamond \bigcirc\right) = 1$$

Distributed schedulers

[Giro and D'Argenio, 2009, Giro, 2010]

Projections

$\mathcal{C} = \mathcal{P}_1 \parallel \cdots \parallel \mathcal{P}_n$, $\sigma \in Paths\,(\mathcal{C})$, the projection $\sigma\,[\mathcal{P}_i]$ is:

$$(\hat{s}_{\mathcal{C}})\,[\mathcal{P}_i] = \pi_i\,(\hat{s}_{\mathcal{C}})$$

$$(\sigma a s)\,[\mathcal{P}_i] = \begin{cases} (\sigma)\,[\mathcal{P}_i] & \text{if } a \notin A^{\mathcal{P}} \\ (\sigma)\,[\mathcal{P}_i]\,a\,(\pi_i\,(s)) & \text{if } a \in A^{\mathcal{P}} \end{cases}$$

$$(\sigma\,(\mu_1 \times \cdots \times \mu_n)\,s)\,[\mathcal{P}_i] = (\sigma\,[\mathcal{P}_i])\,\mu_i\,(\pi_i\,(s))$$

where $\pi_i\,(s_1, \ldots, s_n) = s_i$.

Strongly distributed schedulers

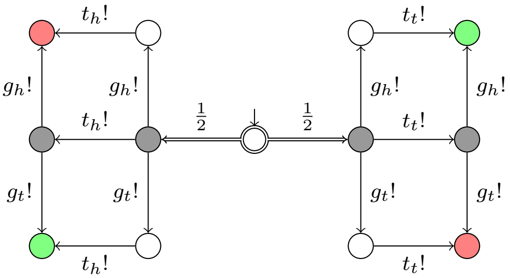
$\mathcal{I}$ of $\mathcal{C} = \mathcal{P}_1 \parallel \cdots \parallel \mathcal{P}_n$ is strongly distributed if:

$\forall \mathcal{P}_i, \mathcal{P}_j, \sigma, \sigma'$:

$$\left.\begin{array}{l} \sigma\left[\mathcal{P}_i\right] = \sigma'\left[\mathcal{P}_i\right] \\ \sigma\left[\mathcal{P}_j\right] = \sigma'\left[\mathcal{P}_j\right] \\ \mathcal{I}\left(\sigma\right)\left(\mathcal{P}_i\right) + \mathcal{I}\left(\sigma\right)\left(\mathcal{P}_j\right) \neq 0 \\ \mathcal{I}\left(\sigma'\right)\left(\mathcal{P}_i\right) + \mathcal{I}\left(\sigma'\right)\left(\mathcal{P}_j\right) \neq 0 \end{array}\right\} \implies$$

$$\implies \frac{\mathcal{I}\left(\sigma\right)\left(\mathcal{P}_i\right)}{\mathcal{I}\left(\sigma\right)\left(\mathcal{P}_i\right) + \mathcal{I}\left(\sigma\right)\left(\mathcal{P}_j\right)} = \frac{\mathcal{I}\left(\sigma'\right)\left(\mathcal{P}_i\right)}{\mathcal{I}\left(\sigma'\right)\left(\mathcal{P}_i\right) + \mathcal{I}\left(\sigma'\right)\left(\mathcal{P}_j\right)}$$

Is the problem solved?



$$\sigma\left[\mathcal{G}_h\right] = \sigma'\left[\mathcal{G}_h\right] \wedge \sigma\left[\mathcal{G}_t\right] = \sigma'\left[\mathcal{G}_t\right]$$

$$\Longrightarrow \frac{\mathcal{I}\left(\sigma\right)\left(\mathcal{G}_h\right)}{\mathcal{I}\left(\sigma\right)\left(\mathcal{G}_h\right) + \mathcal{I}\left(\sigma\right)\left(\mathcal{G}_t\right)} = \frac{\mathcal{I}\left(\sigma'\right)\left(\mathcal{G}_t\right)}{\mathcal{I}\left(\sigma'\right)\left(\mathcal{G}_h\right) + \mathcal{I}\left(\sigma'\right)\left(\mathcal{G}_t\right)}$$

But...

