Modelos para la descripción de sistemas temporizados estocásticos

Pedro R. D'Argenio

Cadenas de Markov de tiempo discreto (DTMC)

Una DTMC es una estructura

$$(S, \mathbf{P}, s_0, PA, L)$$

donde,

- S es un conjunto numerable de estados, siendo $s_0 \in S$ el estado incial,
- $\mathbf{P} : S \times S \to [0, 1]$ es la función de probabilidad de transición, tal que, para todo $s \in S$, $\sum_{s' \in S} \mathbf{P}(s, s') = 1$, y
- $L : S \to \mathscr{P}(PA)$ es la función de etiquetedo, donde PA es un conjunto de proposiciones atómicas.

Para model checking sólo vamos a considerar conjuntos finitos de estados

kov de tiempo discreto (DTMC)

Una DTMC es u estructura

$$(S, \mathbf{P}, s_0, PA, L)$$

$\mathbf{P}(s, s')$ es la probabilidad de pasar al estado s' dado que el sistema se encuentra en el estado s.

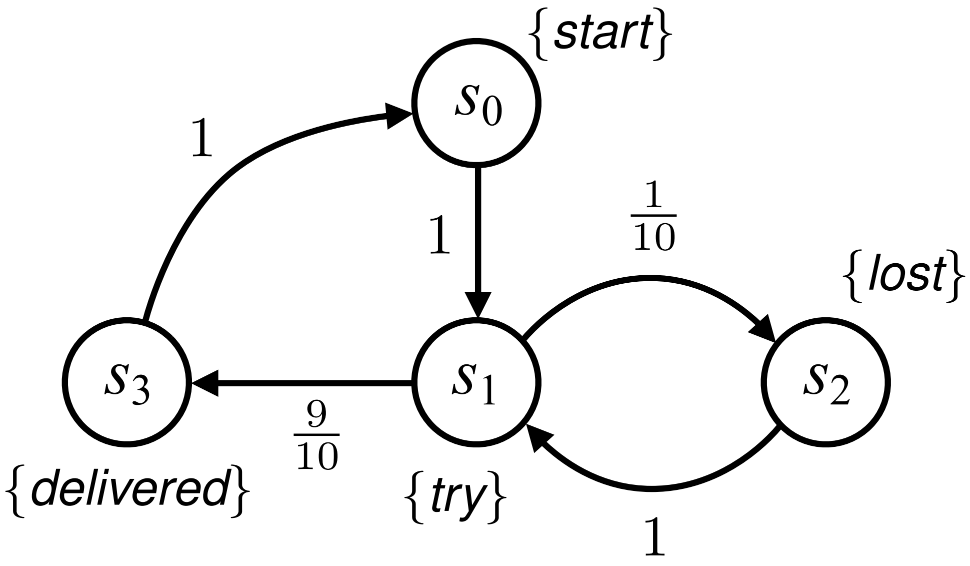
donde,

- S es un conjunto numerable de estados, siendo $s_0 \in S$ el estado incial,
- $\mathbf{P} : S \times S \to [0, 1]$ es la función de probabilidad de transición, tal que, para todo $s \in S$, $\sum_{s' \in S} \mathbf{P}(s, s') = 1$, y
- $L : S \to \mathscr{P}(PA)$ es la función de etiquetedo, donde PA es un conjunto de proposiciones atómicas.

CONICET

UNC

Un protocolo simple



$S = \{s_0, s_1, s_2, s_3\}$

s_0 es el estado inicial

$$\mathbf{P} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{10} & \frac{9}{10} \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

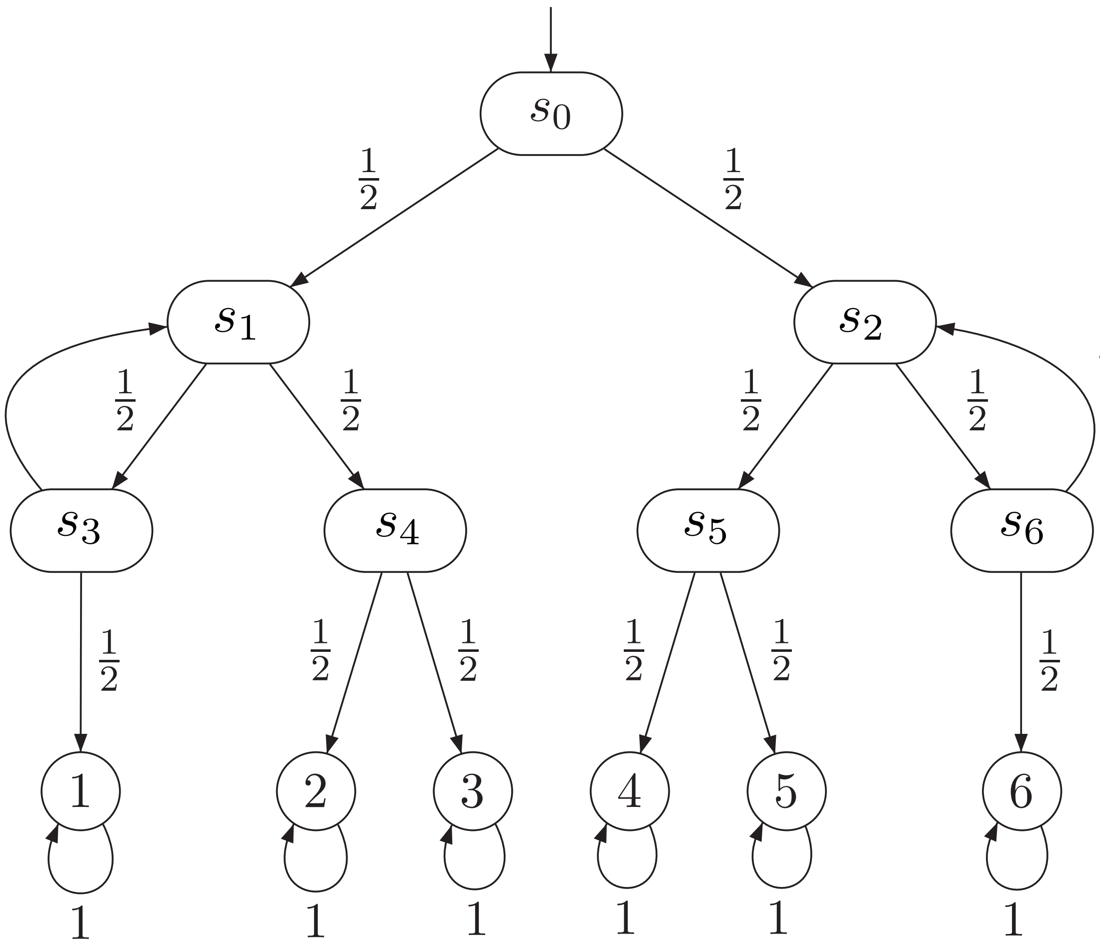
$PA = \{\textit{start}, \textit{try}, \textit{delivered}, \textit{lost}\}$

$L(s_0) = \{\textit{start}\}$
$L(s_1) = \{\textit{try}\}$
$L(s_2) = \{\textit{lost}\}$
$L(s_3) = \{\textit{delivered}\}$

CONICET

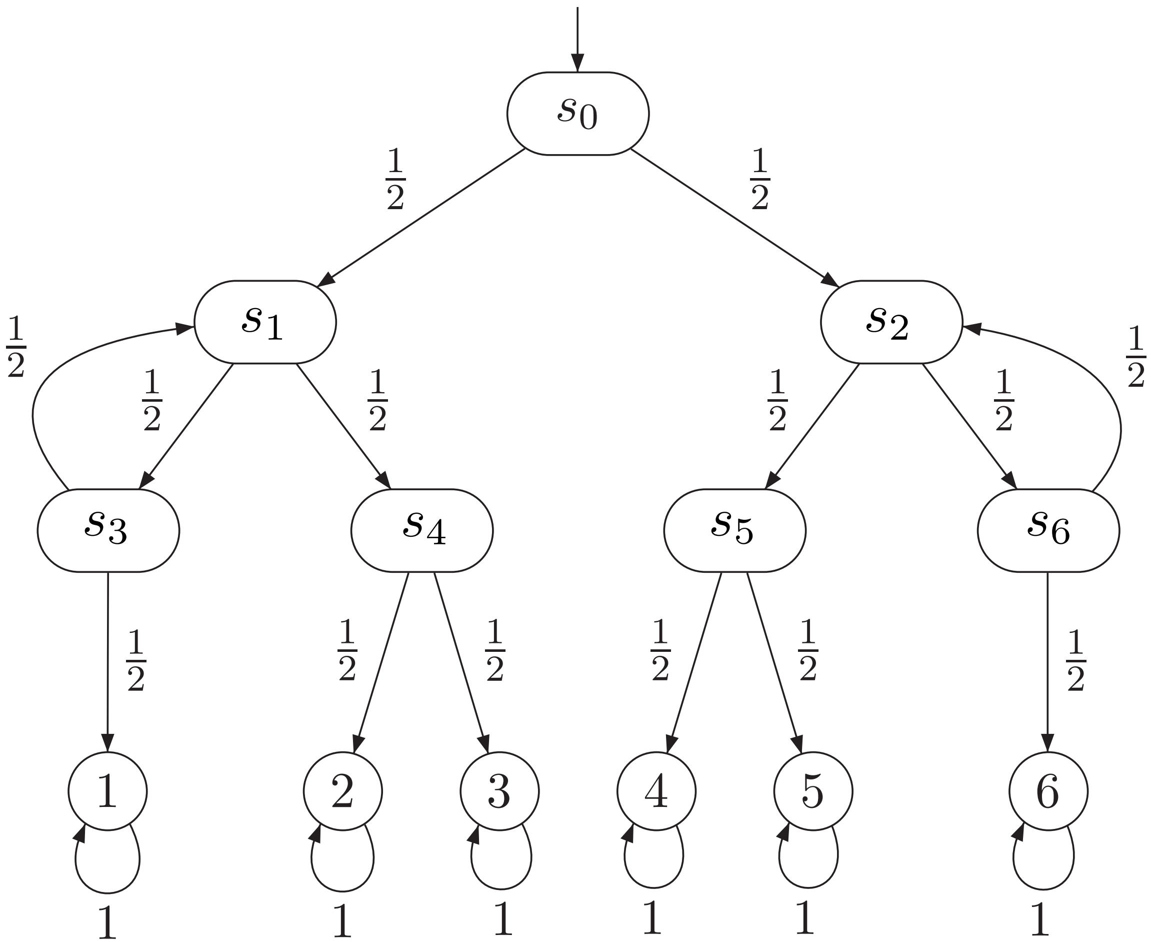
UNC

Simulando un dado con una moneda



¿$P(\mathtt{F}\,2)$?

Simulando un dado con una moneda



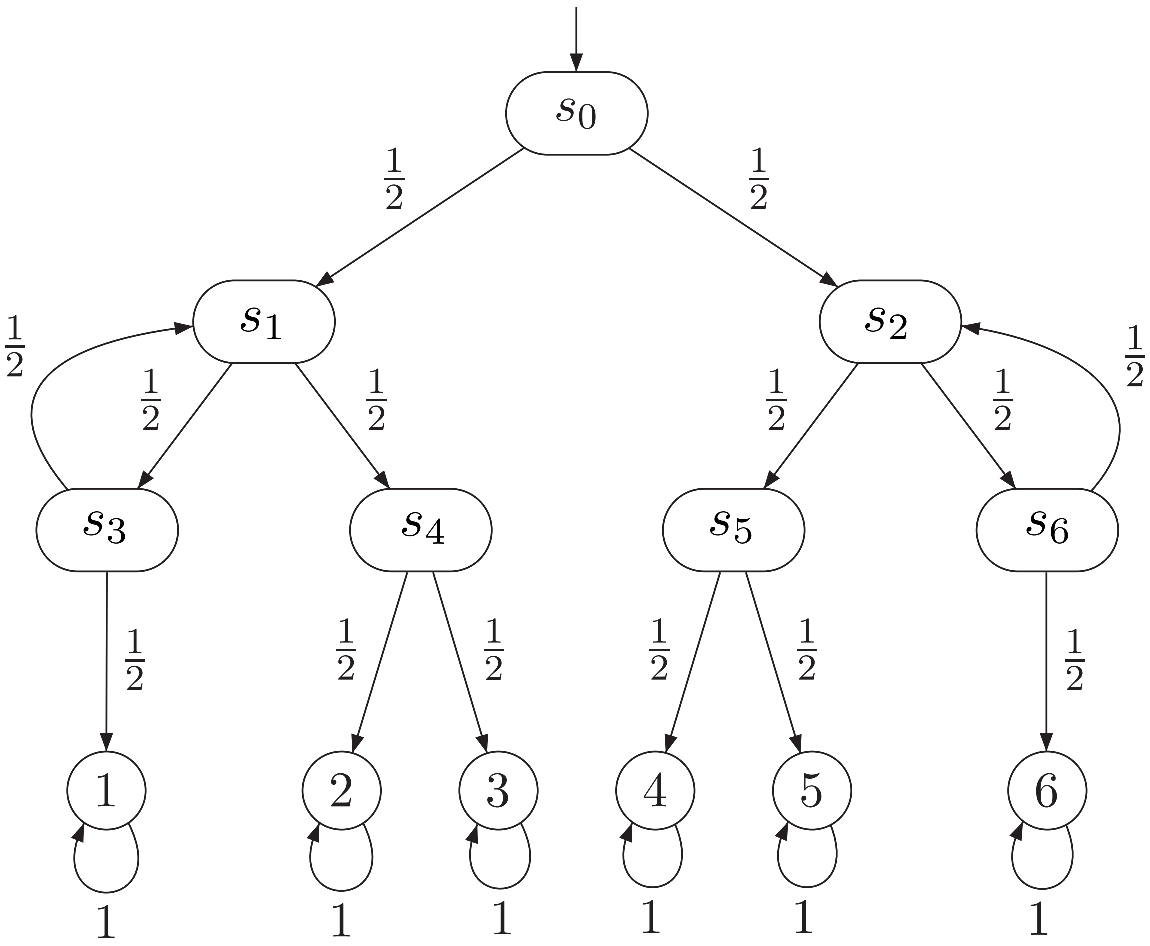
$$\underbrace{P(s_0 s_1 s_4 2)}_{} + P(s_0 s_1 s_3 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_3 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_3 s_1 s_3 s_1 s_4 2) + \cdots$$

$$\mathbf{P}(s_0, s_1) \cdot \mathbf{P}(s_1, s_4) \cdot \mathbf{P}(s_4, 2)$$

CONICET

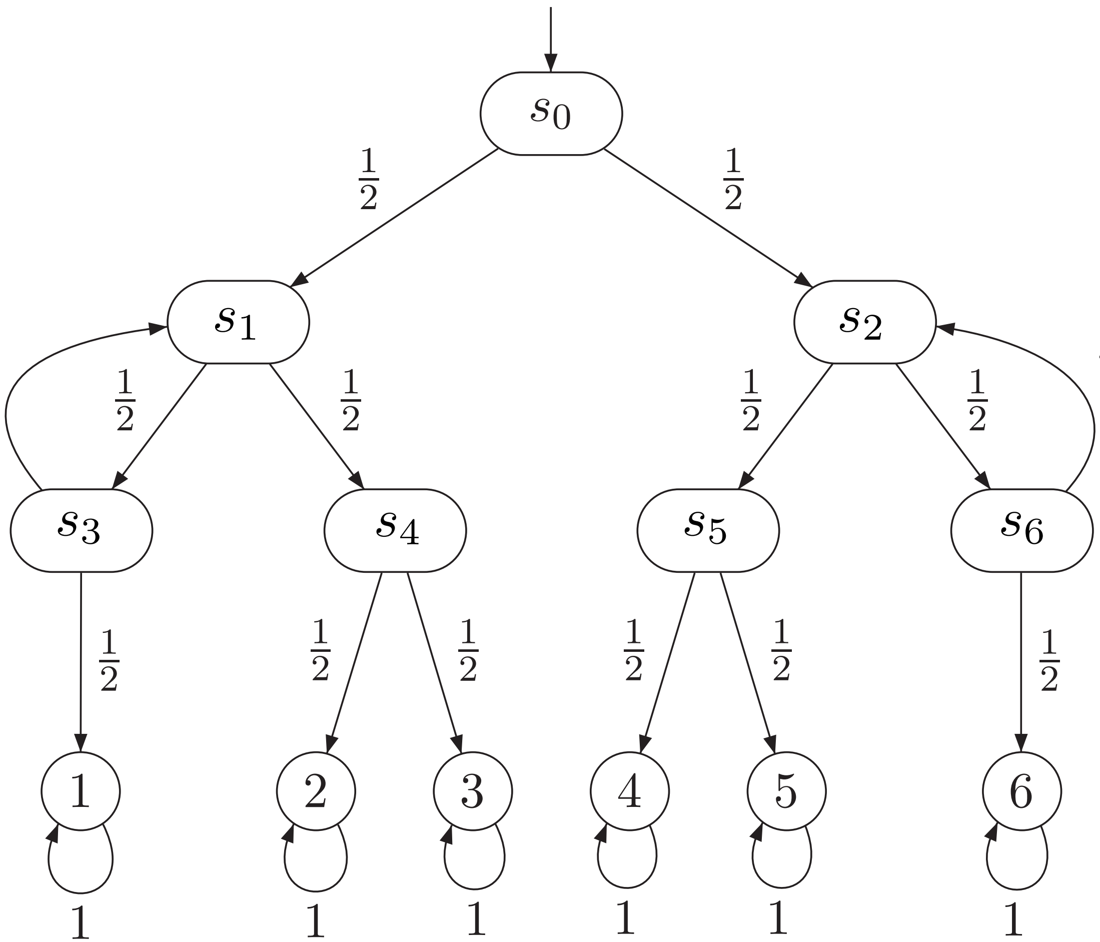
UNC

Simulando un dado con una moneda



$$\underbrace{P(s_0s_1s_42)}_{\frac{1}{8}} + \underbrace{P(s_0s_1s_3s_1s_42)}_{\frac{1}{32}} + \underbrace{P(s_0s_1s_3s_1s_3s_1s_42)}_{\frac{1}{128}} + \underbrace{P(s_0s_1s_3s_1s_3s_1s_3s_1s_42)}_{\frac{1}{512}} + \cdots$$

