Verificación de Sistemas con Probabilidad y Nodeterminismo

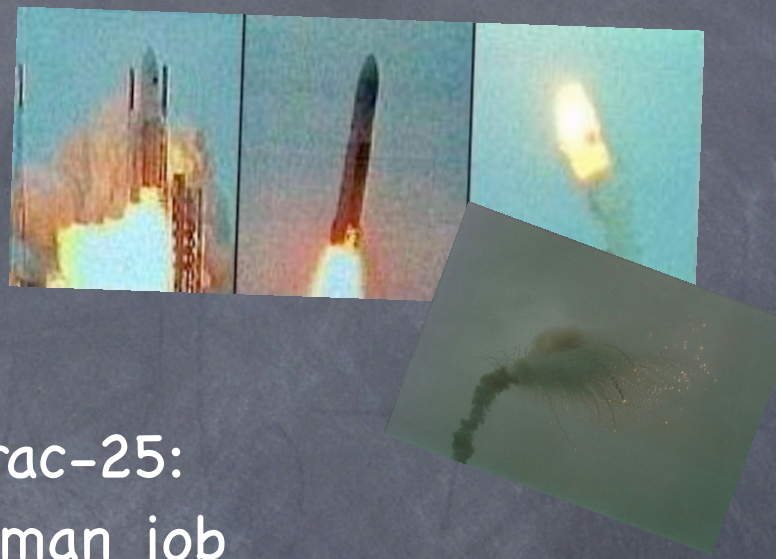
Pedro R. D'Argenio
FaMAF, UNC - CONICET

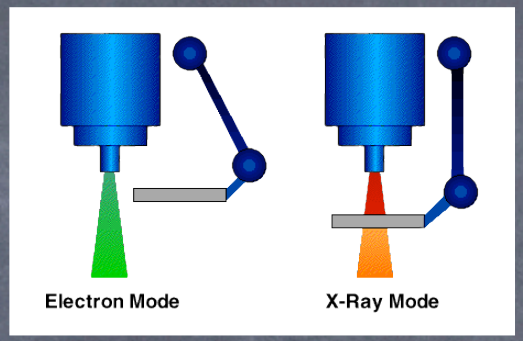
JCC - Rosario
28-Oct-2010

¿Por qué verificación?

Pentium:
FDIV

Ariane 5:
64 bits fp
vs 16 bits int





Therac-25:
one man job

Mars Climate Orbiter:
Métrico vs Imperial

HMS Sheffield:
Exocet amigo

Voto electrónico:
Integridad/Confidencialidad

CONICET

FaMAF

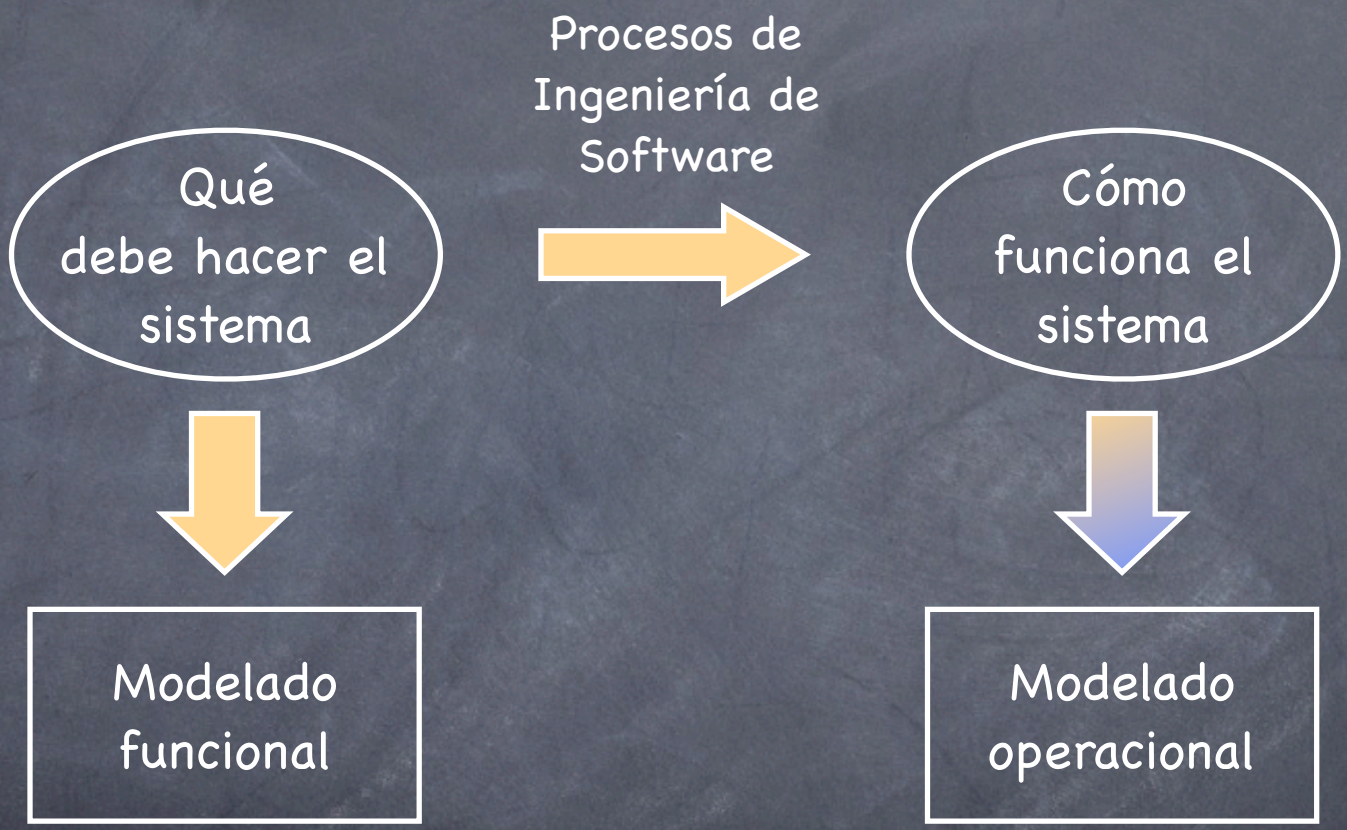
El proceso de verificación

El proceso de v

Proceso informal
(si bien puede ser riguroso)

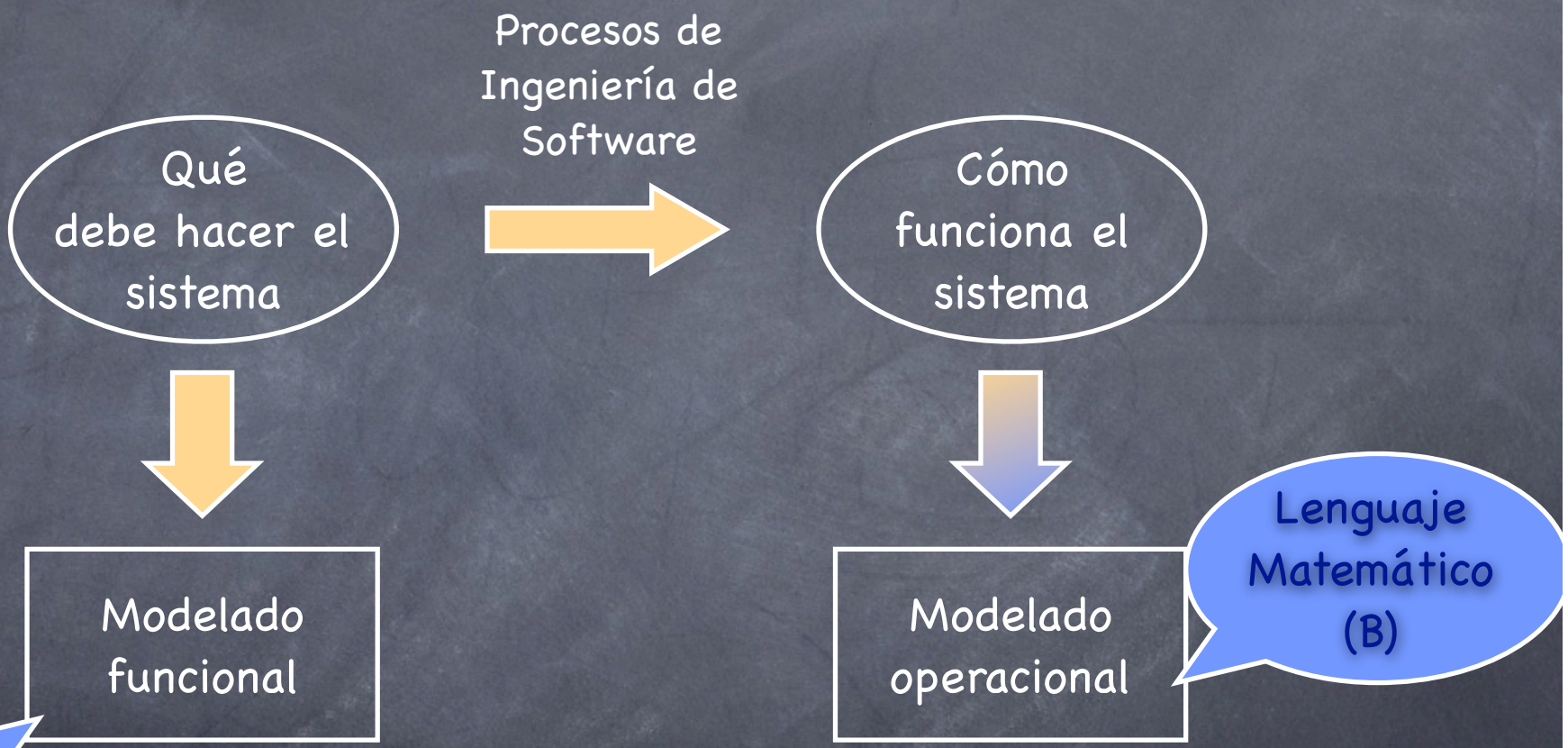
El proceso de v

Proceso informal
(si bien puede ser riguroso)