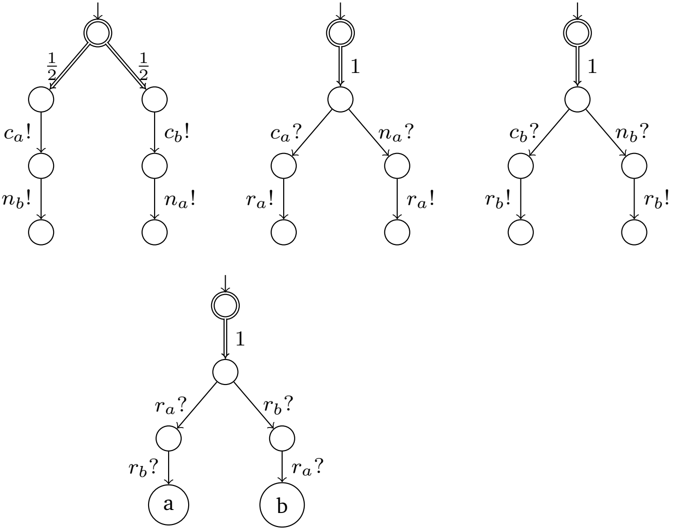
Unbounded reachability is undecidable [Giro and D'Argenio, 2007]

:-(

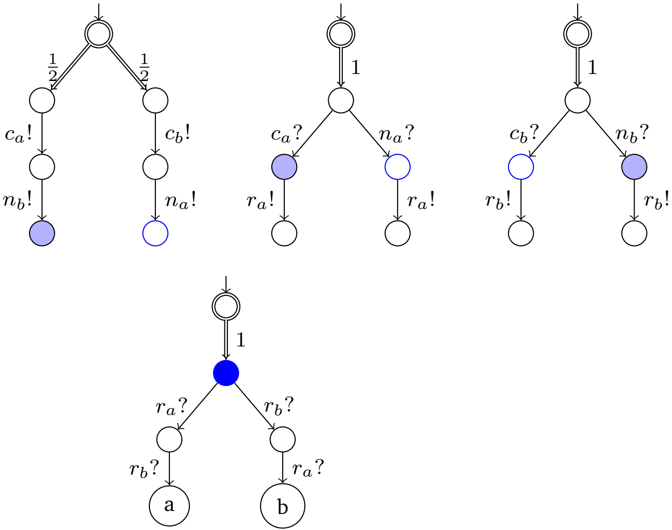
Bounded reachability IS decidable [Calin et al., 2010]:

Throught parametric interpretation, unfolding, and non-linear constrains
$\rightsquigarrow$ reduces to a non-linear programming problem

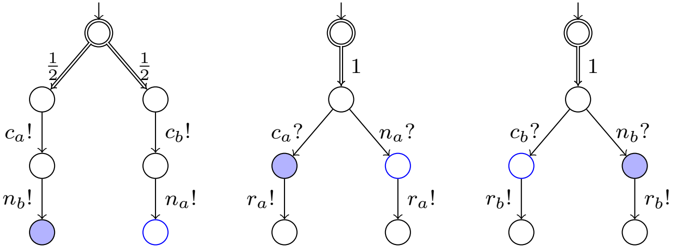
Anyway, they are sometimes still too powerful...

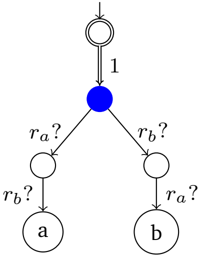


1/2
1/2
$c_a!$
$n_b!$
$c_b!$
$n_a!$
1
$c_a?$
$n_a?$
$r_a!$
$r_a!$
1
$c_b?$
$n_b?$
$r_b!$
$r_b!$
1
$r_a?$
$r_b?$
$r_b?$
$r_a?$
a
b