Simulando un dado con una moneda



$$P(s_0 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_3 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_3 s_1 s_3 s_1 s_4 2) + \cdots$$

$$\sum_{n \in \mathbb{N}} \frac{1}{2^{2n+3}} = \frac{1}{6}$$

Propiedades de alcanzabilidad

Formalmente, se soluciona a través del siguiente sistema de ecuaciones:

$$
\begin{array}{ll}
x_s = \displaystyle\sum_{t \in \boldsymbol{S} \setminus (\boldsymbol{S}^{=0} \cup \boldsymbol{B})} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t) & \text{si } s \in \boldsymbol{S} \setminus (\boldsymbol{S}^{=0} \cup \boldsymbol{B}) \\
x_s = 1 & \text{si } s \in B \\
x_s = 0 & \text{si } s \in \boldsymbol{S}^{=0}
\end{array}
$$

CONICET

UNC

Propiedades de alcanzabilidad

Formalmente, se soluciona a través del siguiente sistema de ecuaciones:

$$
\begin{aligned}
x_s &= \sum_{t \in \boldsymbol{S} \setminus (\boldsymbol{S}^{=0} \cup \boldsymbol{B})} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t) && \text{si } s \in \boldsymbol{S} \setminus (\boldsymbol{S}^{=0} \cup \boldsymbol{B}) \\
x_s &= 1 && \text{si } s \in B \\
x_s &= 0 && \text{si } s \in \boldsymbol{S}^{=0}
\end{aligned}
$$

Normalmente se utilizan los métodos de Jacobi o de Gauss-Seidel para converger a la solución

Estados que no alcanzan a B

CONICET

UNC

La necesidad del no-determinismo

- Composición Paralela / Componentes Distribuidas:
  - las probabilidades en una componente son fáciles de estimar
  - las probabilidades relativas entre eventos de distintas componentes dependen de un estado global impredecible
- Subespecificación:
  - algunas probabilidades pueden desconocerse al momento de modelado
- Abstracción:
  - los modelos son abstracciones del sistema en estudio
- Síntesis de controladores y planeamiento:
  - la subespecificación es intencional para sintetizar decisiones óptimas

CONICET

UNC

Procesos de Decisión de Markov (MDP)

Un MDP es una estructura

$$(S, Act, \mathbf{P}, s_0, PA, L)$$

donde

- S es un conjunto finito de estados, siendo $s_0 \in S$ el estado incial,
- Act es un conjunto finito de acciones,
- $\mathbf{P} : S \times Act \times S \to [0, 1]$ es la función de probabilidad de transición, tal que, para todo $s \in S$ y $\alpha \in Act$, $\sum_{s' \in S} \mathbf{P}(s, \alpha, s') \in \{0, 1\}$, y
- $L : S \to \mathscr{P}(PA)$ es la función de etiquetedo, donde PA es un conjunto de proposiciones atómicas.

e Decisión de Markov (MDP)

Si *Act* = {α} el MDP
es una DTMC

Un MDP es una estructura

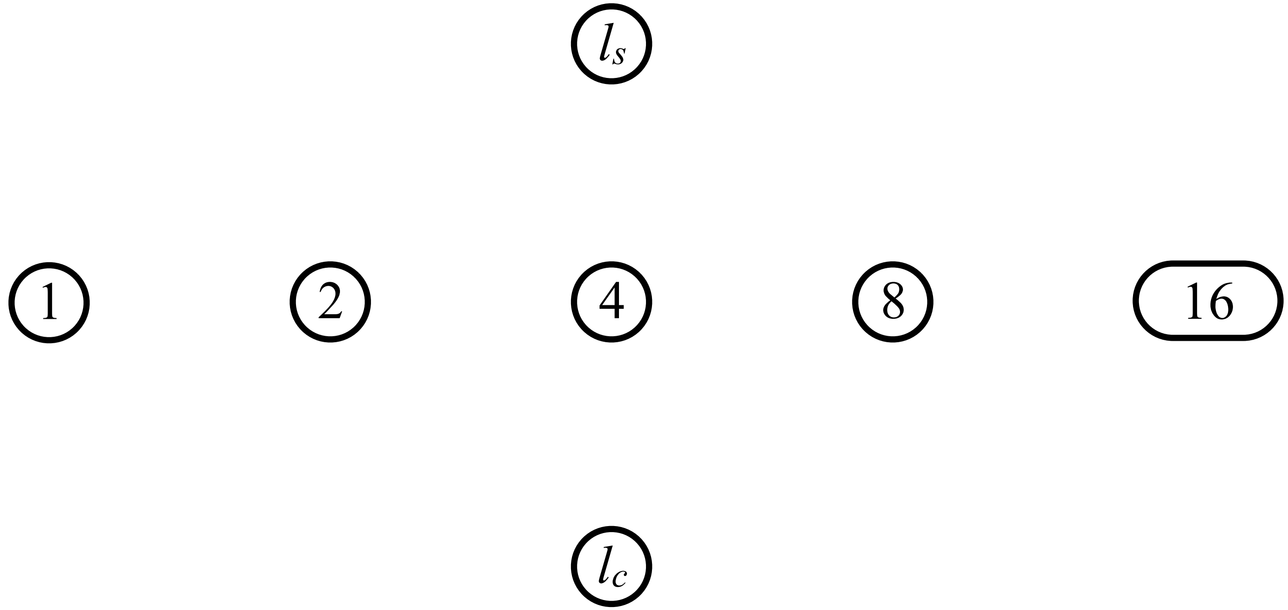
$$(S, Act, \mathbf{P}, s_0, PA, L)$$

$\mathbf{P}(s, \alpha, s')$ es la probabilidad de pasar al estado s' dado que el sistema se encuentra en el estado s y la acción α fue seleccionada para ejecutar.

donde

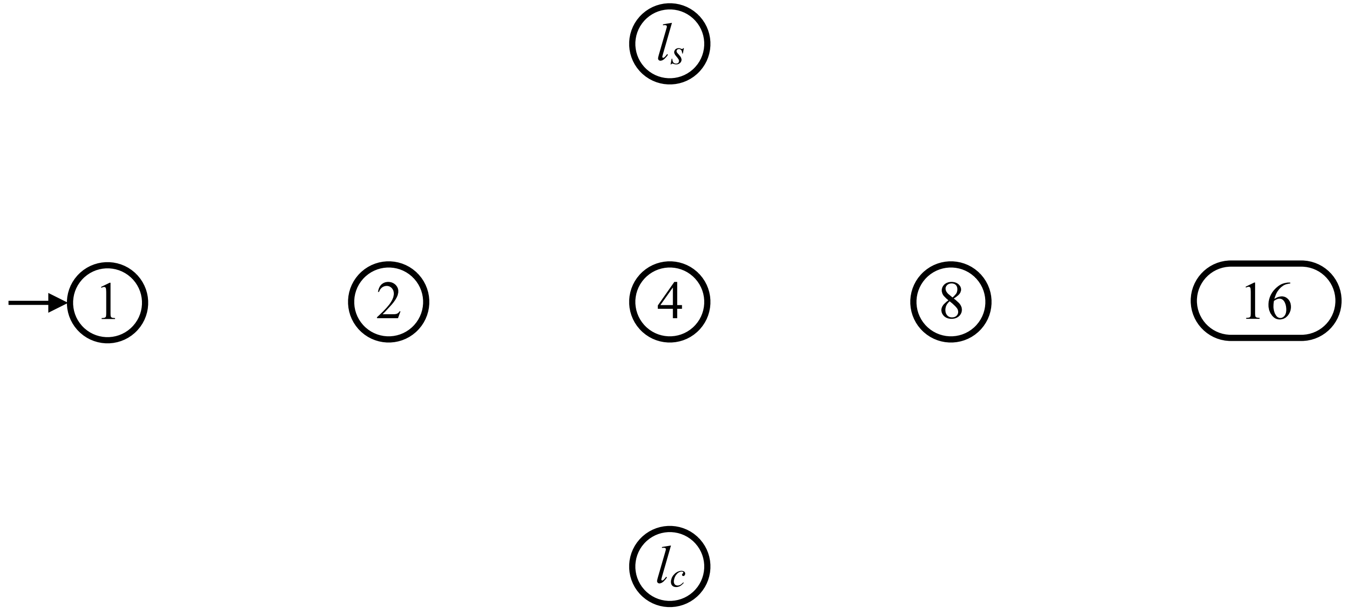
- S es un conjunto finito de estados, siendo $s_0 \in S$ el estado incial,
- Act es un conjunto finito de acciones,
- $\mathbf{P} : S \times Act \times S \to [0, 1]$ es la función de probabilidad de transición, tal que, para todo $s \in S$ y $\alpha \in Act$, $\sum_{s' \in S} \mathbf{P}(s, \alpha, s') \in \{0, 1\}$, y
- $L : S \to \mathscr{P}(PA)$ es la función de etiquetedo, donde PA es un conjunto de proposiciones atómicas.

Procesos de Decisión de Markov (MDP)



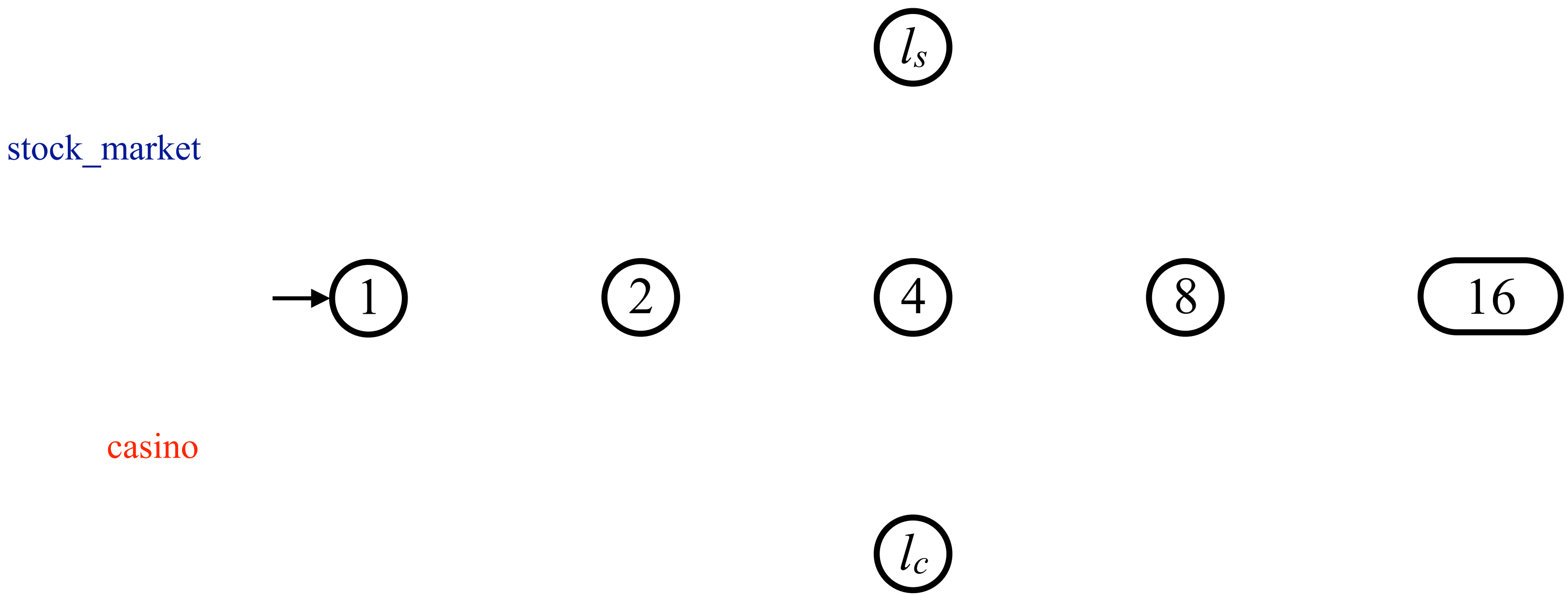
$$(S, Act, \mathbf{P}, s_0, PA, L)$$

Procesos de Decisión de Markov (MDP)