El proceso de v

Proceso informal
(si bien puede ser riguroso)



CONICET

FaMAF

El proceso de v

Proceso informal
(si bien puede ser riguroso)

Lenguaje Matemático (A)

Lenguaje Matemático (B)

Responde a una relación de satisfacción: B⊨A

CONICET

FaMAF

El proceso de v

El proceso de v

Técnicas Asercionales

- (Pre,Pos)
- Programa
- Sist. de deducción

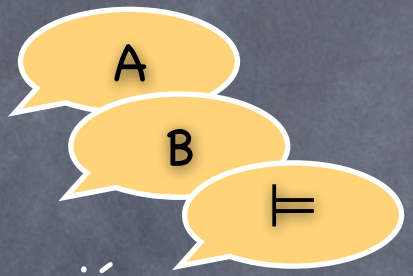
CONICET

FaMAF

El proceso de v

Técnicas Asercionales

- (Pre,Pos)
- Programa
- Sist. de deducción



El proceso de v

Relación de sat:

Lenguaje Matemático (A)

Lenguaje Matemático (B)

{Pre} S {Pos}

Lógica de Hoare / WP / Owicki-Gries / Separation Logic

Técnicas Asercionales

- (Pre,Pos)
- Programa
- Sist. de deducción

A

B

⊨

El proceso de v

Técnicas Asercionales

- (Pre,Pos)
- Programa
- Sist. de deducción

Model Checking

- Fórmula temporal
- Modelo del programa
- Def. satisfactibilidad

CONICET

FaMAF

El proceso de v

Relación de sat:
B⊨A

Lenguaje Matemático (A)

Proceso de Verificación

Lenguaje Matemático (B)

Modelado funcional

Modelado operacional

M(S) ⊨ Φ

M(S) es un sistema de estados y transiciones y "⊨" se verifica automáticamente

Técnicas Asercionales

- (Pre,Pos)
- Programa
- Sist. de ded

Model Checking

- Fórmula temporal
- Modelo del programa
- Def. satisfactibilidad

CONICET

FaMAF

El proceso de v

Relación de sat:
B⊨A

Lenguaje Matemático (A)

Proceso de Verificación

Lenguaje Matemático (B)

Modelado funcional

$G(p \Rightarrow F\, q)$

$M(S) \models \Phi$

M(S) es un sistema de estados y transiciones y "⊨" se verifica automáticamente

Técnicas Asercionales

- (Pre,Pos)
- Programa
- Sist. de ded

Model Checking

- Fórmula temporal
- Modelo del programa
- Def. satisfactibilidad

CONICET

FaMAF

El proceso de v

Técnicas Asercionales
- (Pre,Pos)
- Programa
- Sist. de deducción

Álgebras de Procesos
- Un término
- Otro término
- Teoría ecuacional

Model Checking
- Fórmula temporal
- Modelo del programa
- Def. satisfactibilidad

CONICET

FaMAF

El proceso de v

Relación de sat: $B \models A$

Lenguaje Matemático (A)

Proceso de Verificación

Lenguaje Matemático (B)

Modelado funcional

Modelado operacional

Técnicas Asercionales
- (Pre,Pos)
- Programa
- Sist. de deducción

Álgebras de Procesos
- Un término
- Otro término
- Teoría ecuacional

Model Checking
- Fórmula temporal
- Modelo del programa
- Def. satisfactibilidad

Relaciones Semánticas
- Modelo propiedad
- Modelo del programa
- Equivalencia semántica

CONICET

FaMAF

Lo que hacemos en nuestro grupo

Técnicas para la verificación de sistemas

Lo que hacemos en nuestro grupo

Técnicas para la verificación de sistemas

- Model Checking
- Asercionales
- Algebras de Procesos
- Basadas en relaciones

Lo que hacemos en nuestro grupo

Técnicas para la verificación de sistemas

- Model Checking
- Asercionales
- Algebras de Procesos
- Basadas en relaciones

- Concurrentes/distribuidos
- Componentes aleatorias
- Tiempo real
- Tolerancia a fallas
- Seguridad

CONICET

FaMAF

Lo que hacemos en nuestro grupo

Técnicas para la verificación de sistemas

- Model Checking
- Asercionales
- Algebras de Procesos
- Basadas en relaciones

- Concurrentes/distribuidos
- Componentes aleatorias
- Tiempo real
- Tolerancia a fallas
- Seguridad

Semántica

CONICET

FaMAF

Lo que hacemos en nuestro grupo

Técnicas para la verificación de sistemas

- Model Checking
- Asercionales
- Algebras de Procesos
- Basadas en relaciones

- Concurrentes/distribuidos
- Componentes aleatorias
- Tiempo real
- Tolerancia a fallas
- Seguridad

Semántica

FaMAF

Lo que hacemos en nuestro grupo

Técnicas para la verificación de sistemas

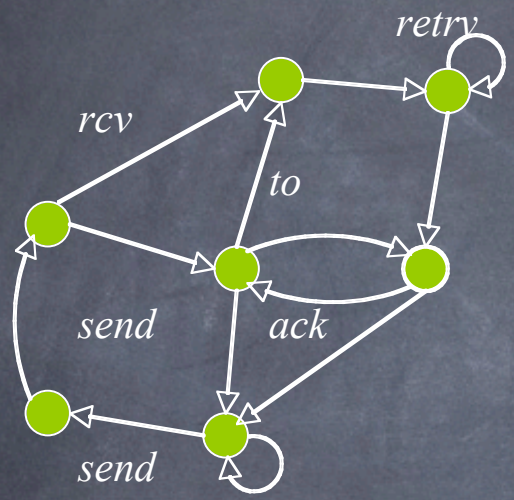
- Model Checking
- Asercionales
- Algebras de Procesos
- Basadas en relaciones

- Concurrentes/distribuidos
- Componentes aleatorias
- Tiempo real
- Tolerancia a fallas
- Seguridad

Semántica


Mo Ch ing
Co rentes/dis
Aserciona
C s aleat
Al ras Procesos
T o
Ba s en relaci
T fallas
Segu d
Sem ca

Model checking Tradicional

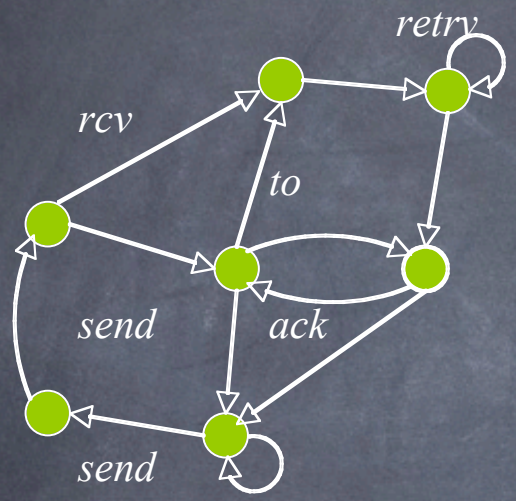


$\models$ G (send(msg) => F rcv(msg))

CONICET

FaMAF

Model checking Tradicional



$\models$ G (send(msg) => F rcv(msg))