$\frac{1}{2}$
$\frac{1}{2}$
$c_a!$
$c_b!$
$n_b!$
$n_a!$
1
$c_a?$
$n_a?$
$r_a!$
$r_a!$
1
$c_b?$
$n_b?$
$r_b!$
$r_b!$
1
$r_a?$
$r_b?$
$r_b?$
$r_a?$
a
b





$$\sigma_{\bullet}(\mathcal{A}) \neq \sigma_{\circ}(\mathcal{A})\,;\sigma_{\bullet}(\mathcal{B}) \neq \sigma_{\circ}(\mathcal{B}) \implies$$

$$\mathcal{I}(\sigma_{\bullet})(\mathcal{A}) = 1, \mathcal{I}(\sigma_{\bullet})(\mathcal{B}) = 0$$

$$\mathcal{I}(\sigma_{\circ})(\mathcal{A}) = 0, \mathcal{I}(\sigma_{\circ})(\mathcal{B}) = 1$$

is a valid scheduler

Projection up to secrecy equivalence

Given:

$\mathcal{C} = \mathcal{P}_1 \parallel \cdots \parallel \mathcal{P}_n$

a path $\sigma \in Paths\left(\mathcal{C}\right)$

equivalence relations $\sim \subseteq S_i, \approx \subseteq A_i$ $(i = 1, \ldots, n)$

Projection $\left[\sigma\left[\mathcal{P}_i\right]\right]_\sim$ of σ is:

$$\left[\left(\hat{s}_\mathcal{C}\right)\left[\mathcal{P}_i\right]\right]_\sim = \left[\pi_i\left(\hat{s}_\mathcal{C}\right)\right]_\sim$$

$$\left[\left(\sigma a s\right)\left[\mathcal{P}_i\right]\right]_\sim = \begin{cases} \left[\left(\sigma\right)\left[\mathcal{P}_i\right]\right]_\sim & \text{if } a \notin A_{\mathcal{P}_i} \\ \left[\left(\sigma\right)\left[\mathcal{P}_i\right]\right]_\sim \left[a\right]_\approx \left[\pi_i\left(s\right)\right]_\sim & \text{if } a \in A_{\mathcal{P}_i} \end{cases}$$

$$\left[\left(\sigma\left(\mu_1 \times \cdots \times \mu_n\right) s\right)\left[\mathcal{P}_i\right]\right]_\sim = \left[\left(\sigma\left[\mathcal{P}_i\right]\right)\right]_\sim \mu_i\left(\left[\pi_i\left(s\right)\right]_\sim\right)$$

$$\mu_i\left(\left[s\right]_\sim\right) = \sum_{s' \in [s]_\sim} \mu_i\left(s'\right)$$

Distributed scheduler with secrecy

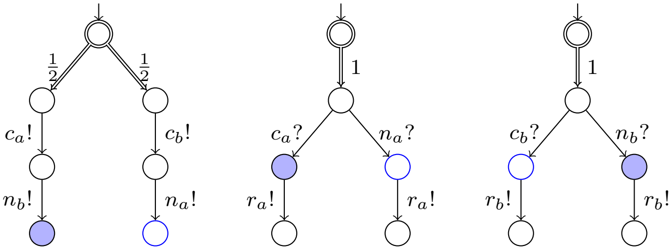
$\mathcal{I}$ of $\mathcal{C} = \mathcal{P}_1 \parallel \cdots \parallel \mathcal{P}_n$ such that

$\forall \mathcal{P}_i, \mathcal{P}_j, \sigma, \sigma'$:

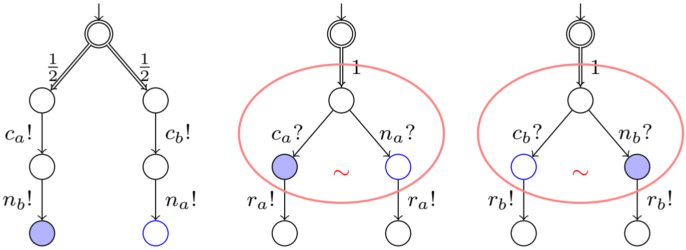
$$\begin{array}{c} [\sigma\,[\mathcal{P}_i]]_\sim = [\sigma'\,[\mathcal{P}_i]]_\sim \\ [\sigma\,[\mathcal{P}_j]]_\sim = [\sigma'\,[\mathcal{P}_j]]_\sim \end{array} \qquad \left.\begin{array}{c} \mathcal{I}\,(\sigma)\,(\mathcal{P}_i) \\ \mathcal{I}\,(\sigma)\,(\mathcal{P}_j) \\ \mathcal{I}\,(\sigma')\,(\mathcal{P}_i) \\ \mathcal{I}\,(\sigma')\,(\mathcal{P}_j) \end{array}\right\} \neq 0$$

$$\Downarrow$$

$$\frac{\mathcal{I}\,(\sigma)\,(\mathcal{P}_i)}{\mathcal{I}\,(\sigma)\,(\mathcal{P}_i) + \mathcal{I}\,(\sigma)\,(\mathcal{P}_j)} = \frac{\mathcal{I}\,(\sigma')\,(\mathcal{P}_i)}{\mathcal{I}\,(\sigma')\,(\mathcal{P}_i) + \mathcal{I}\,(\sigma')\,(\mathcal{P}_j)}$$



$\frac{1}{2}$
$\frac{1}{2}$
$c_a!$
$c_b!$
$n_b!$
$n_a!$
1
$c_a?$
$n_a?$
$r_a!$
$r_a!$
1
$c_b?$
$n_b?$
$r_b!$
$r_b!$



$$[\sigma_{\bullet}(\mathcal{A})]_{\sim} = [\sigma_{\circ}(\mathcal{A})]_{\sim} \wedge [\sigma_{\bullet}(\mathcal{B})]_{\sim} = [\sigma_{\circ}(\mathcal{B})]_{\sim}$$

$$\Downarrow$$

$$\mathcal{I}(\sigma_{\bullet})(\mathcal{A}) = 1, \mathcal{I}(\sigma_{\bullet})(\mathcal{B}) = 0$$

$$\mathcal{I}(\sigma_{\circ})(\mathcal{A}) = 0, \mathcal{I}(\sigma_{\circ})(\mathcal{B}) = 1$$

is NOT a valid scheduler

Closing remarks

In verification of distributed systems with *random behavior* + *privacy concerns*

$\rightarrow$ traditional probabilistic model-checking techniques are inadequate

Distributed schedulers work better

+ realistic bounds for probabilities
– undecidable in general
+ bounded reachability is decidable $\rightsquigarrow$ non-linear programming problem
– too powerful in some cases

We introduce *secrecy*

– some drawbacks of distributed schedulers
+ even more realistic results
+ also reducible to non-linear program
! some validation pending

References

[Calin et al., 2010] Calin, G., Crouzen, P., D'Argenio, P., Hahn, E., and Zhang, L. (2010). Time-bounded reachability in distributed input/output interactive probabilistic chains. In van de Pol, J. and Weber, M., editors, *Model Checking Software*, volume 6349 of *Lecture Notes in Computer Science*, pages 193–211. Springer Berlin / Heidelberg. 10.1007/978-3-642-16164-3-15.

[Giro, 2010] Giro, S. (2010). *On the automatic verification of distributed probabilistic automata with partial information*. PhD thesis, FaMAF, UNC.

[Giro and D'Argenio, 2009] Giro, S. and D'Argenio, P. (2009). On the expressive power of schedulers in distributed probabilistic systems. *Electronic Notes in Theoretical Computer Science*, 253(3):45 – 71. Proceedings of Seventh Workshop on Quantitative Aspects of Programming Languages (QAPL 2009).

[Giro and D'Argenio, 2007] Giro, S. and D'Argenio, P. R. (2007). Quantitative model checking revisited: Neither decidable nor approximable. In Raskin, J.-F. and Thiagarajan, P. S., editors, *FORMATS*, volume 4763 of *LNCS*, pages 179–194. Springer.