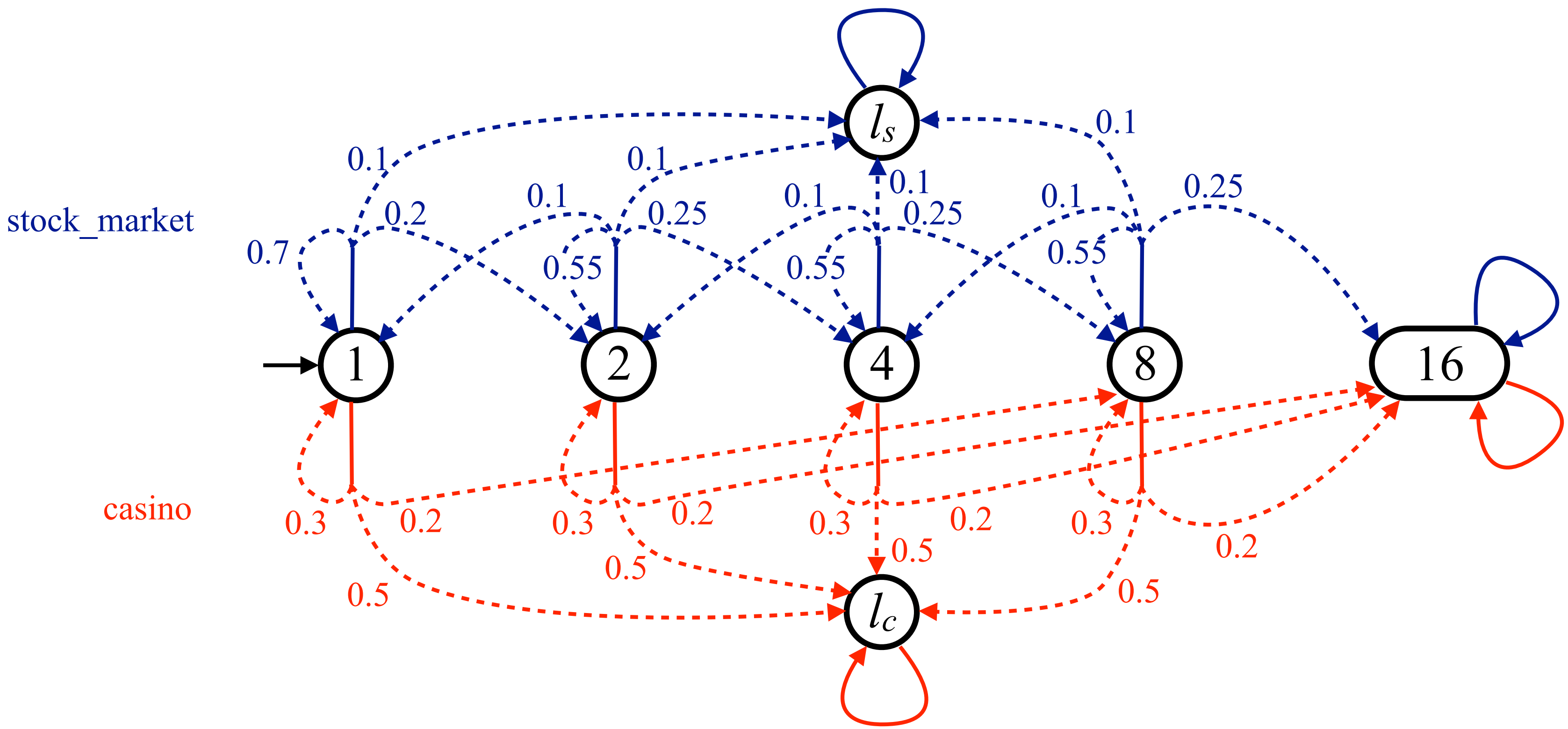
$$(S, Act, \mathbf{P}, s_0, PA, L)$$

Procesos de Decisión de Markov (MDP)



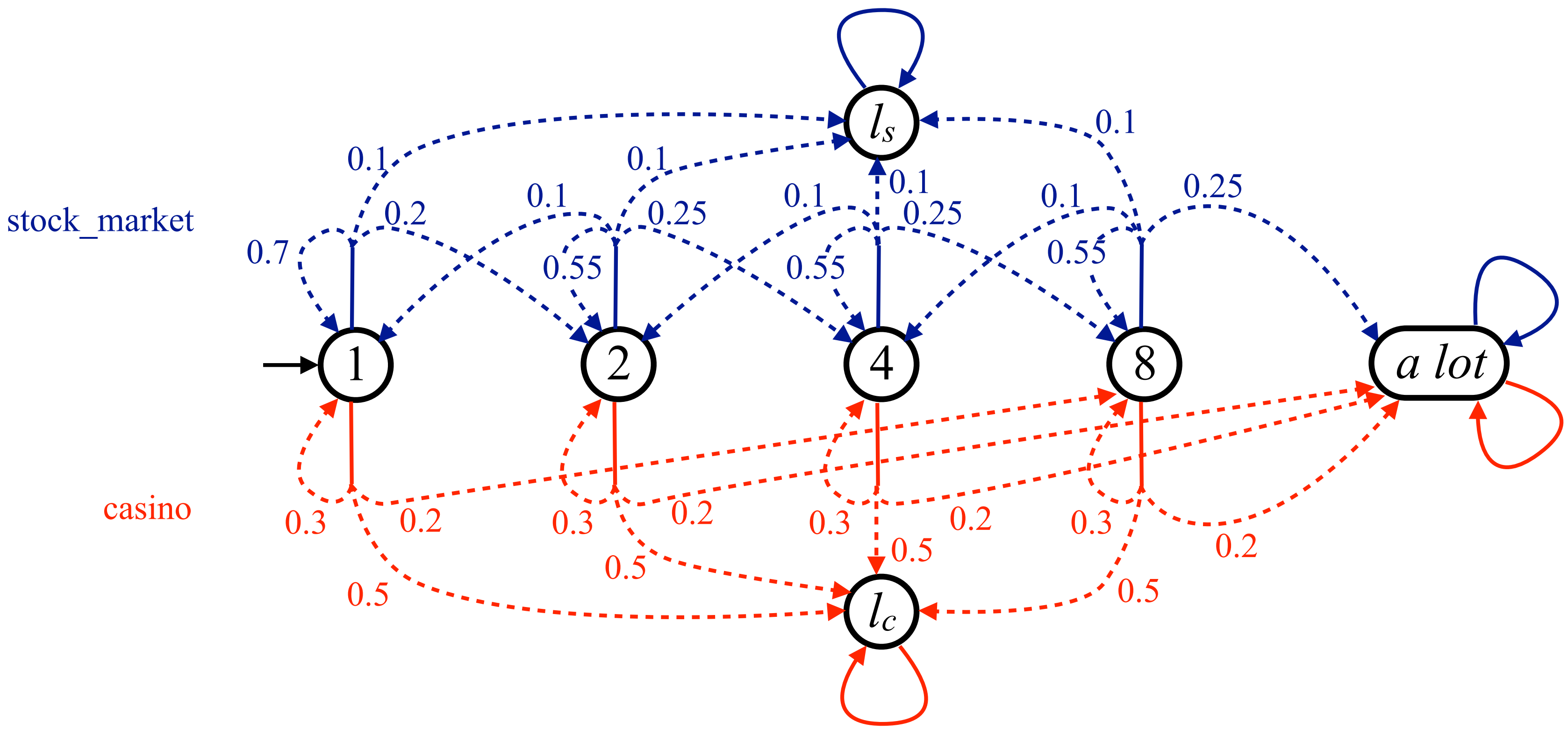
$$(S, Act, \mathbf{P}, s_0, PA, L)$$

Procesos de Decisión de Markov (MDP)



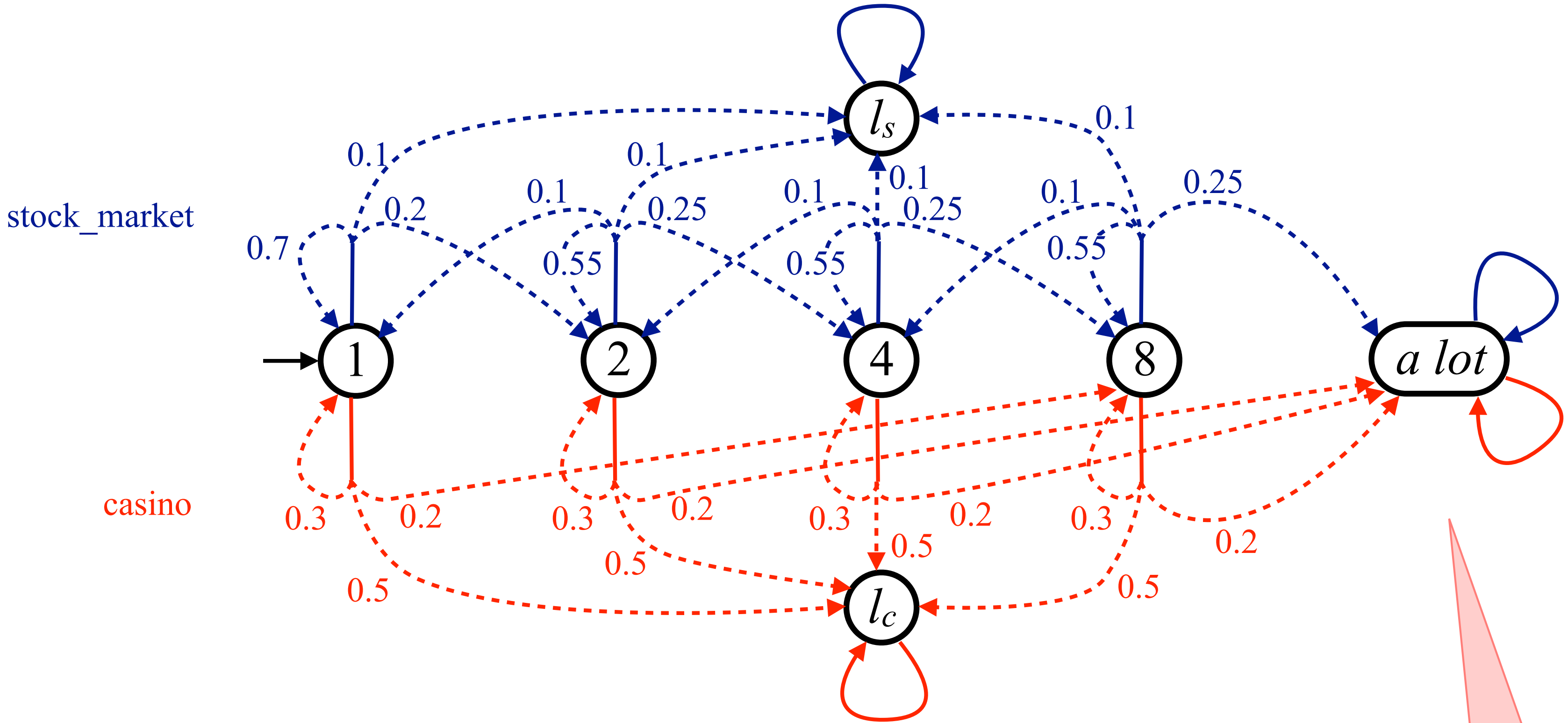
$$(S, Act, \mathbf{P}, s_0, PA, L)$$

Procesos de Decisión de Markov (MDP)



$$(S, Act, \mathbf{P}, s_0, PA, L)$$

Procesos de Decisión de Markov (MDP)

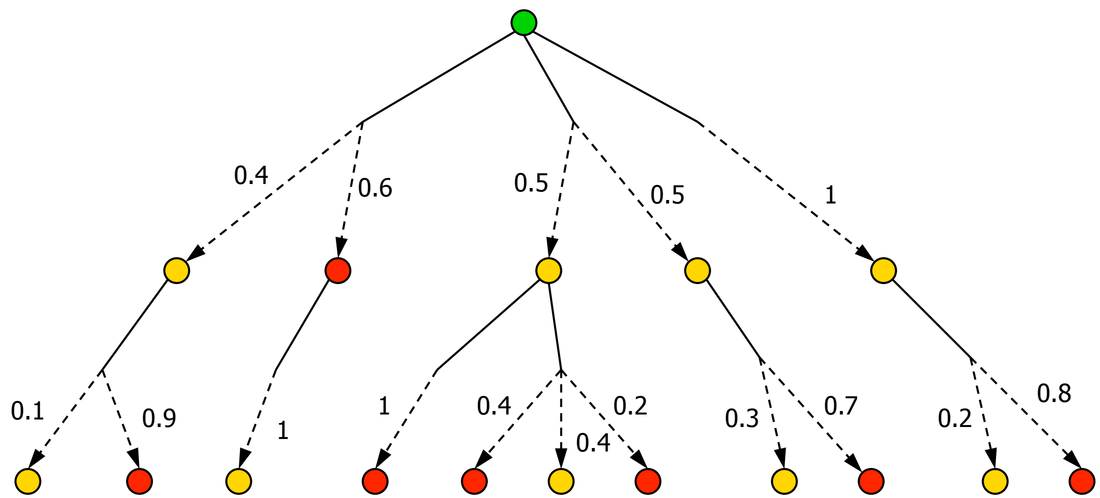


$$(S, Act, \mathbf{P}, s_0, PA, L)$$

¿Cuál es la probabilidad de $\mathtt{F}$ "*a lot*"?

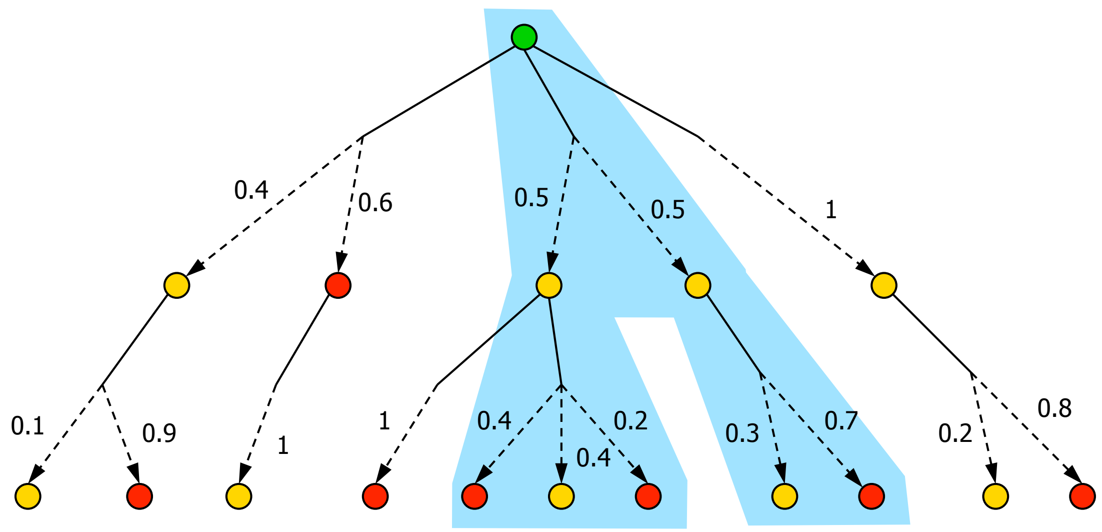
Resolución del no-determinismo

- Para calcular las probabilidades en un MDP, el no-determinismo necesita ser resuelto.
- Los schedulers (o adversarios) son funciones que eligen la siguiente acción a realizar teniendo en cuenta lo ejecutado.



Resolución del no-determinismo

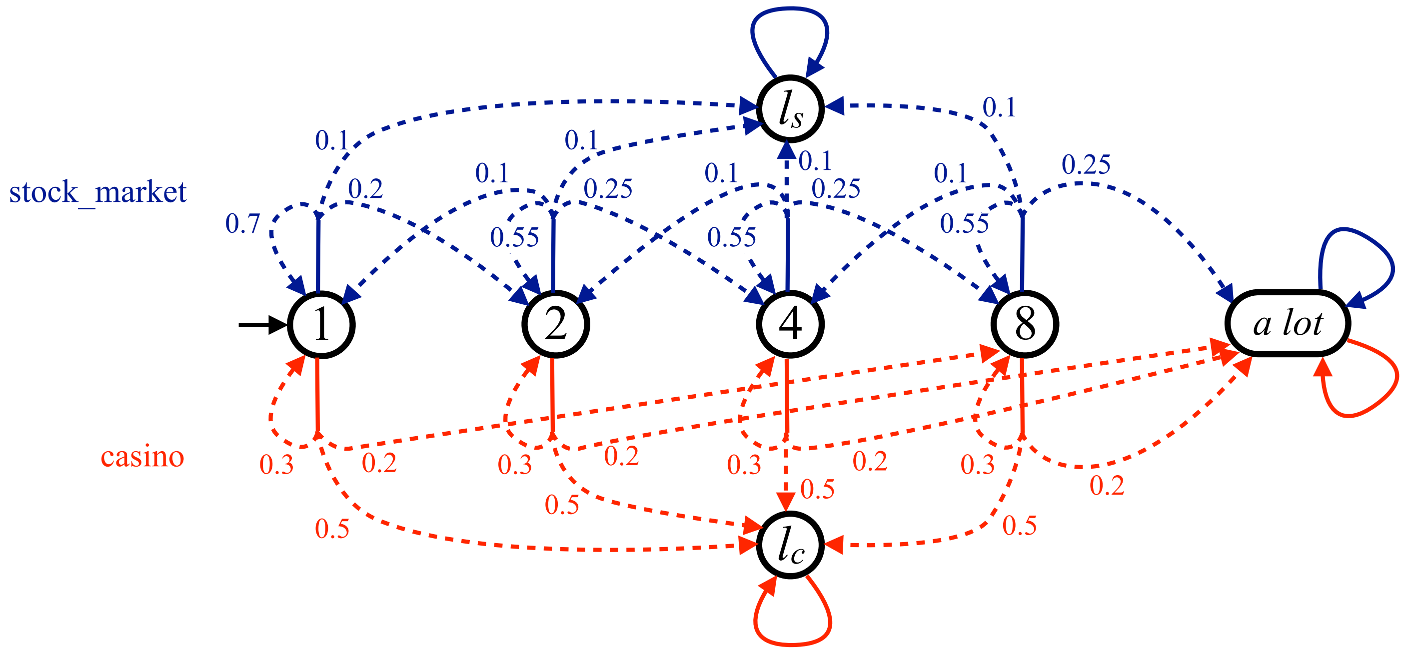
- Para calcular las probabilidades en un MDP, el no-determinismo necesita ser resuelto.
- Los schedulers (o adversarios) son funciones que eligen la siguiente acción a realizar teniendo en cuenta lo ejecutado.