Comportamiento no determinista

Las propiedades sólo pueden ser verdaderas o falsas

CONICET

FaMAF

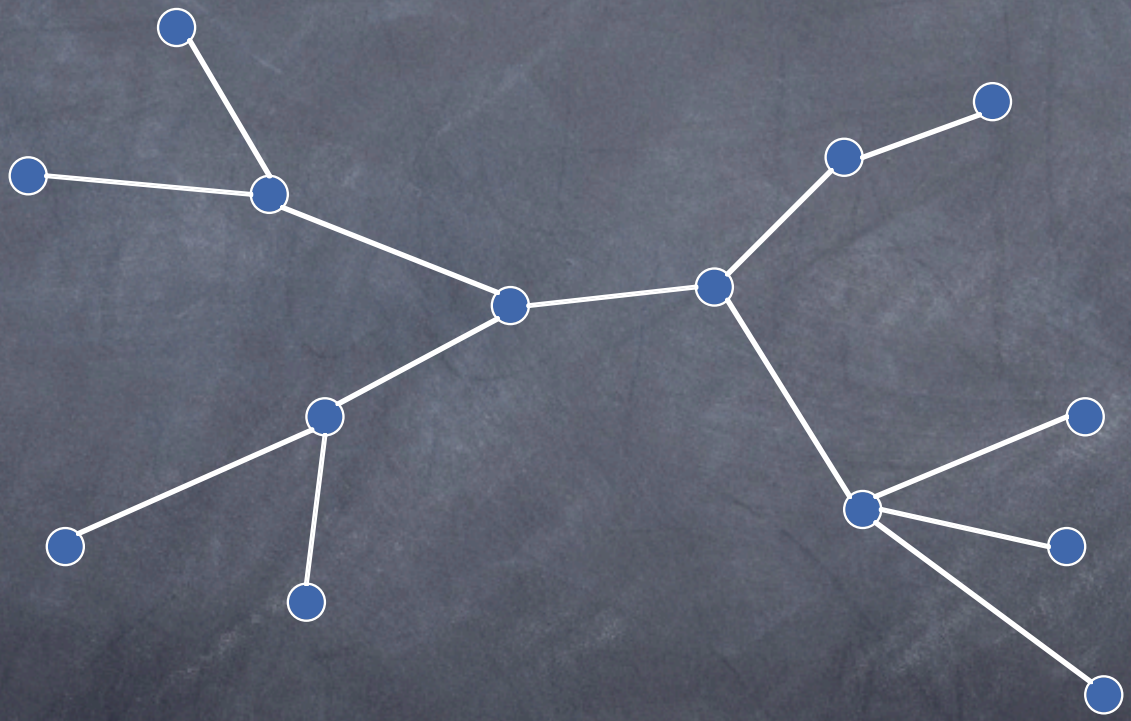
Problemas en el MC tradicional

Sin embargo:

- Muchos algoritmos proponen (mejores) soluciones utilizando soluciones aleatorias
- Ej
  - Leader Election Protocol en IEEE 1394 "Firewire"
  - Binary Exponential Backoff Algorithm en IEEE 802.3 "Ethernet"