Un scheduler permite construir una DTMC

(También hay schedulers que eligen con aleatoriedad)

Probabilidad inducida por un scheduler



$\mathfrak{S}$ elige siempre casino $\qquad \Pr^{\mathfrak{S}}(① \models \mathtt{F}\,\text{"}a\ lot\text{"}) \approx 0.0816$

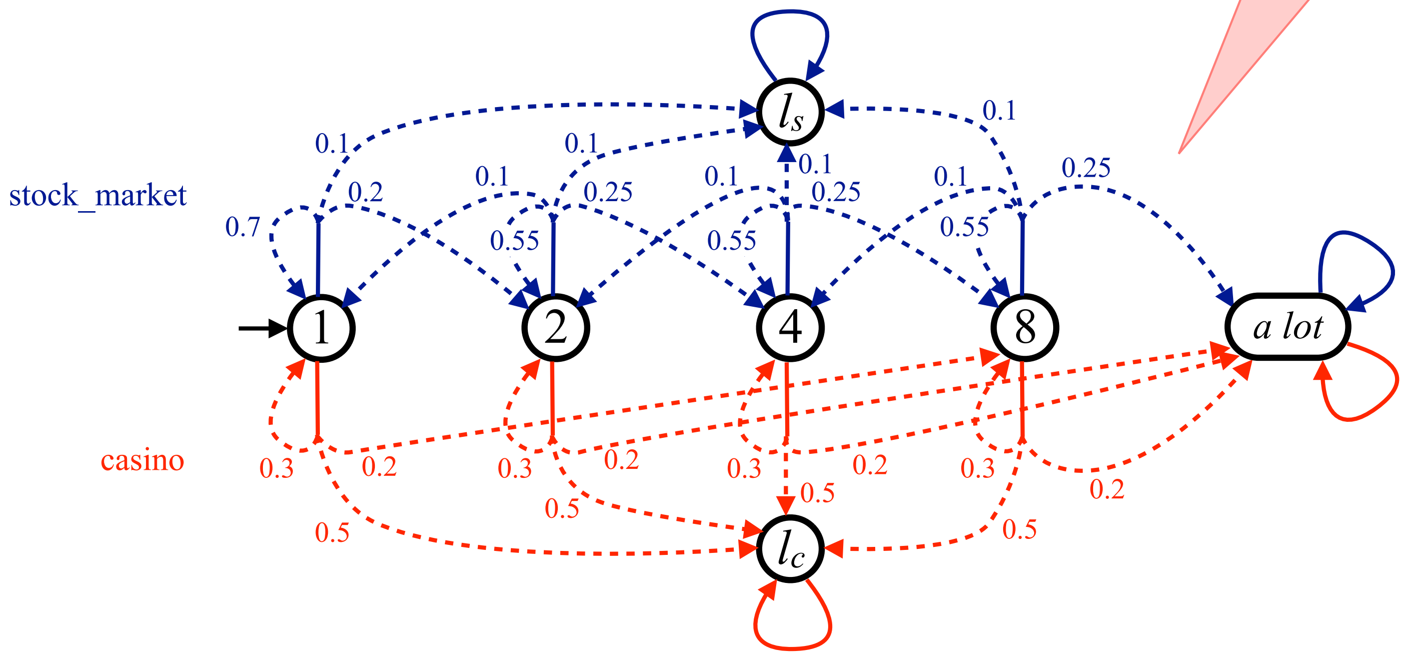
$\mathfrak{S}$ elige siempre stock_market $\qquad \Pr^{\mathfrak{S}}(① \models \mathtt{F}\,\text{"}a\ lot\text{"}) \approx 0.0443$

$\mathfrak{S}$ alterna entre stock_market y casino $\qquad \Pr^{\mathfrak{S}}(① \models \mathtt{F}\,\text{"}a\ lot\text{"}) \approx 0.1504$

$\mathfrak{S}$ alterna al revés $\qquad \Pr^{\mathfrak{S}}(① \models \mathtt{F}\,\text{"}a\ lot\text{"}) \approx 0.1332$

Probabilidad inducida por

Pero entonces,
¡¿¿cuál es la probabilidad de
F "*a lot*"??!



$\mathfrak{S}$ elige siempre casino	$\mathrm{Pr}^{\mathfrak{S}}(① \models \mathtt{F}\,\text{"}a\ lot\text{"}) \approx 0.0816$
$\mathfrak{S}$ elige siempre stock_market	$\mathrm{Pr}^{\mathfrak{S}}(① \models \mathtt{F}\,\text{"}a\ lot\text{"}) \approx 0.0443$
$\mathfrak{S}$ alterna entre stock_market y casino	$\mathrm{Pr}^{\mathfrak{S}}(① \models \mathtt{F}\,\text{"}a\ lot\text{"}) \approx 0.1504$
$\mathfrak{S}$ alterna al revés	$\mathrm{Pr}^{\mathfrak{S}}(① \models \mathtt{F}\,\text{"}a\ lot\text{"}) \approx 0.1332$

Probabilidades supremas e ínfimas

Dado que cualquier resolución del no-determinismo es posible, se buscan las mejores y peores cotas que garanticen la satisfacción de la propiedad ω-regular bajo estudio.

Esto es, si $\mathcal{L}$ es dicha propiedad, se busca

$$\mathrm{Pr}^{\max}(s \models \mathcal{L}) \triangleq \sup_{\mathfrak{S}} \mathrm{Pr}^{\mathfrak{S}}(s \models \mathcal{L}), \quad \text{y}$$

$$\mathrm{Pr}^{\min}(s \models \mathcal{L}) \triangleq \inf_{\mathfrak{S}} \mathrm{Pr}^{\mathfrak{S}}(s \models \mathcal{L})$$

CONICET

UNC

Probabilidades supremas e ínfimas

Dado que cualquier resolución del no-determinismo es posible, se buscan las mejores y peores cotas que garanticen la satisfacción de la propiedad ω-regular bajo estudio.

Esto es, si $\mathcal{L}$ es dicha propiedad, se busca

$$\mathrm{Pr}^{\max}(s \models \mathcal{L}) \triangleq \sup_{\mathfrak{S}} \mathrm{Pr}^{\mathfrak{S}}(s \models \mathcal{L}), \qquad \text{y}$$

$$\mathrm{Pr}^{\min}(s \models \mathcal{L}) \triangleq \inf_{\mathfrak{S}} \mathrm{Pr}^{\mathfrak{S}}(s \models \mathcal{L})$$

Para alcanzabilidad es
suficiente considerar solo los schedulers que
en un estado siempre eligen la misma acción
(i.e. deterministas y sin memoria)

CONICET

Solución a través de ecuaciones de Bellman

El calculo de la probabilidad máxima de alcanzar un estado de B tiene solución en el mínimo punto fijo del siguiente sistemas de ecuaciones

$$
\begin{array}{ll}
x_s = 1 & \text{if } s \in B \\
x_s = 0 & \text{if } s \in S^{=0} \\
x_s = \max_{\alpha \in Act(s)} \sum_{t \in S} \mathbf{P}(s, \alpha, t) \cdot x_t & \text{if } s \in S \backslash (S^{=0} \cup B)
\end{array}
$$

CONICET

UNC

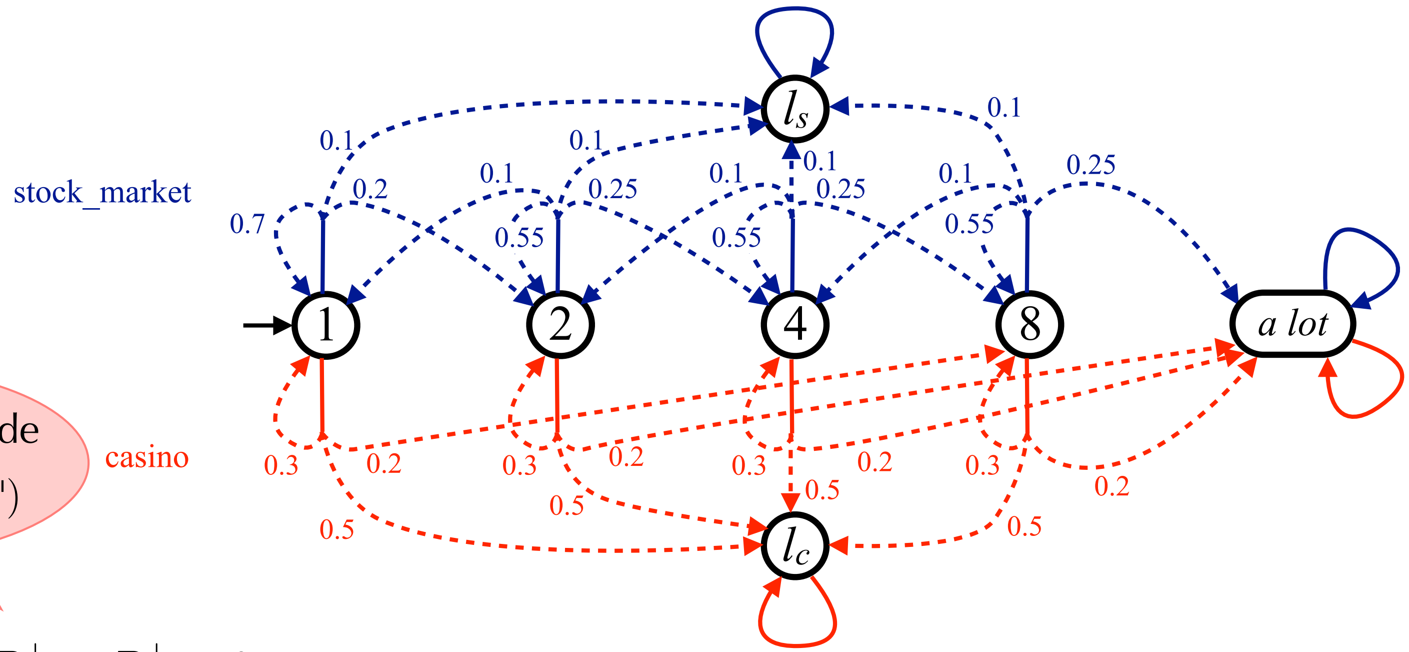
Solución a través de ecuaciones de Bellman

El calculo de la probabilidad máxima de alcanzar un estado de B tiene solución en el mínimo punto fijo del siguiente sistemas de ecuaciones

$$
\begin{aligned}
x_s &= 1 && \text{if } s \in B \\
x_s &= 0 && \text{if } s \in S^{=0} \\
x_s &= \max_{\alpha \in Act(s)} \sum_{t \in S} \mathbf{P}(s, \alpha, t) \cdot x_t && \text{if } s \in S \setminus (S^{=0} \cup B)
\end{aligned}
$$

Para calcular la probabilidad mínima, reemplazar por "min"

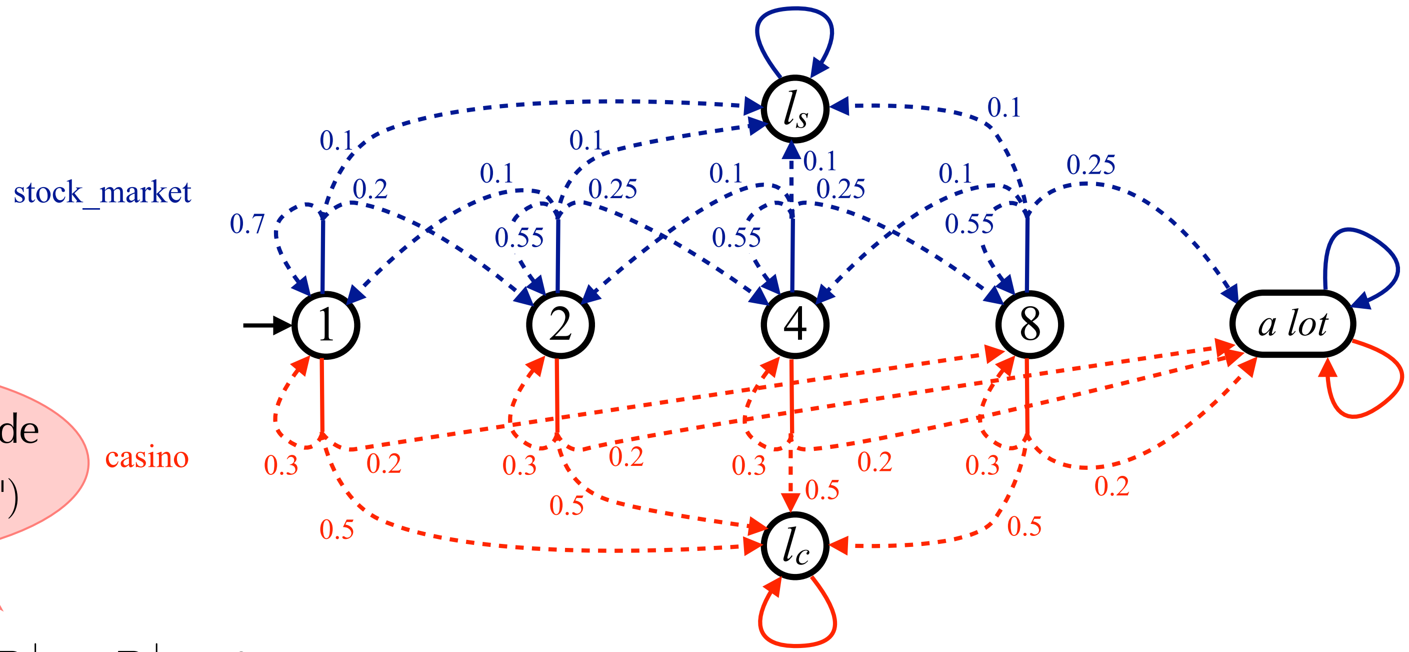
Alcanzabilidad cuantitativa



P_s^+ es abreviación de $\Pr^{\max}(s \models \mathtt{F}\,\text{"}a\ lot\text{"})$