Problemas en el MC tradicional

Ej: IEEE 1394 Leader election protocol

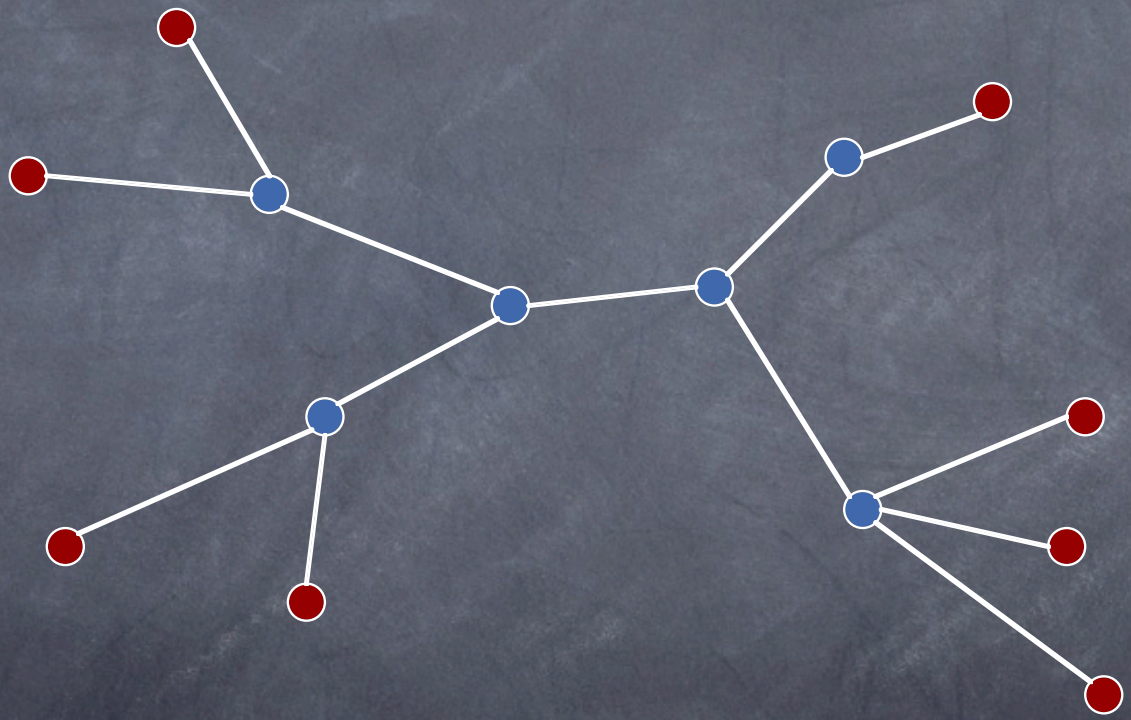


CONICET

FaMAF

Problemas en el MC tradicional

Ej: IEEE 1394 Leader election protocol

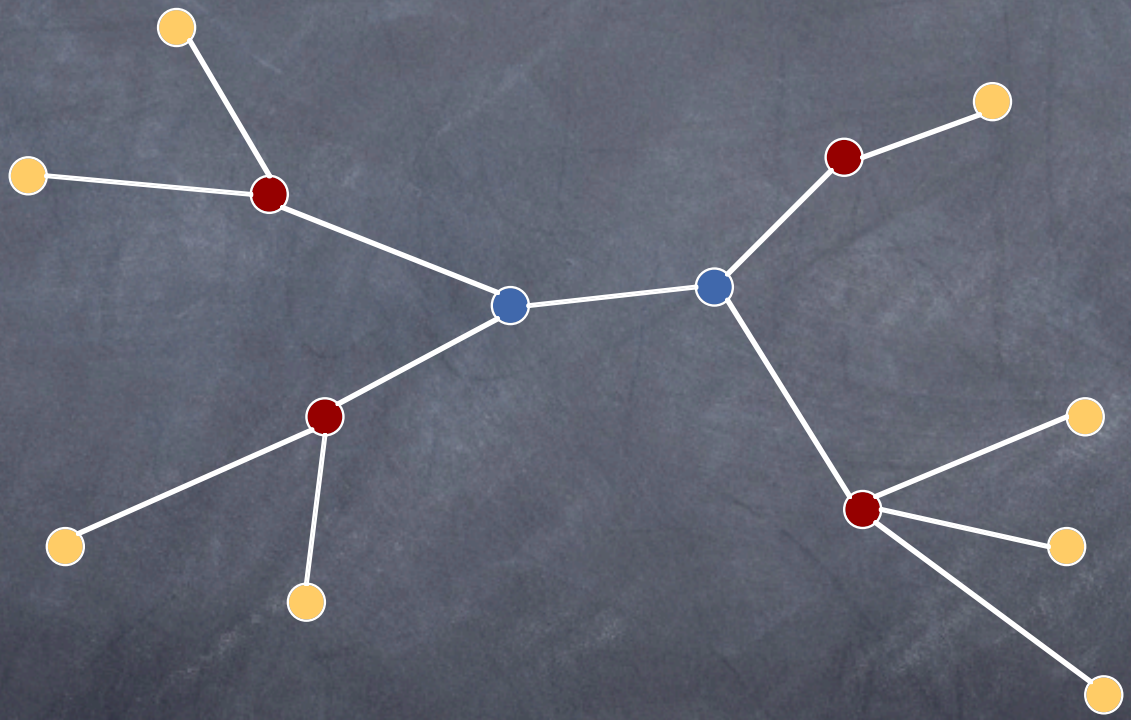


CONICET

FaMAF

Problemas en el MC tradicional

Ej: IEEE 1394 Leader election protocol

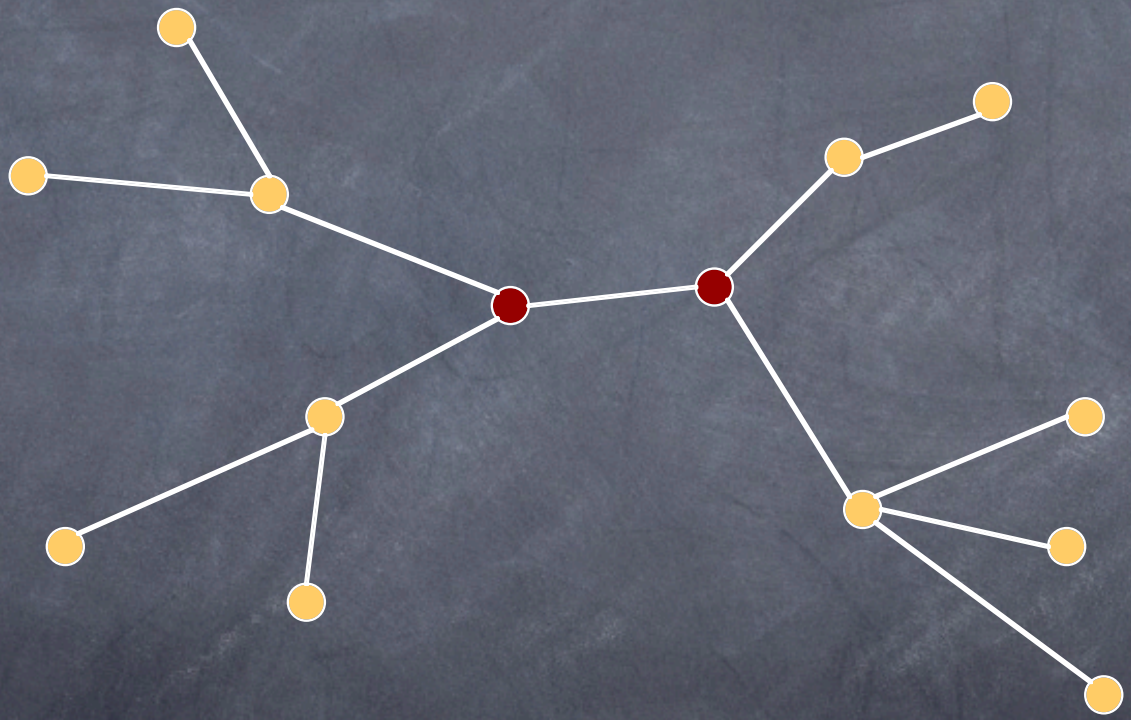


CONICET

FaMAF

Problemas en el MC tradicional

Ej: IEEE 1394 Leader election protocol



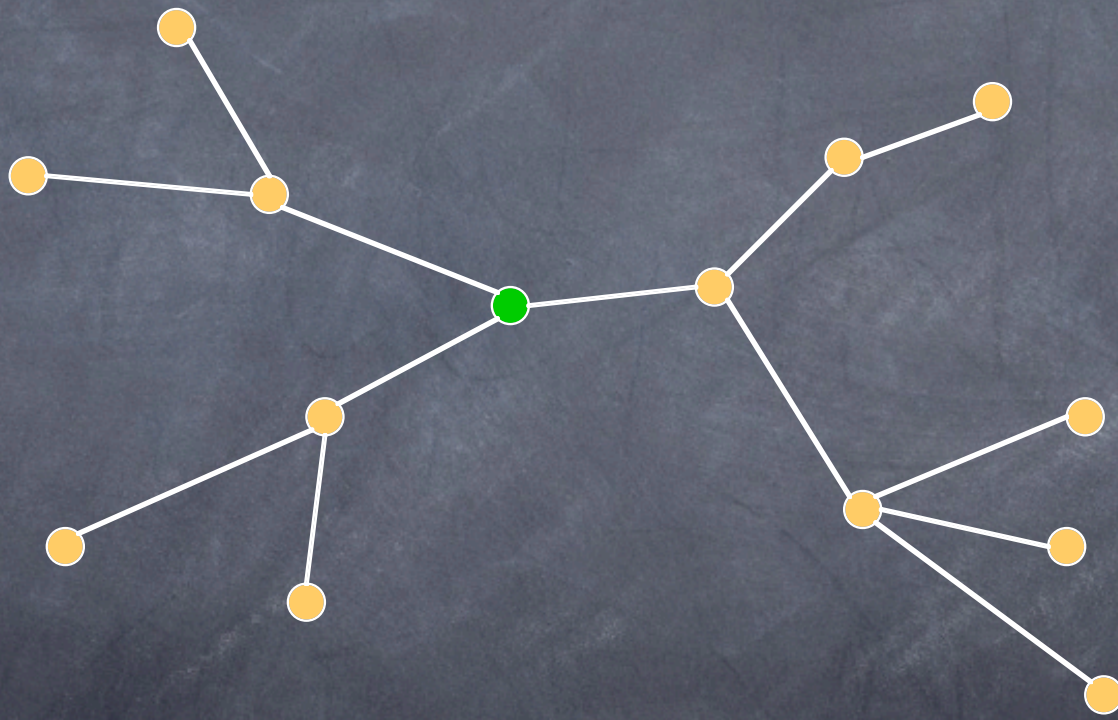
Root contention!

CONICET

FaMAF

Problemas en el MC tradicional

Ej: IEEE 1394 Leader election protocol



Se soluciona "tirando una moneda"

CONICET

FaMAF

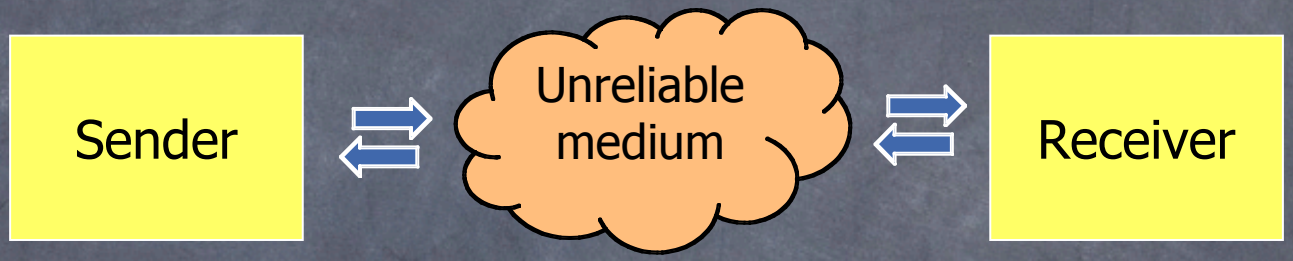
Problemas en el MC tradicional

Sin embargo:

- Muchas veces, la corrección no se puede establecer cualitativamente. En cambio la validez de una propiedad sólo puede medirse cuantitativamente
- Ej:
  - Bounded Retransmission Protocol en Philips RC6
  - Binary Exponential Backoff Algorithm en IEEE 802.3 "Ethernet"

Problemas en el MC tradicional

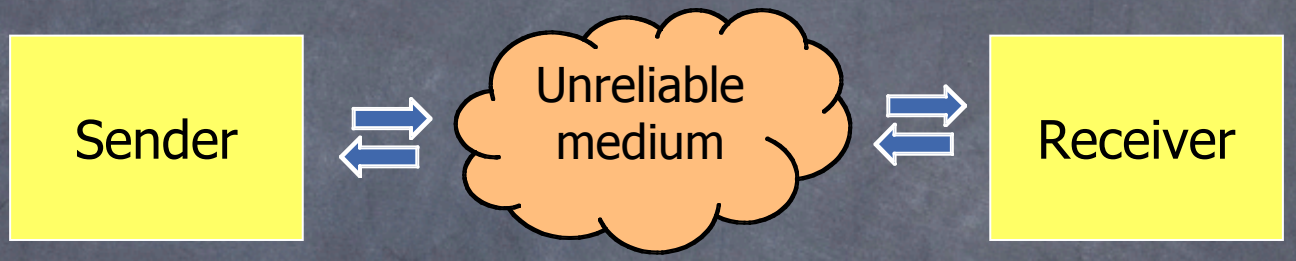
Supongamos la transmisión de un archivo usando un protocolo como el ABP o el de ventanas deslizante:



G (send(msg) => F rcv(msg))

Problemas en el MC tradicional

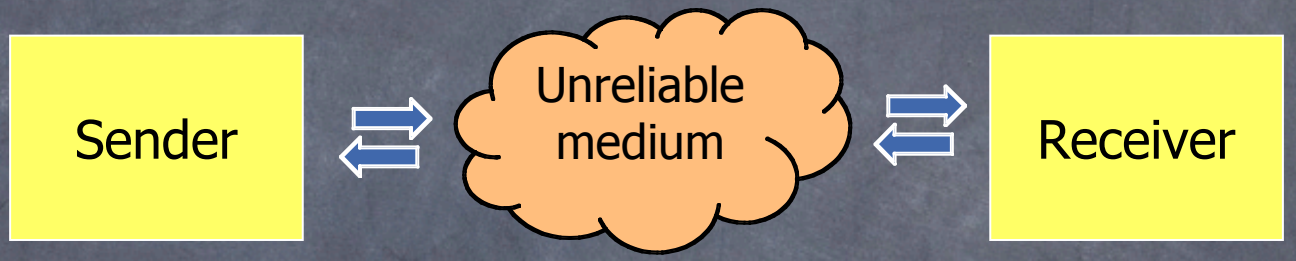
Supongamos la transmisión de un archivo usando un protocolo como el ABP o el de ventanas deslizante:



✔ G (send(msg) => F rcv(msg))

Problemas en el MC tradicional

Supongamos la transmisión de un archivo usando un protocolo como el ABP o el de ventanas deslizante:

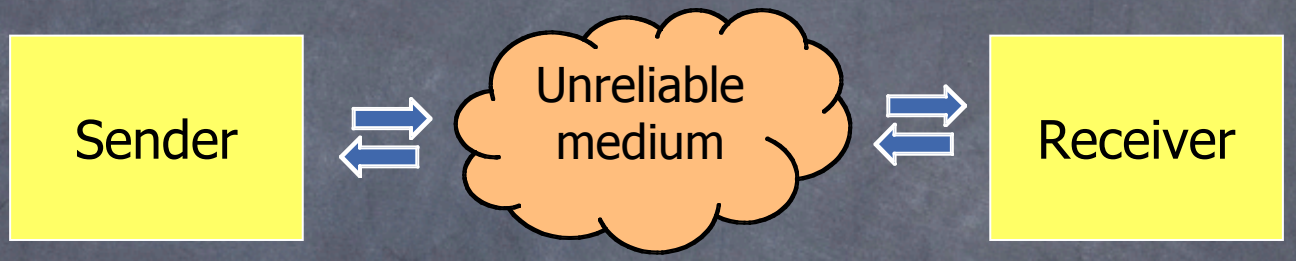


✔ G (send(msg) => F rcv(msg))

bajo la suposición que el protocolo puede reintentar transmitir infinitamente

Problemas en el MC tradicional

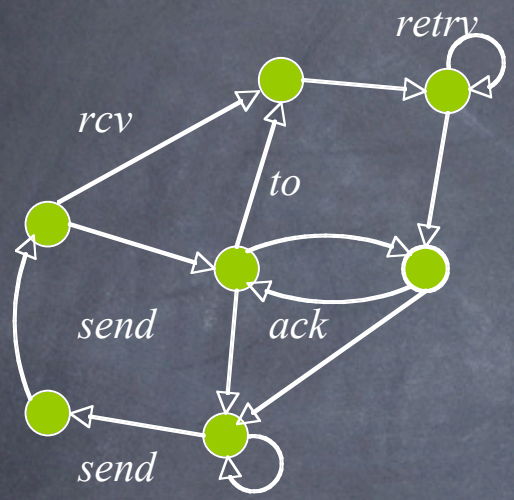
Supongamos la transmisión de un archivo usando un protocolo como el ABP o el de ventanas deslizante:



✗ G (send(msg) => F rcv(msg))

Pero si sólo se permite un número acotado de retransmisiones (Ej: BRP)...

Problemas en el MC tradicional



$\models$ G (send(msg) => F rcv(msg))

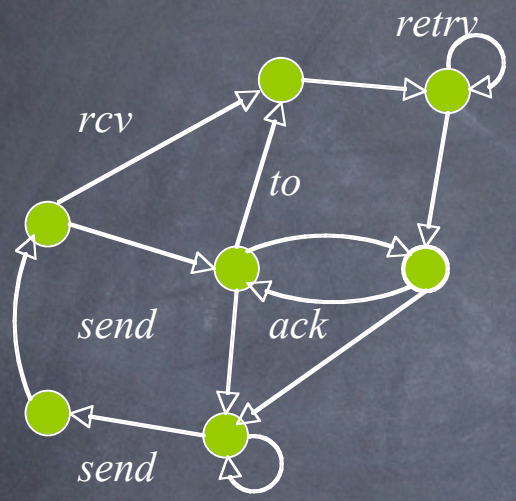
Las propiedades sólo pueden ser verdaderas o falsas

Comportamiento no determinista

CONICET

FaMAF

Problemas en el MC tradicional



$\models$ G (send(msg) => F rcv(msg))

El valor de verdad deben estar cuantificado probabilisticamente

También debe considerar el comportamiento probabilista

CONICET

FaMAF

Si no hay no-determinismo...

Calcular las probabilidades es simple:

estamos en la presencia de una cadena de Markov

Prob(F ●) =

Si no hay no-determinismo...

Calcular las probabilidades es simple:

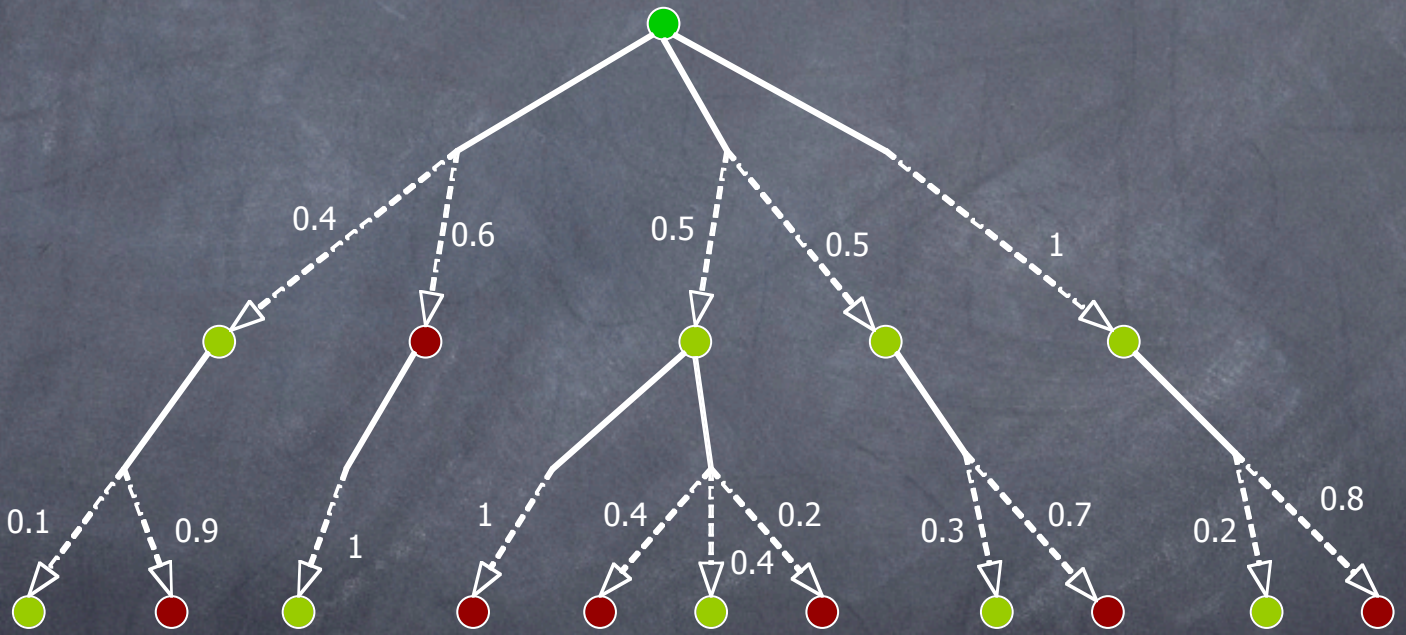
estamos en la presencia de una cadena de Markov

Prob(F ●) = 0.5*(0.4+0.2) + 0.5*0.7 = 0.65

CONICET

FaMAF

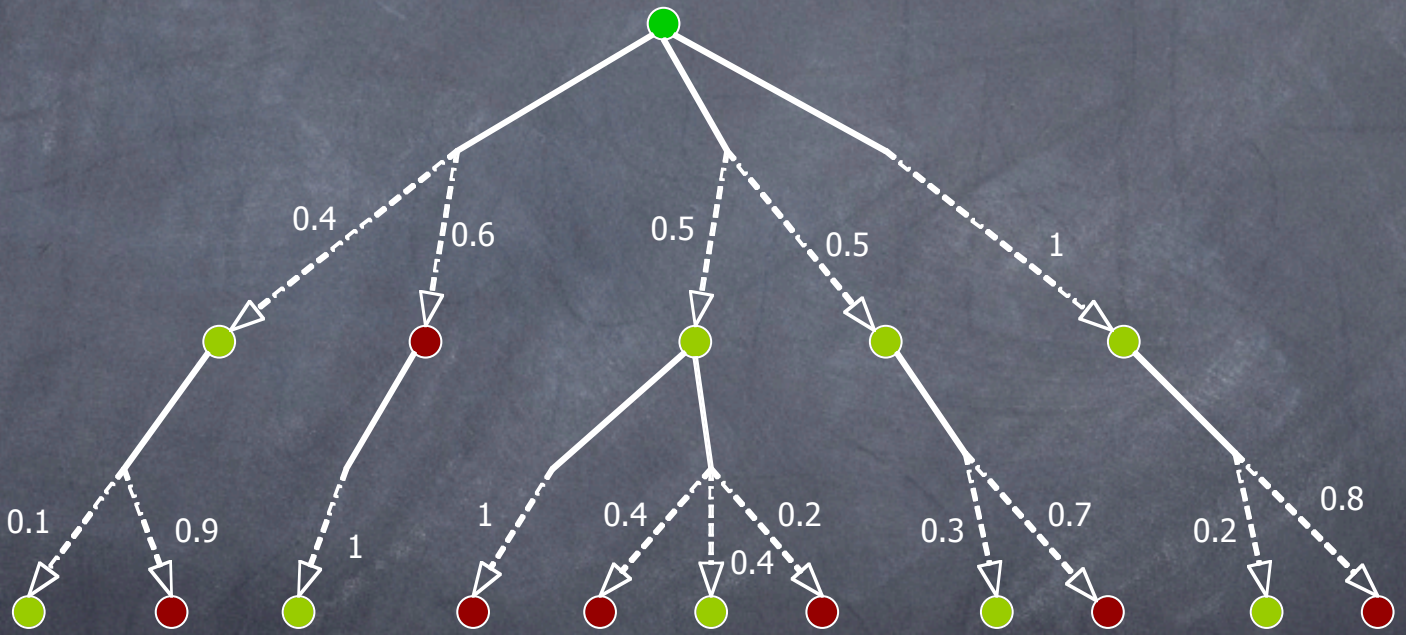
Pero si hay no-determinismo...



Pero si hay no-determinismo...

=> Usar Schedulers

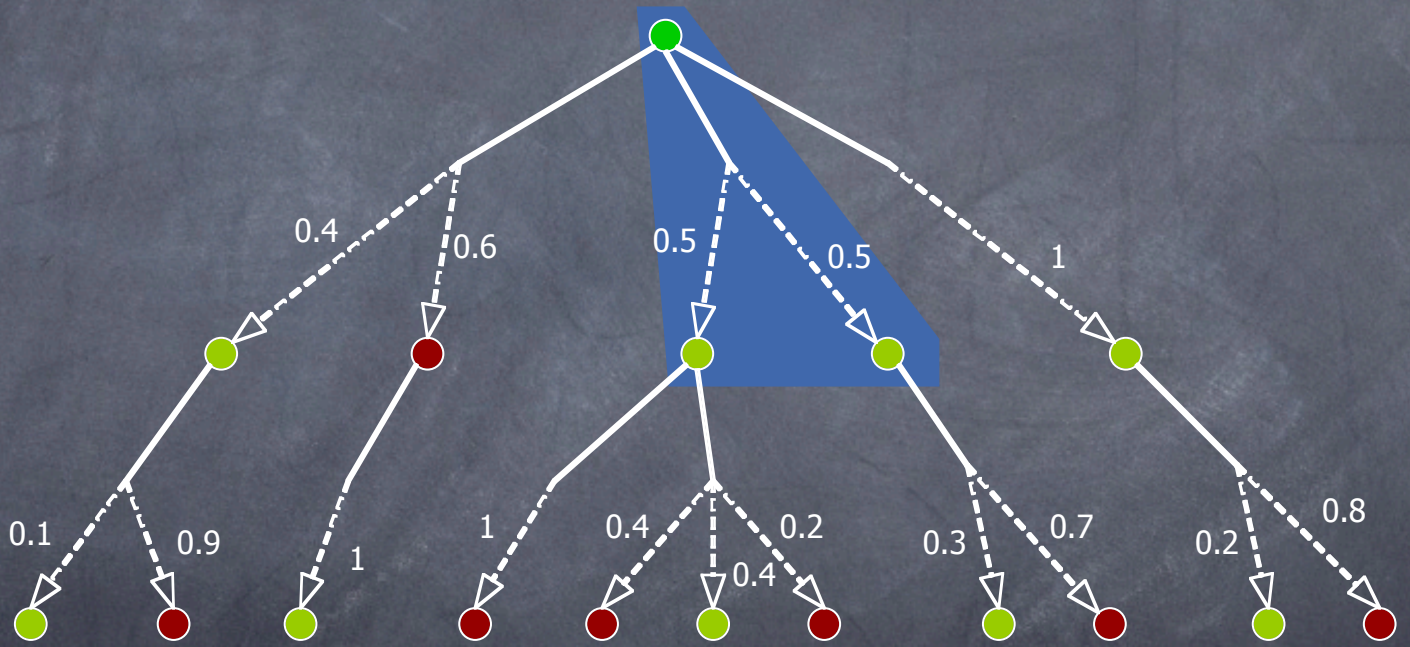
Son funciones que resuelven el nodeterminismo



Pero si hay no-determinismo...

=> Usar Schedulers

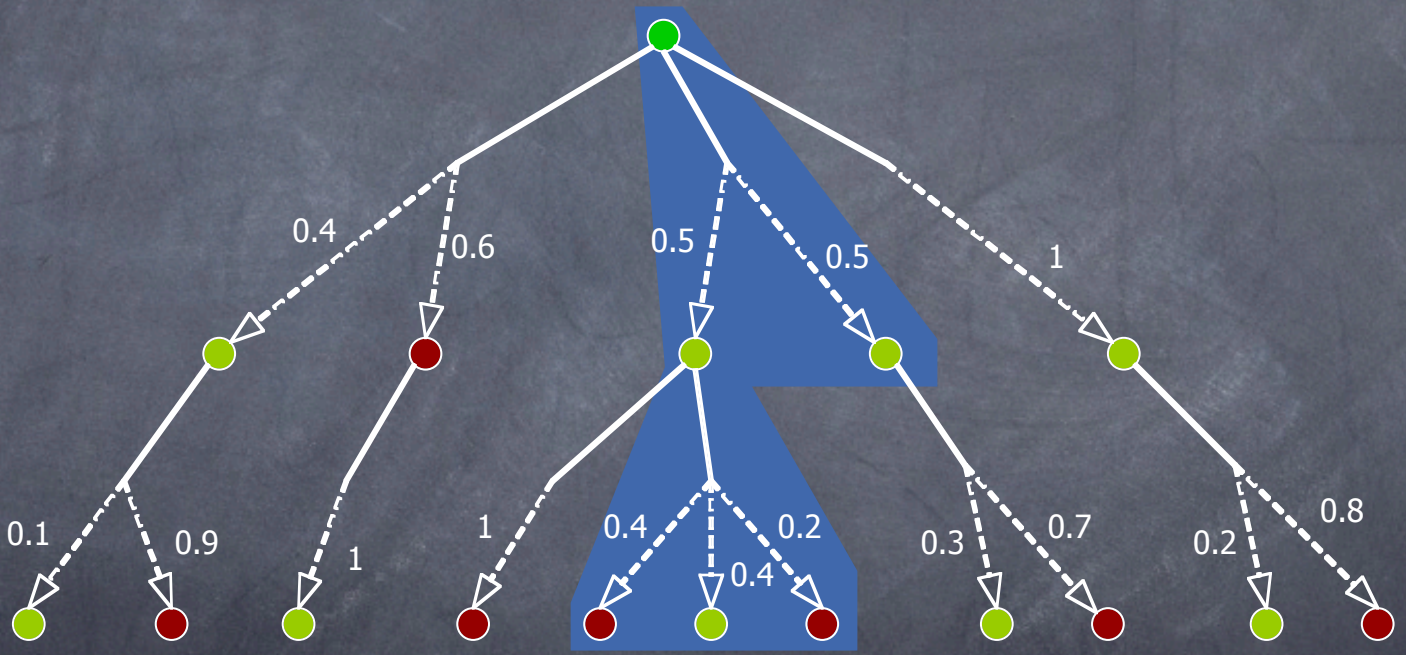
Son funciones que resuelven el nodeterminismo



Pero si hay no-determinismo...