$$P_{l_s}^+ = P_{l_c}^+ = 0$$

Alcanzabilidad cuantitativa

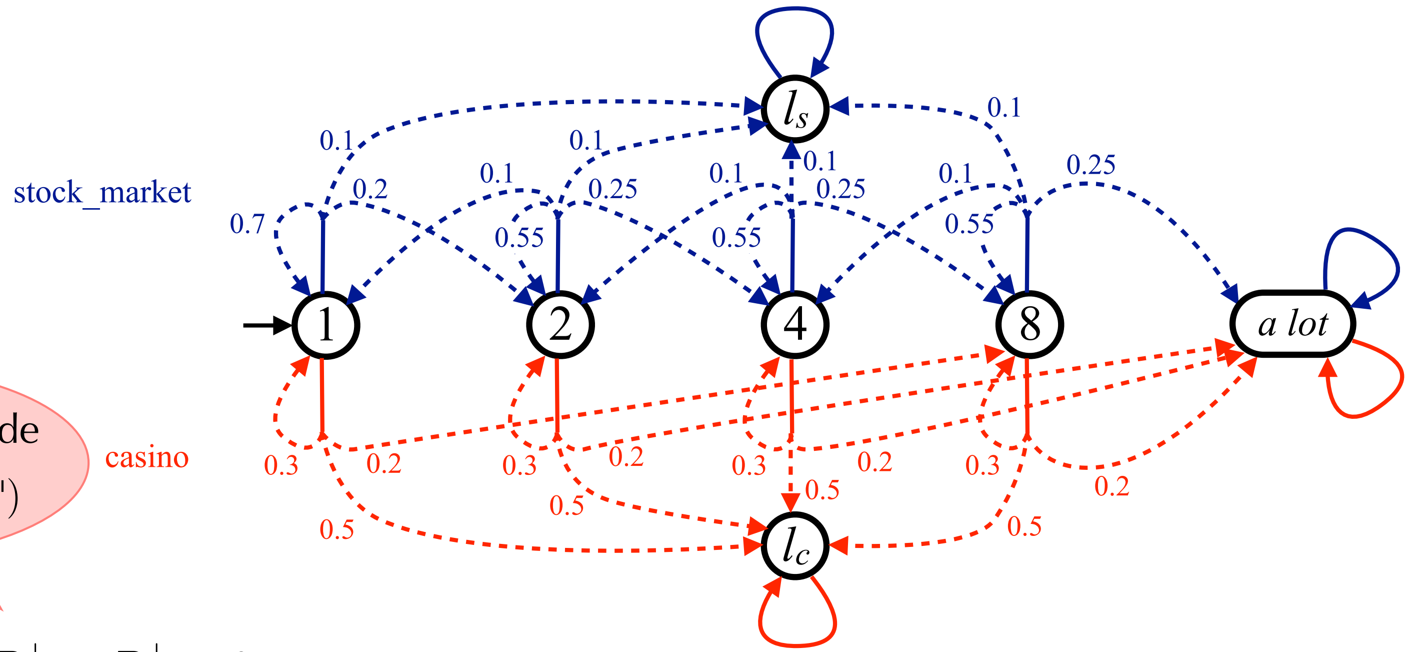


P^+_s es abreviación de $\Pr^{\max}(s \models \mathtt{F}\,\text{"}a\ lot\text{"})$

$$P^+_{l_s} = P^+_{l_c} = 0$$

$$P^+_{al} = 1$$

Alcanzabilidad cuantitativa



P_s^+ es abreviación de $\Pr^{\max}(s \models \mathtt{F}\,\text{"}a\ lot\text{"})$

$$P_{l_s}^+ = P_{l_c}^+ = 0$$

$$P_{al}^+ = 1$$

$$P_1^+ = \max\left(\, 0.7P_1^+ + 0.2P_2^+ + 0.1P_{l_s}^+,\ 0.3P_1^+ + 0.2P_8^+ + 0.5P_{l_c}^+ \,\right)$$

$$P_2^+ = \max\left(\, 0.55P_2^+ + 0.25P_4^+ + 0.1P_1^+ + 0.1P_{l_s}^+,\ 0.3P_2^+ + 0.2P_{al}^+ + 0.5P_{l_c}^+ \,\right)$$

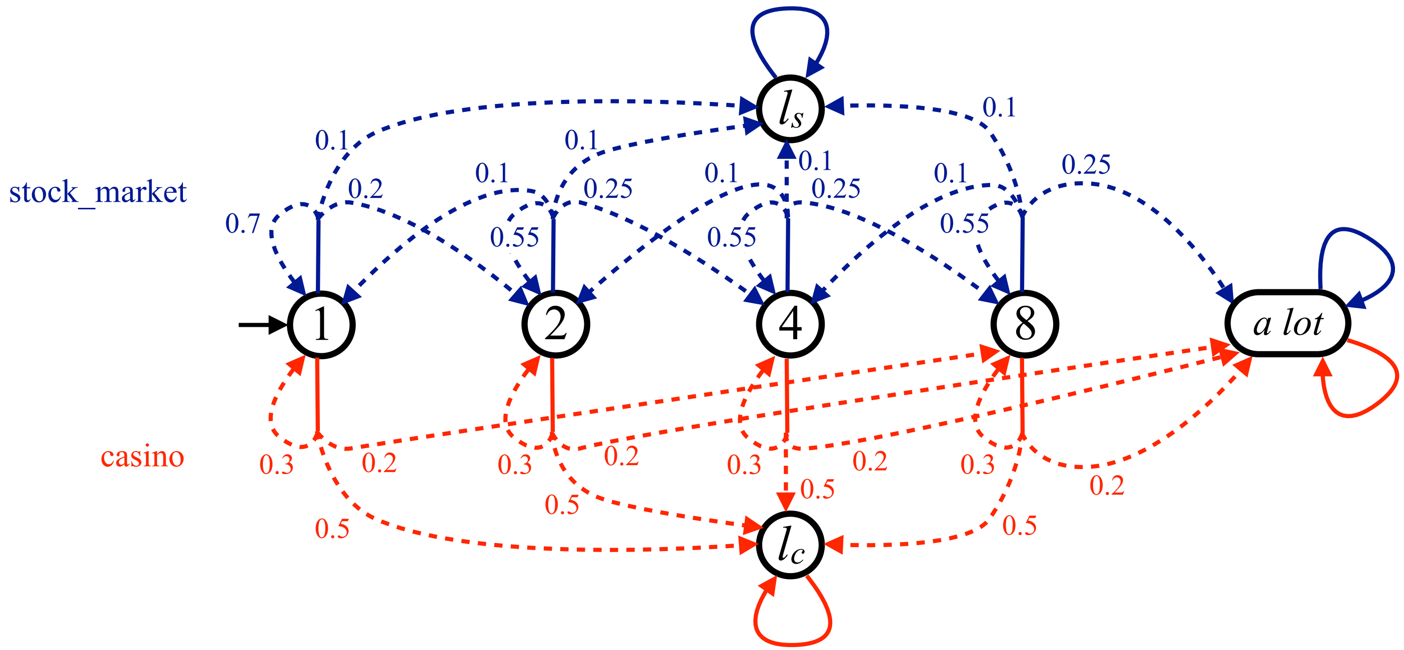
$$P_4^+ = \max\left(\, 0.55P_4^+ + 0.25P_8^+ + 0.1P_2^+ + 0.1P_{l_s}^+,\ 0.3P_4^+ + 0.2P_{al}^+ + 0.5P_{l_c}^+ \,\right)$$

$$P_8^+ = \max\left(\, 0.55P_8^+ + 0.25P_{al}^+ + 0.1P_4^+ + 0.1P_{l_s}^+,\ 0.3P_8^+ + 0.2P_{al}^+ + 0.5P_{l_c}^+ \,\right)$$

CONICET

UNC

Alcanzabilidad cuantitativa



$\Pr^{\max}(① \models \texttt{F}\,"a\ lot") \approx 0.1905$

y se hace máximo en el scheduler $\mathfrak{S}$ definido por

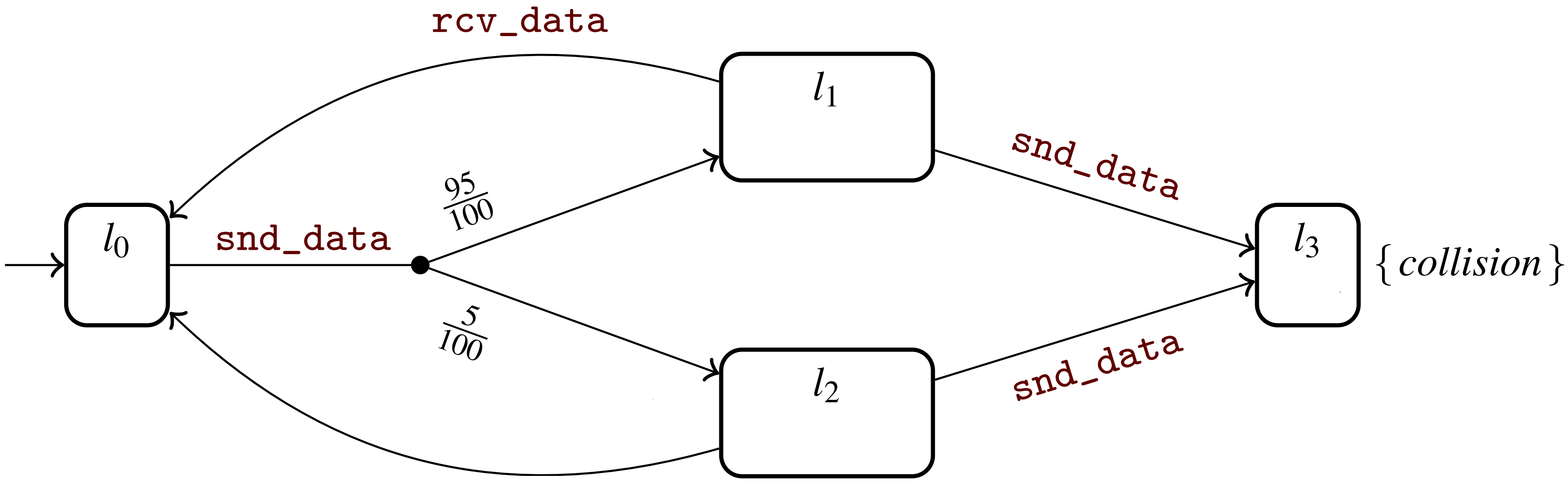
$\mathfrak{S}(①) =$ stock_market

$\mathfrak{S}(②) =$ casino

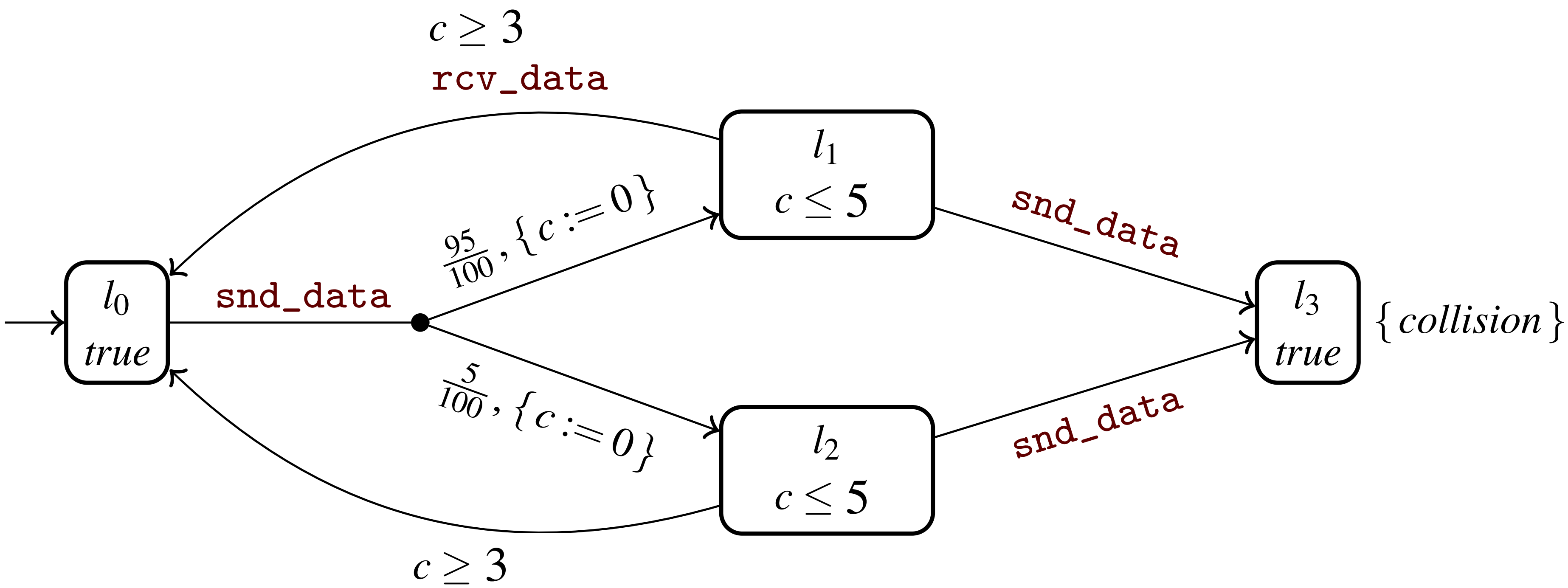
$\mathfrak{S}(④) =$ stock_market

$\mathfrak{S}(⑧) =$ stock_market

Autómatas temporizados con probabilidades (PTA)



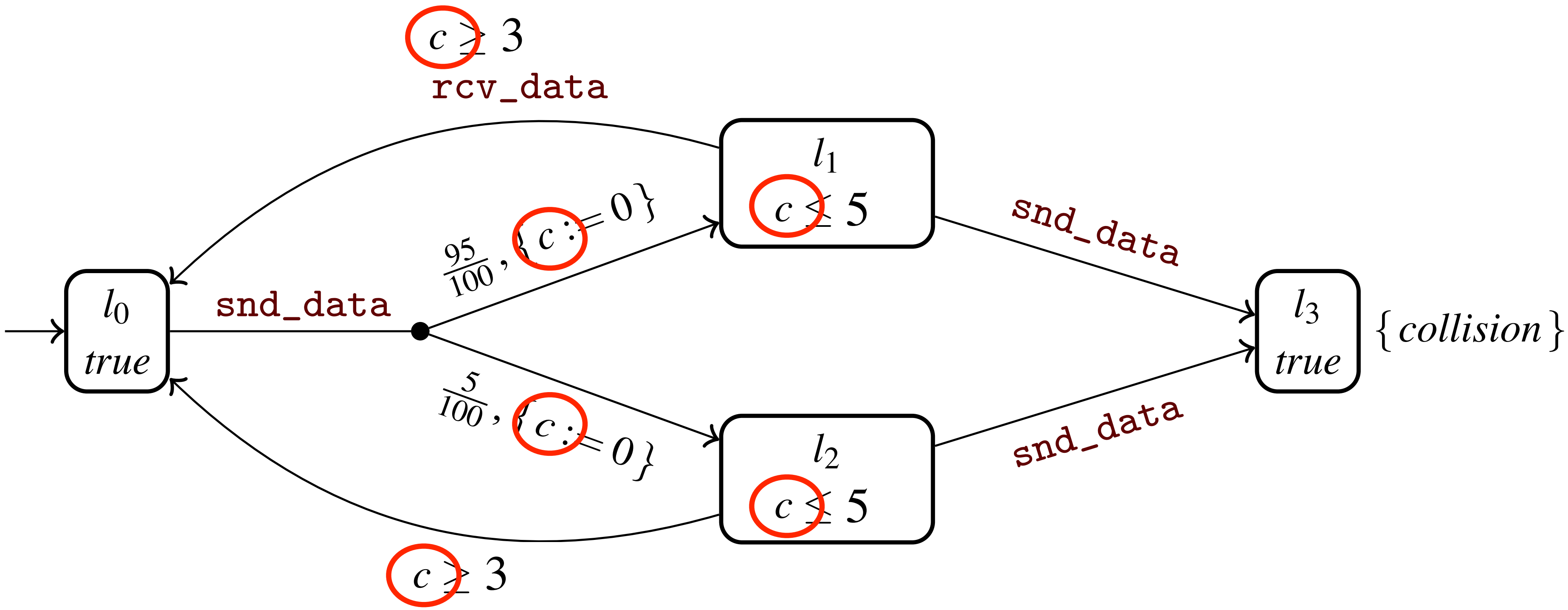
Autómatas temporizados con probabilidades (PTA)



CONICET

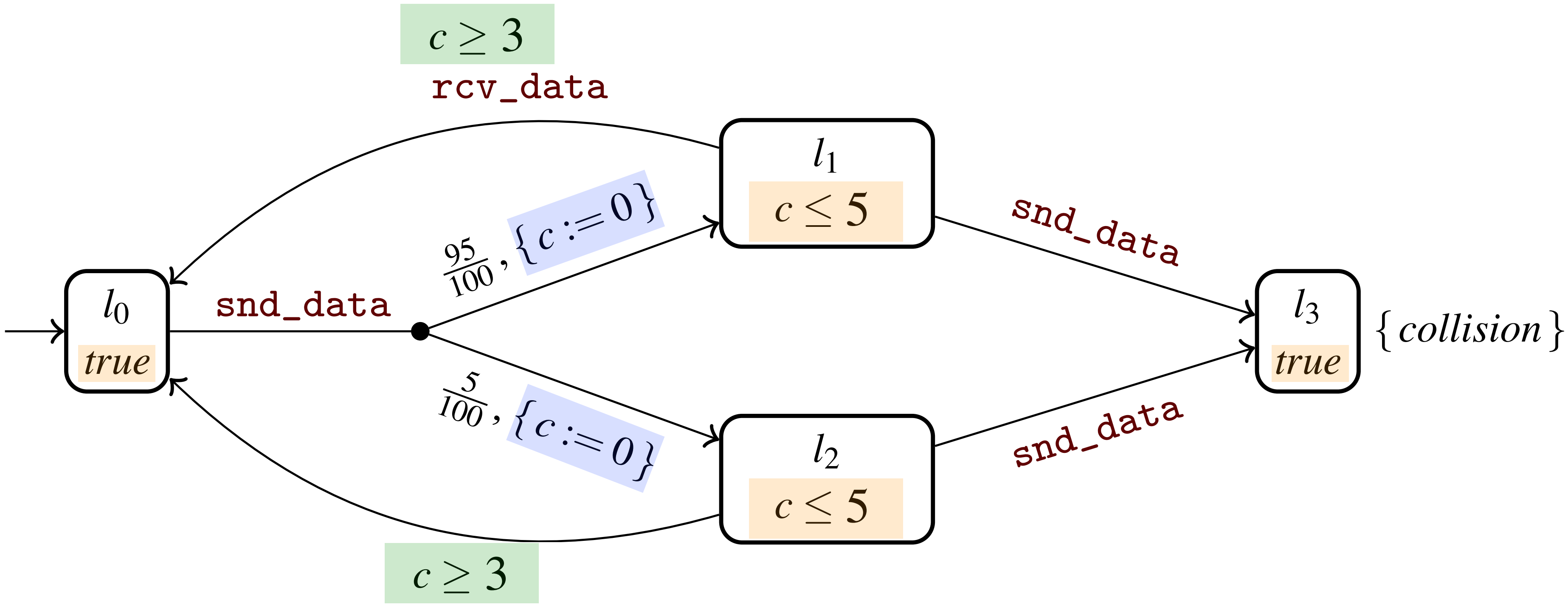
UNC

Autómatas temporizados con probabilidades (PTA)



Relojes: son variables en los reales no negativos que se incrementan sincrónicamente.