=> Usar Schedulers

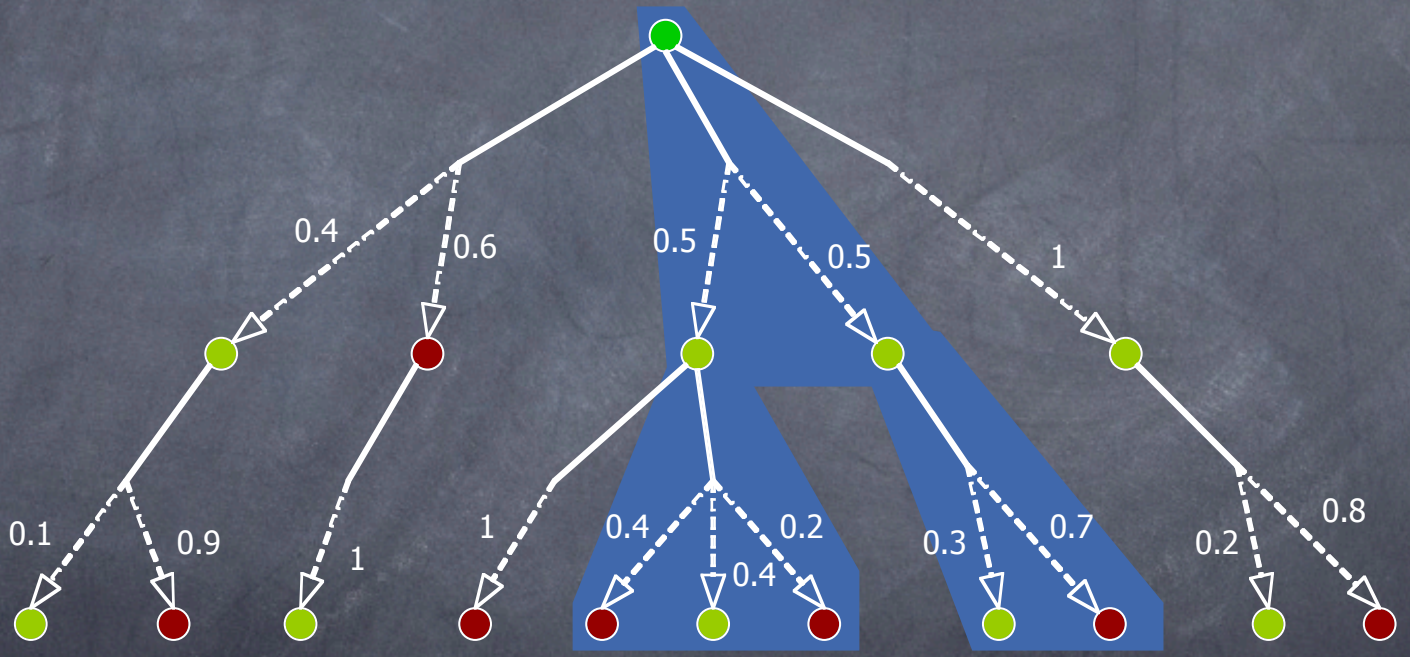
Son funciones que resuelven el nodeterminismo



Pero si hay no-determinismo...