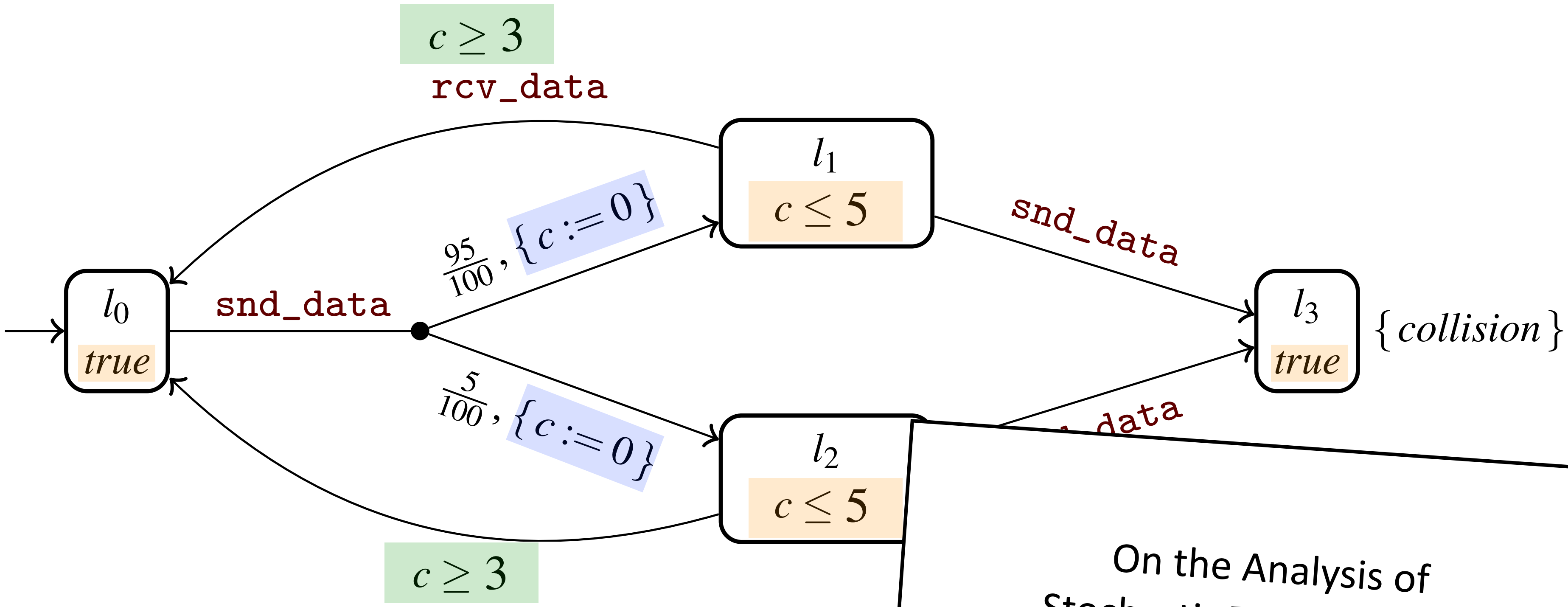
Autómatas temporizados con probabilidades (PTA)



Relojes: son variables en los reales no negativos que se incrementan sincrónicamente.

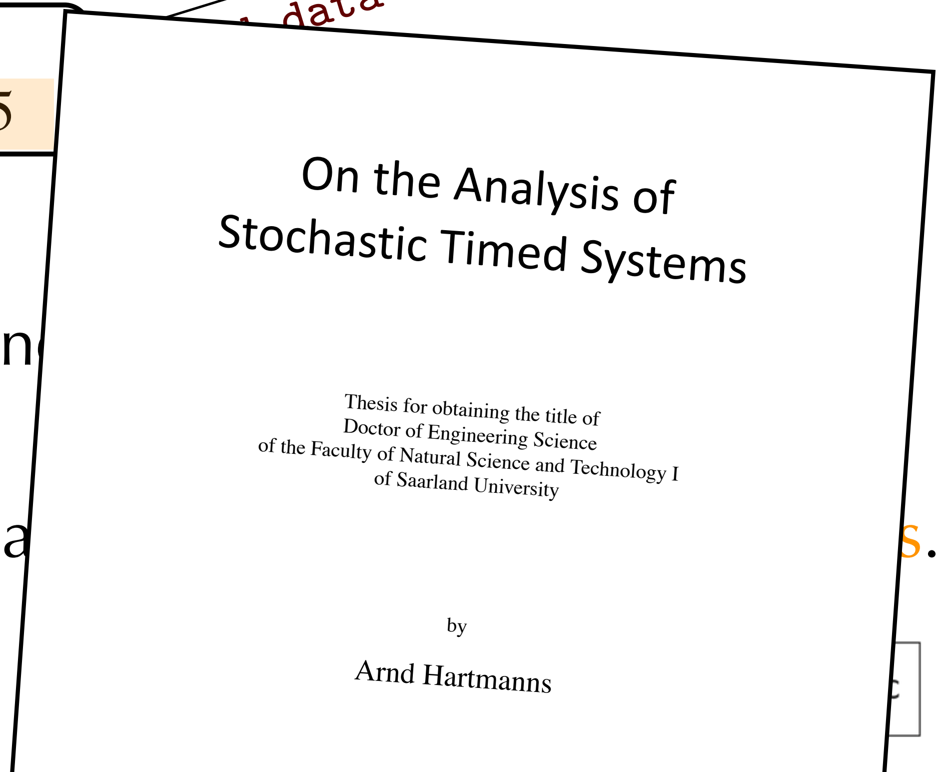
Se pueden resetear y verificar su valor a través de guardas o invariantes.

Autómatas temporizados con probabilidades (PTA)



Relojes: son variables en los reales no n
sincrónicamente.

Se pueden resetear y verificar su valor a s.



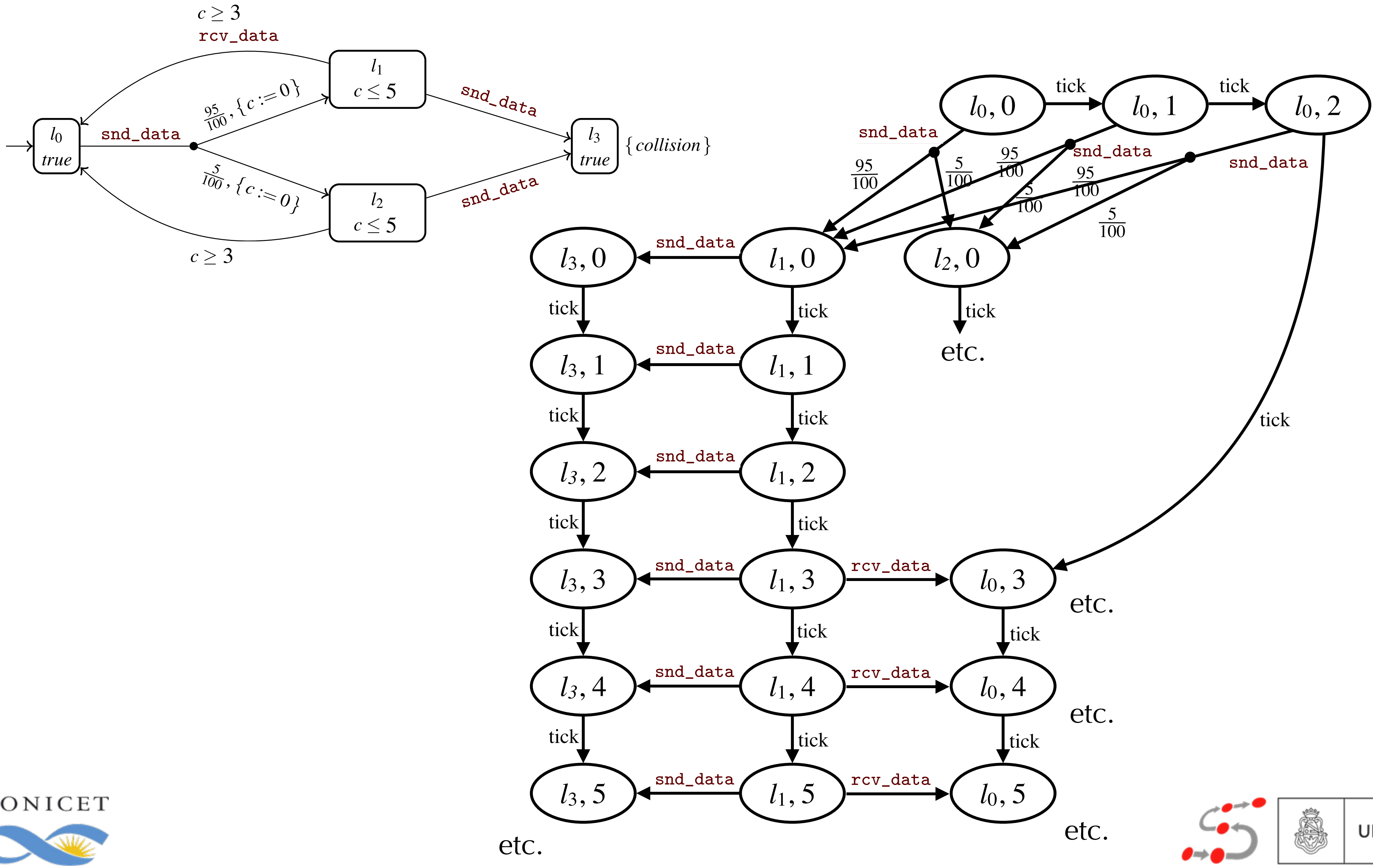
On the Analysis of
Stochastic Timed Systems

Thesis for obtaining the title of
Doctor of Engineering Science
of the Faculty of Natural Science and Technology I
of Saarland University

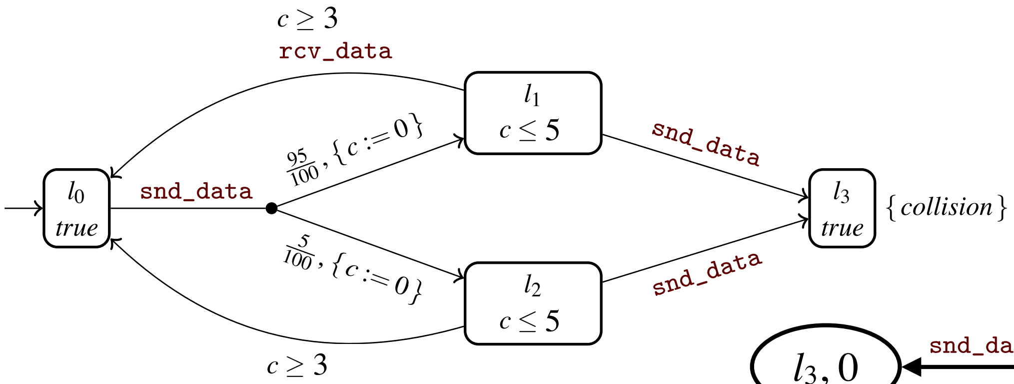
by

Arnd Hartmanns

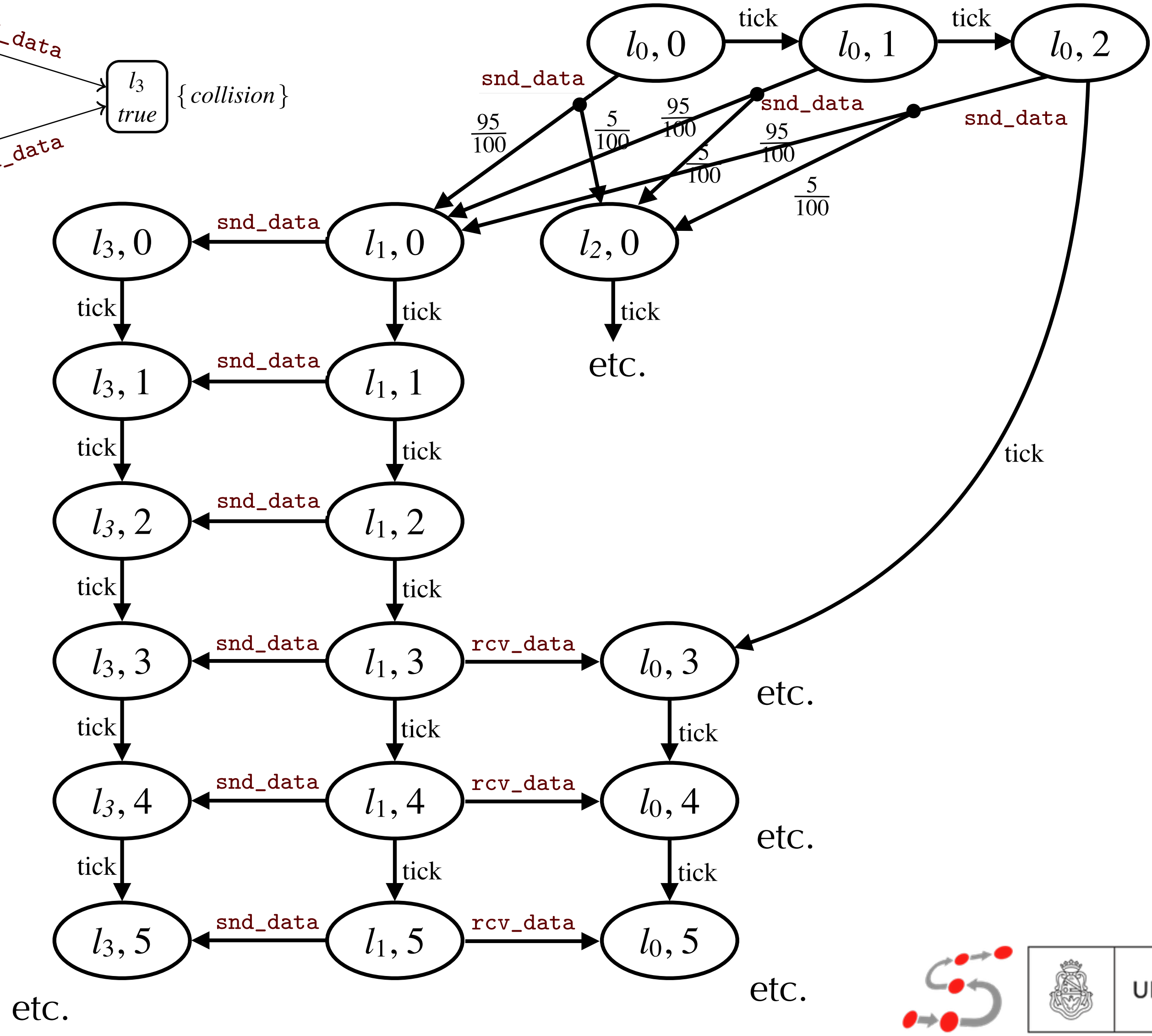
Autómatas temporizados con probabilidades (PTA)



Autómatas temporizados con probabilidades (PTA)



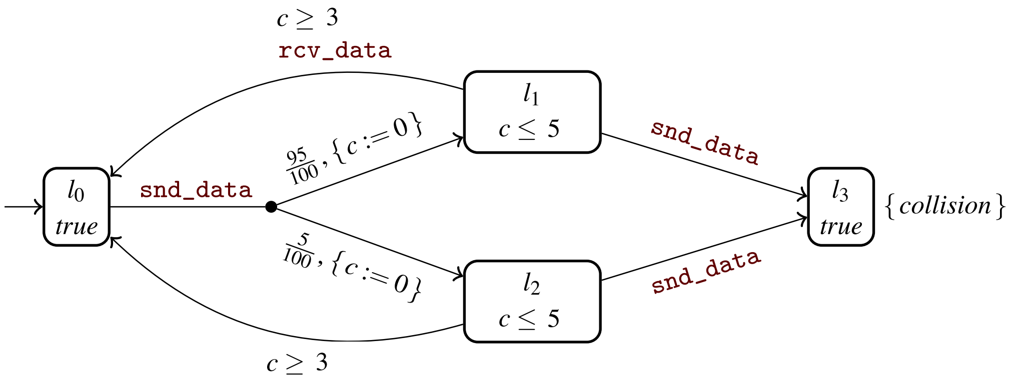
Es un MDP!

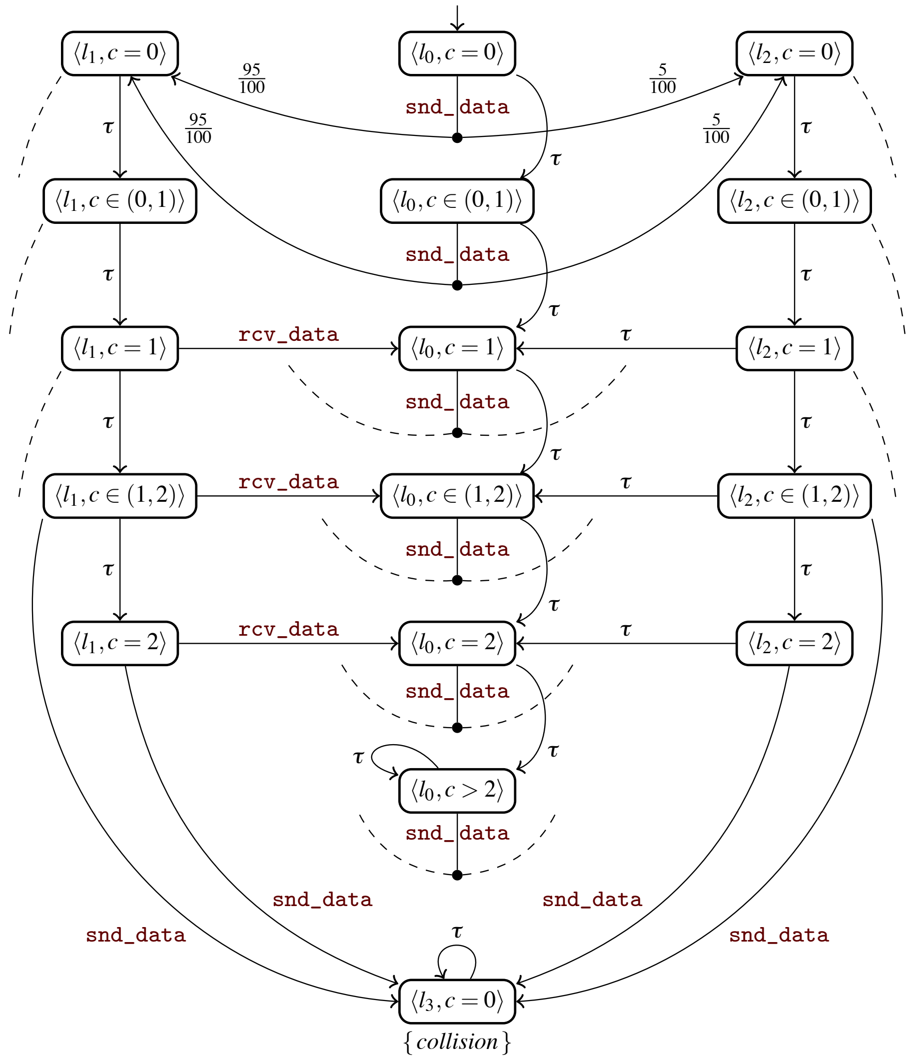


CONICET

UNC

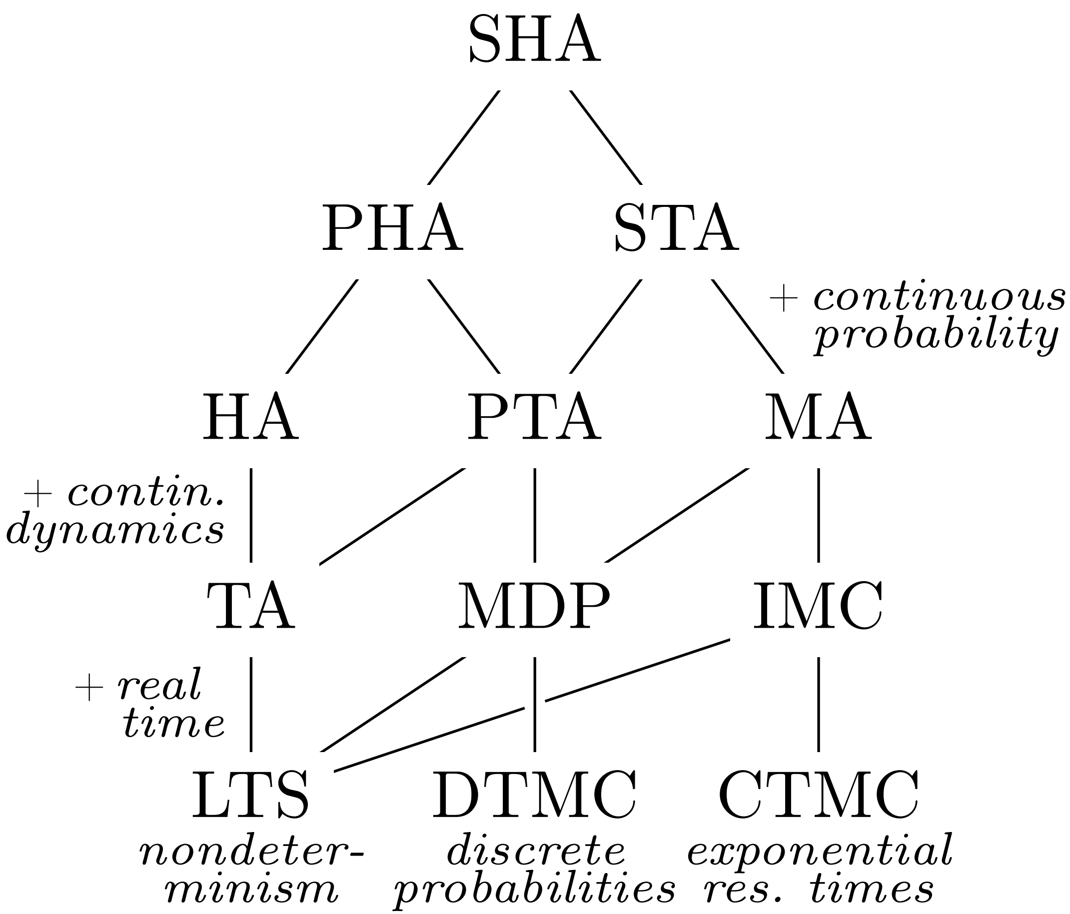
Autómatas temporizados con probabilidades (PTA)



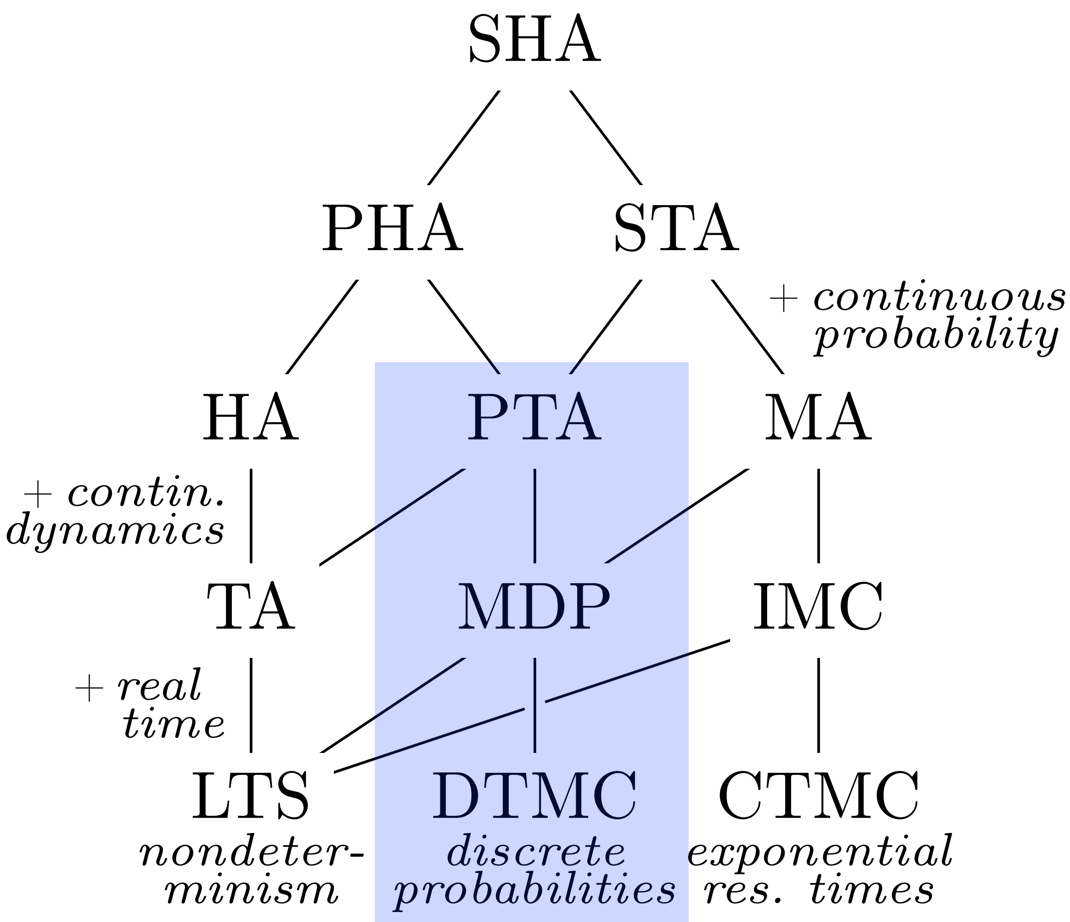


Se puede construir algo parecido para los reales

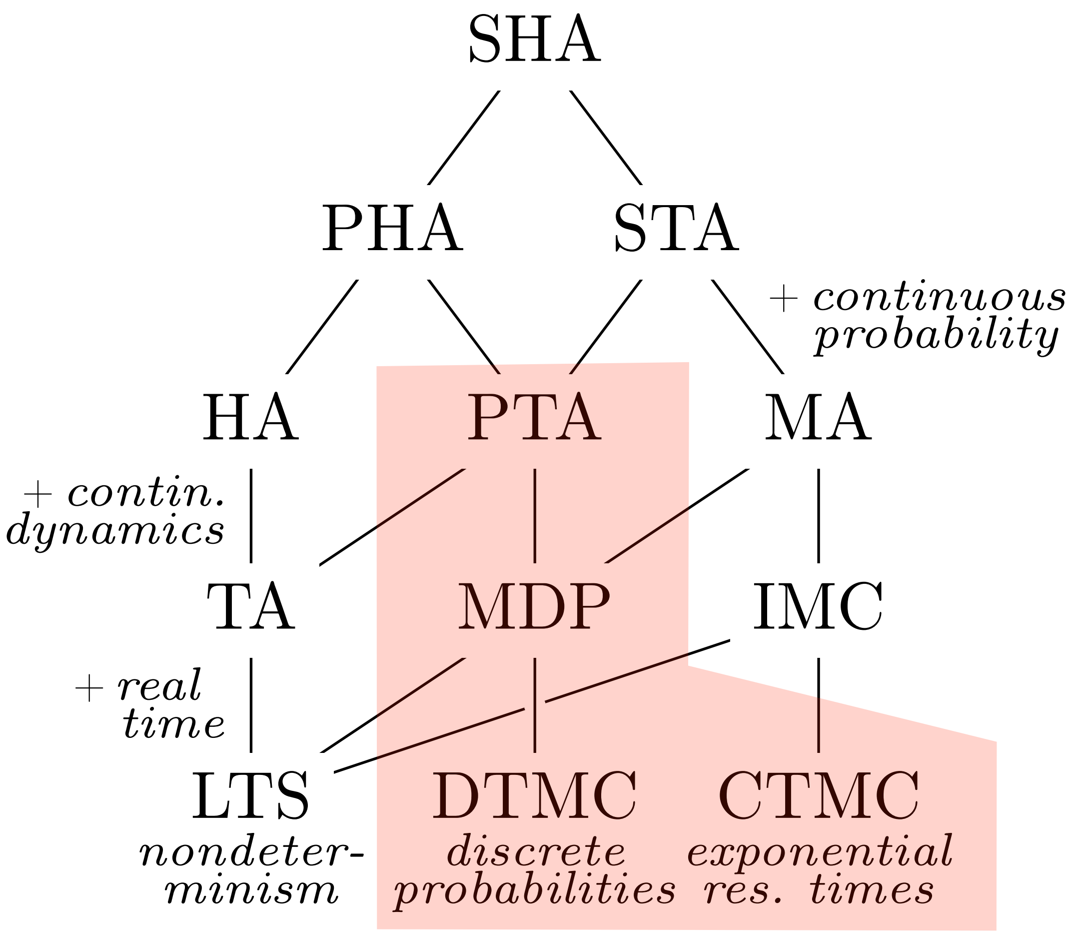
El zoológico de autómatas cuantitativos



El zoológico de autómatas cuantitativos



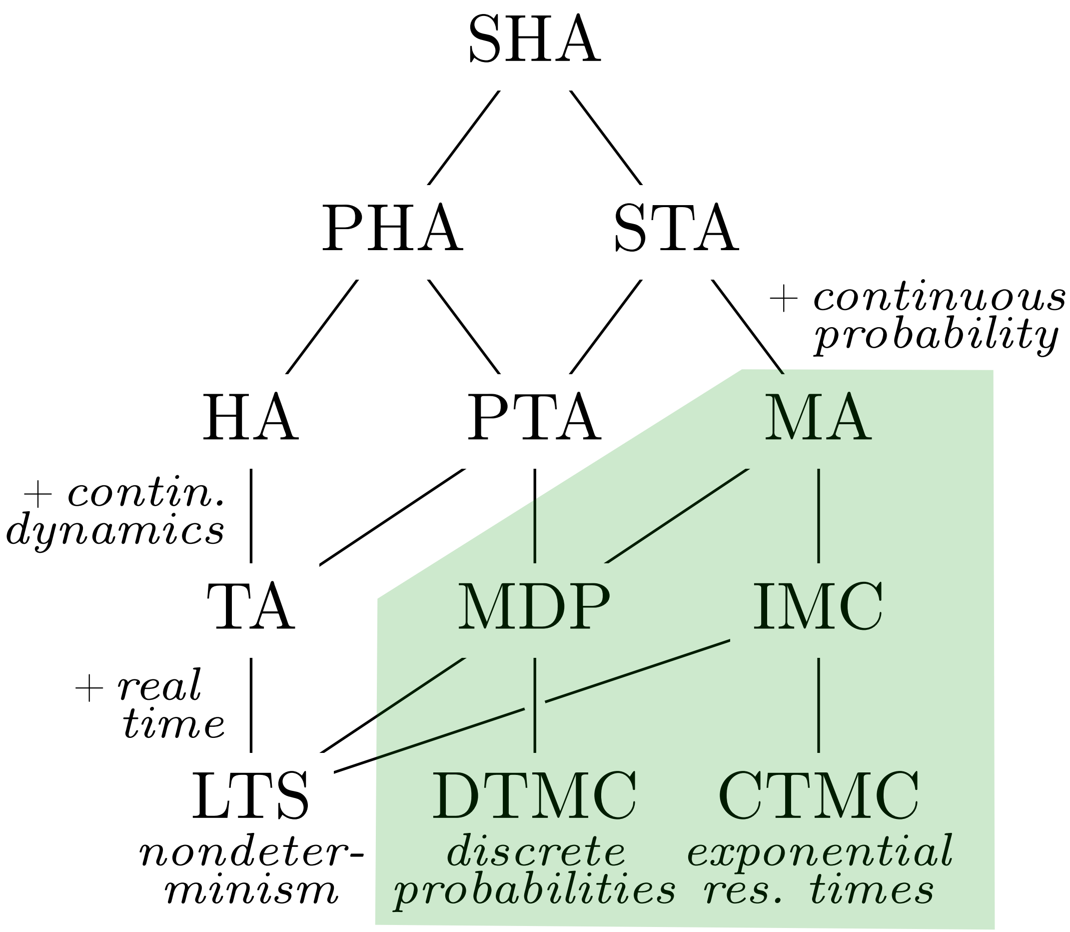
El zoológico de autómatas cuantitativos



PRISM

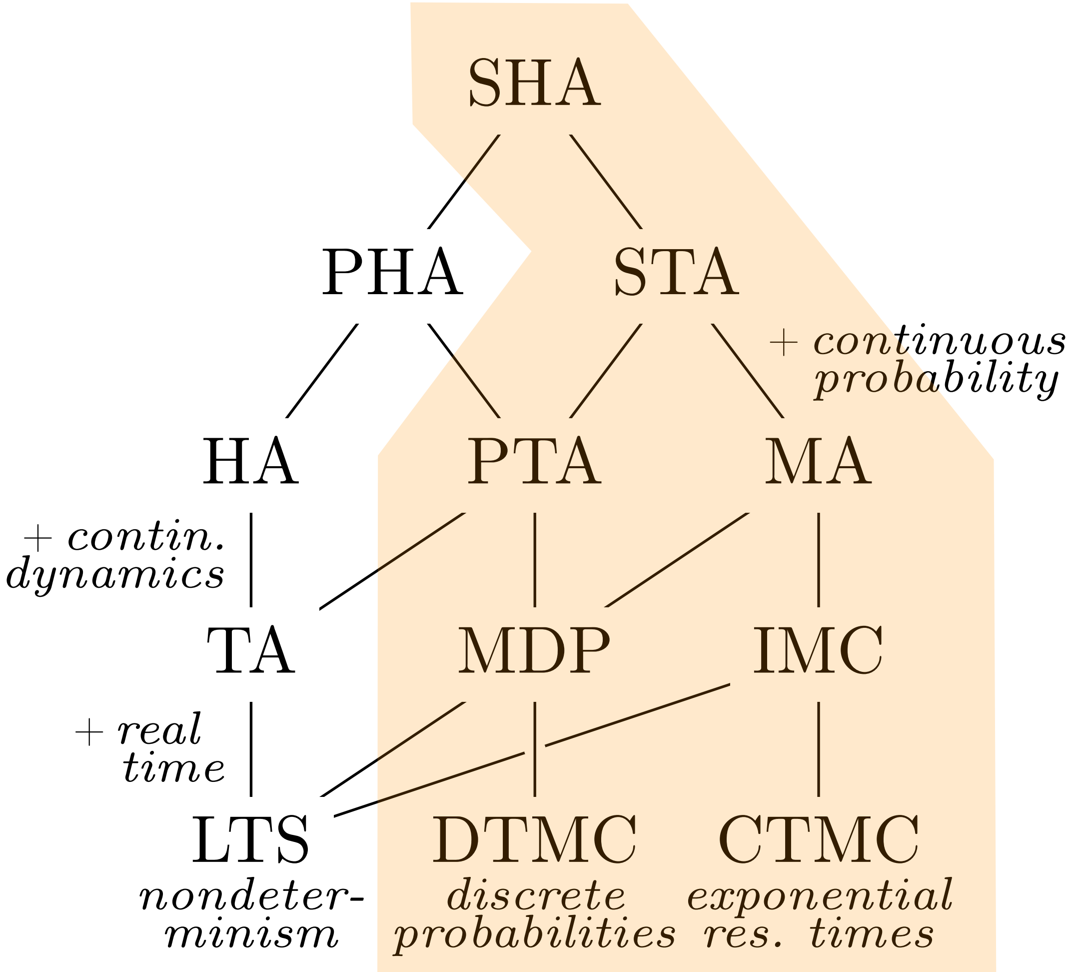
+ POMDP, POPTA

El zoológico de autómatas cuantitativos



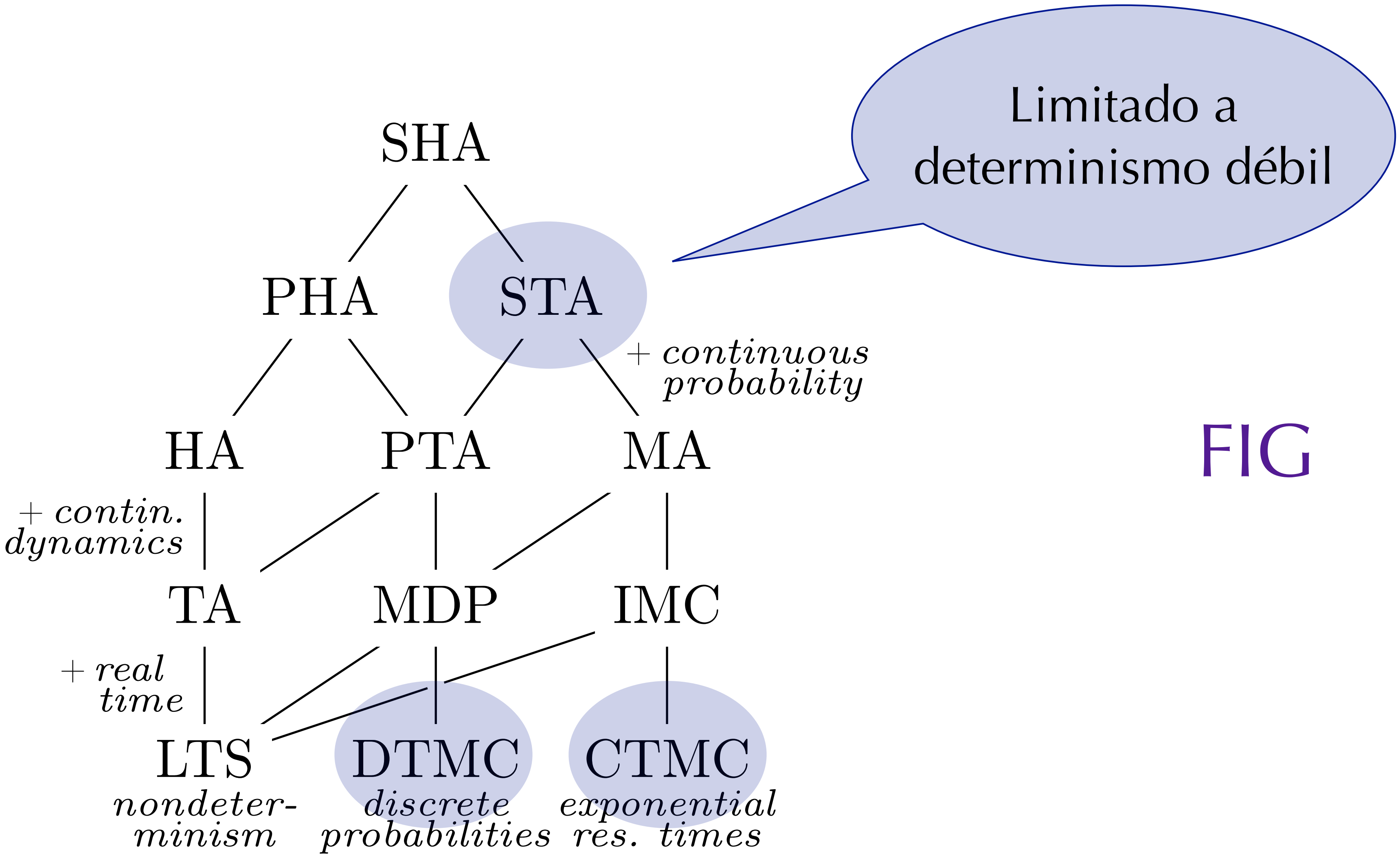
Storm

El zoológico de autómatas cuantitativos



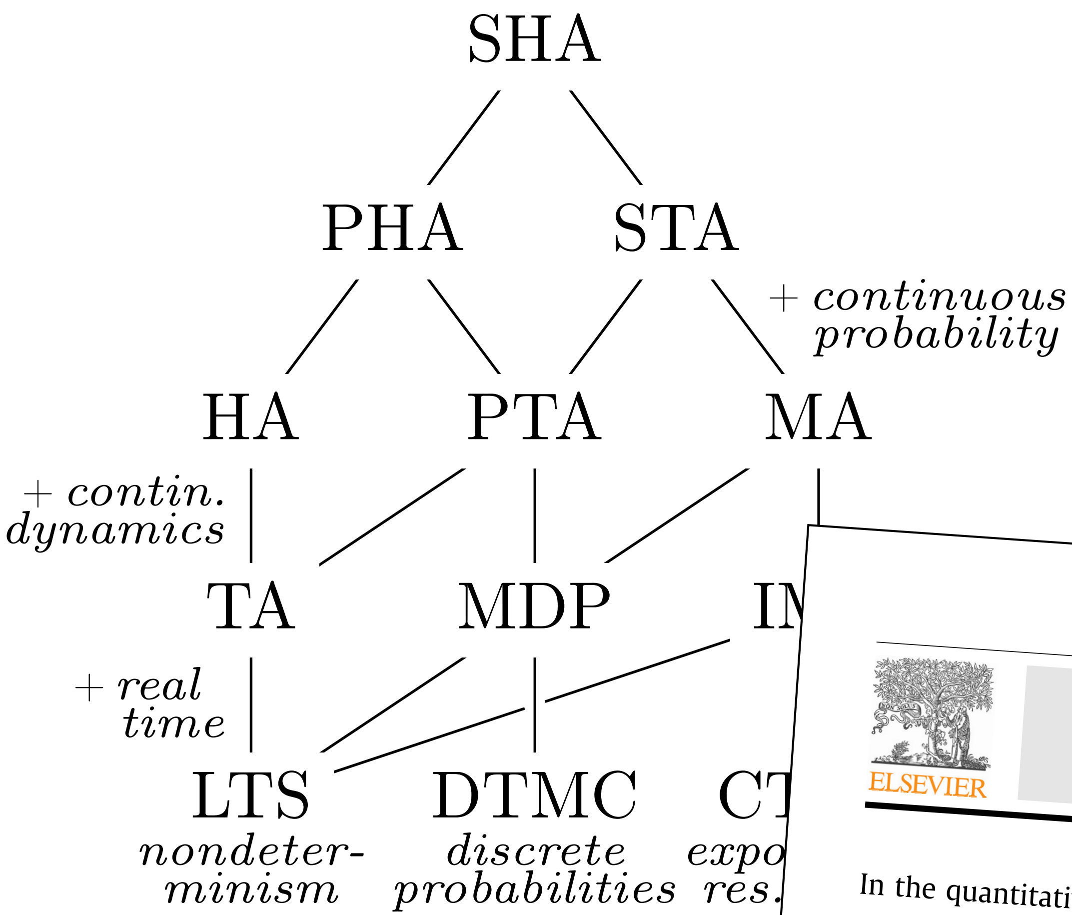
Modest

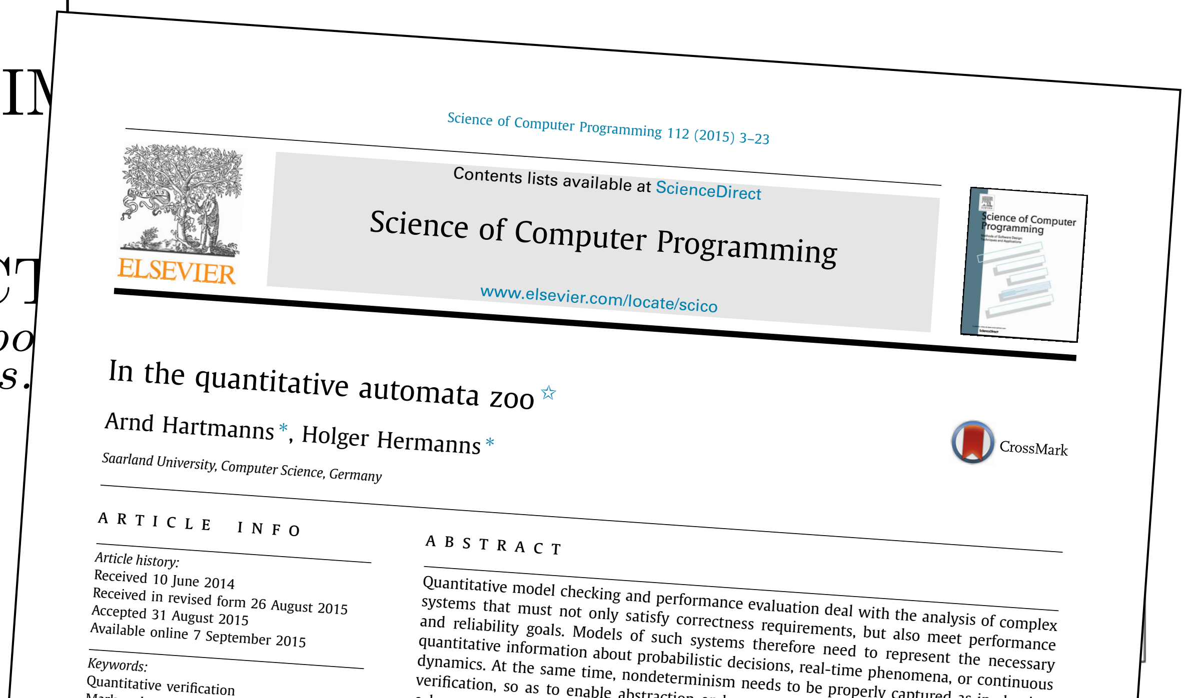
El zoológico de autómatas cuantitativos



FIG

El zoológico de autómatas cuantitativos




Science of Computer Programming 112 (2015) 3–23
Contents lists available at ScienceDirect
Science of Computer Programming
www.elsevier.com/locate/scico

In the quantitative automata zoo ☆

Arnd Hartmanns *, Holger Hermanns *
Saarland University, Computer Science, Germany

ARTICLE INFO
Article history:
Received 10 June 2014
Received in revised form 26 August 2015
Accepted 31 August 2015
Available online 7 September 2015
Keywords:
Quantitative verification

ABSTRACT
Quantitative model checking and performance evaluation deal with the analysis of complex systems that must not only satisfy correctness requirements, but also meet performance and reliability goals. Models of such systems therefore need to represent the necessary quantitative information about probabilistic decisions, real-time phenomena, or continuous dynamics. At the same time, nondeterminism needs to be properly captured as in... verification, so as to enable abstraction...

CONICET