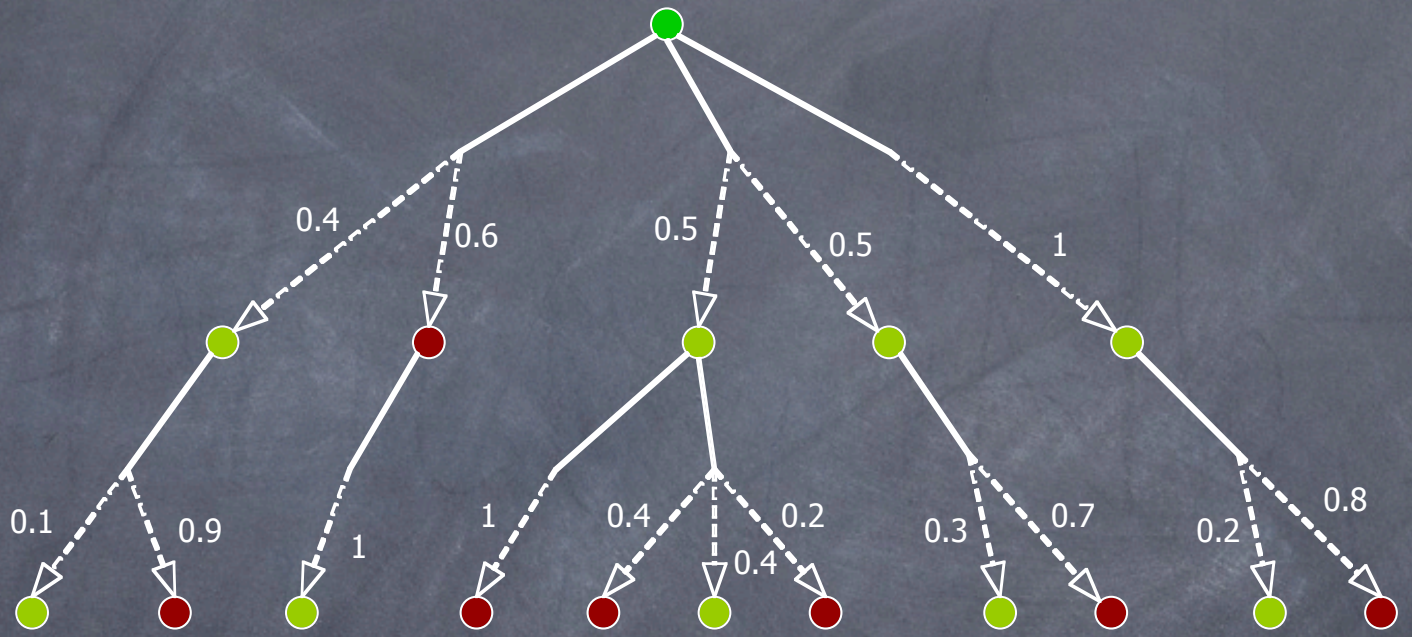
=> Usar Schedulers

Son funciones que resuelven el nodeterminismo

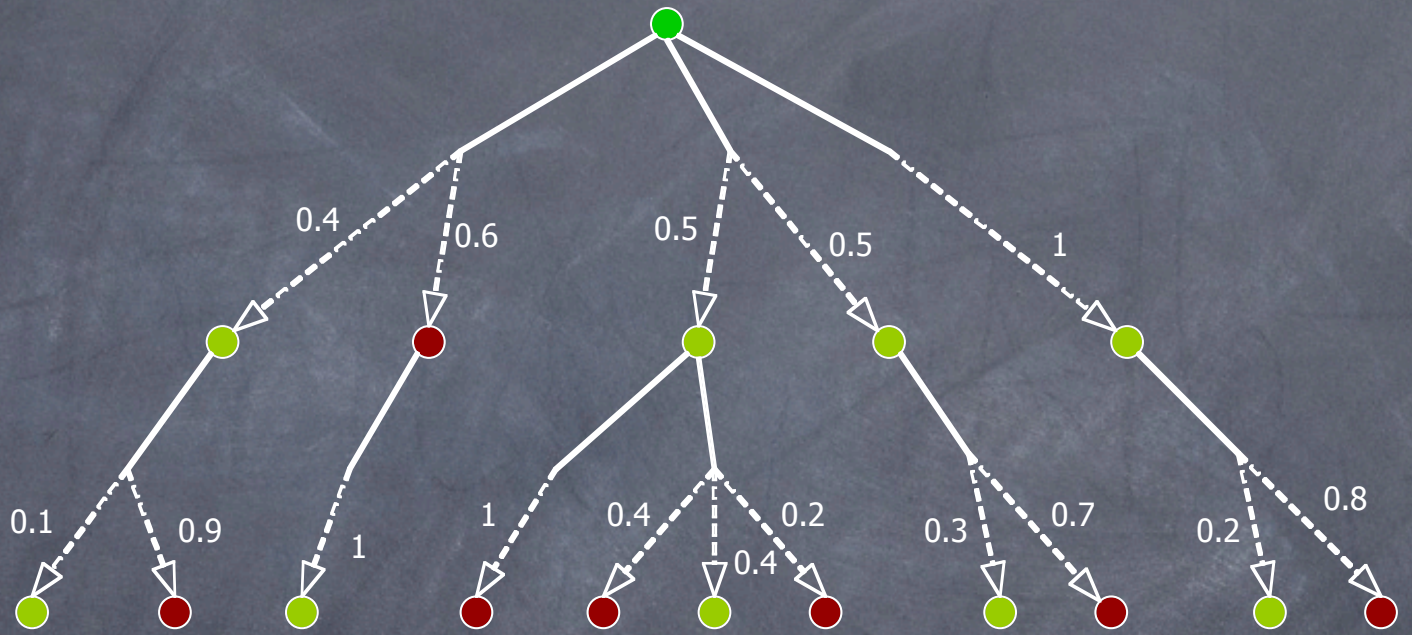


Un scheduler selecciona un árbol probabilista

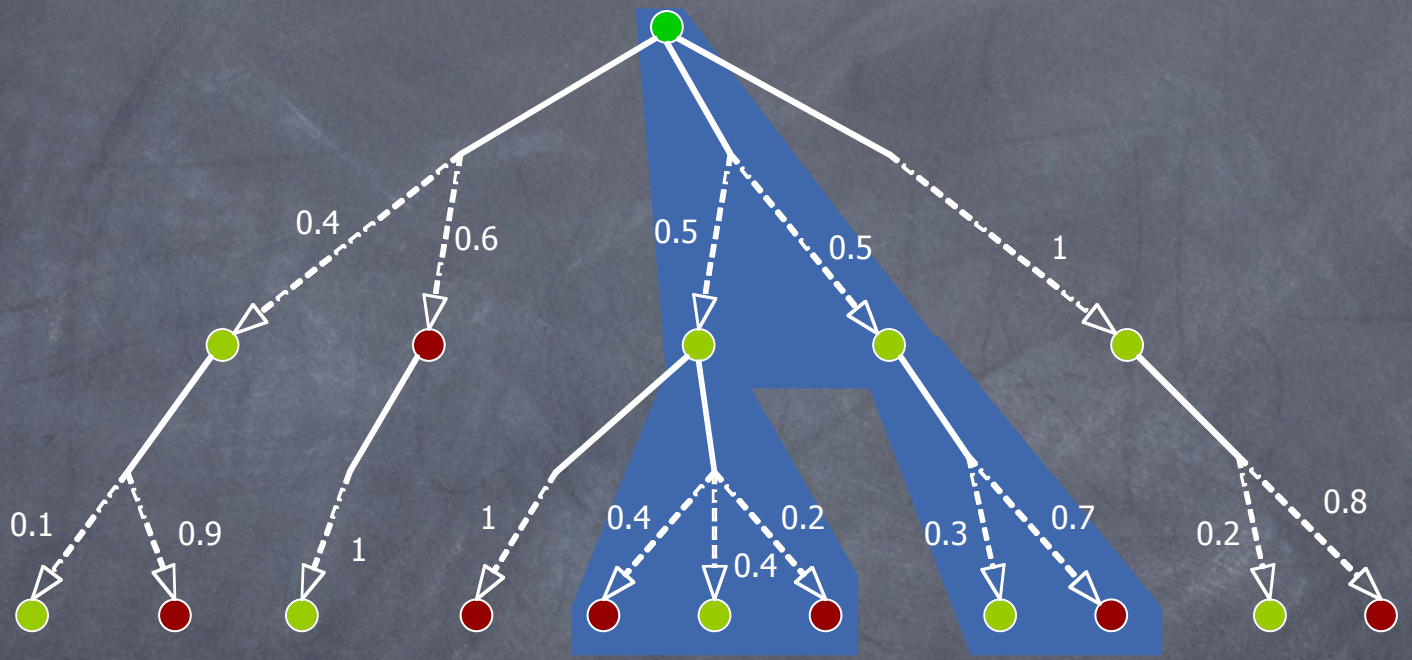
Pero si hay no-determinismo...



Pero si hay no-determinismo...

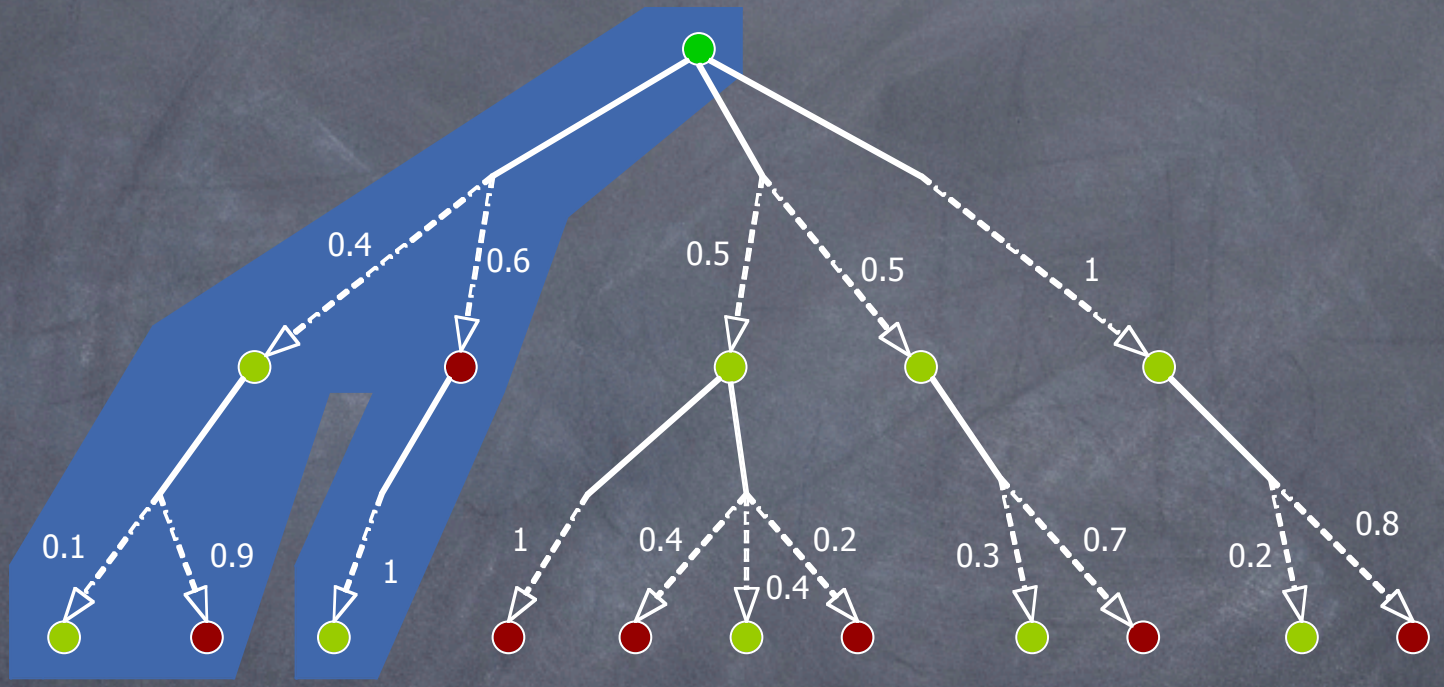


Pero si hay no-determinismo...



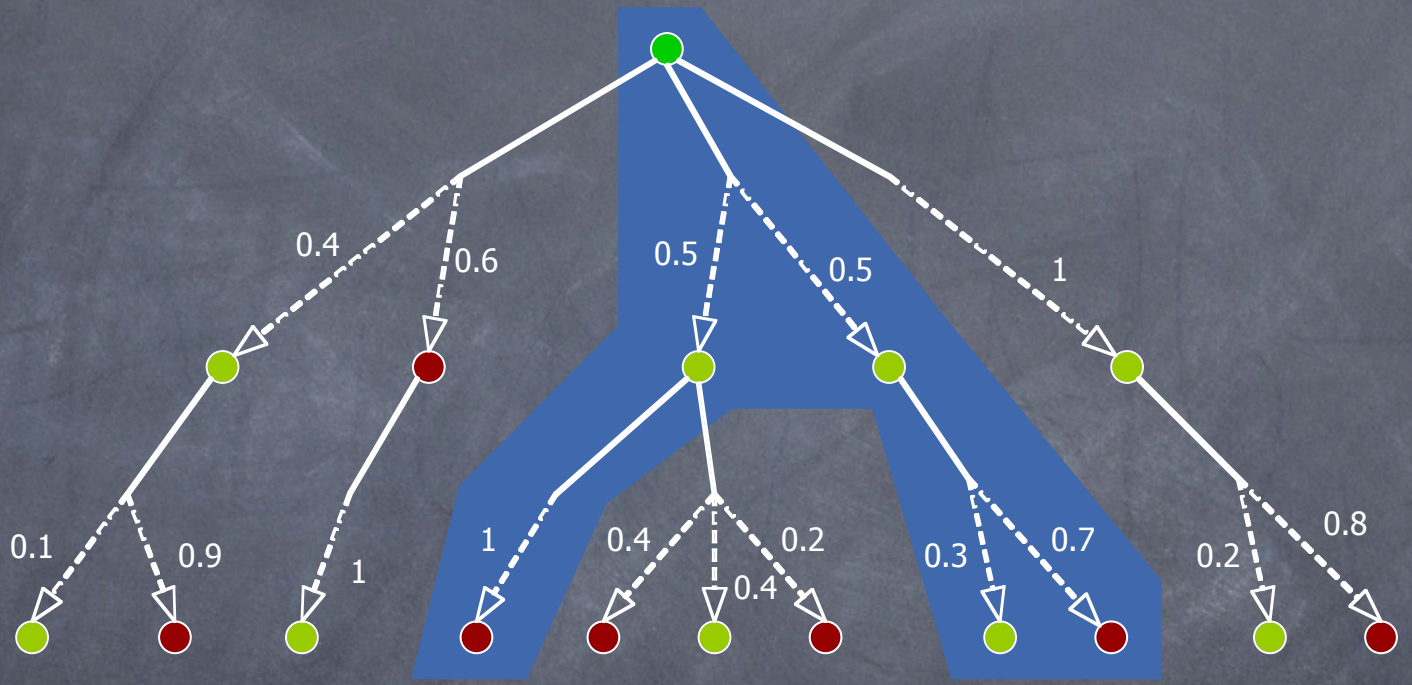
Prob(F ●) = 0.65

Pero si hay no-determinismo...



Prob(F ●) = 0.96

Pero si hay no-determinismo...

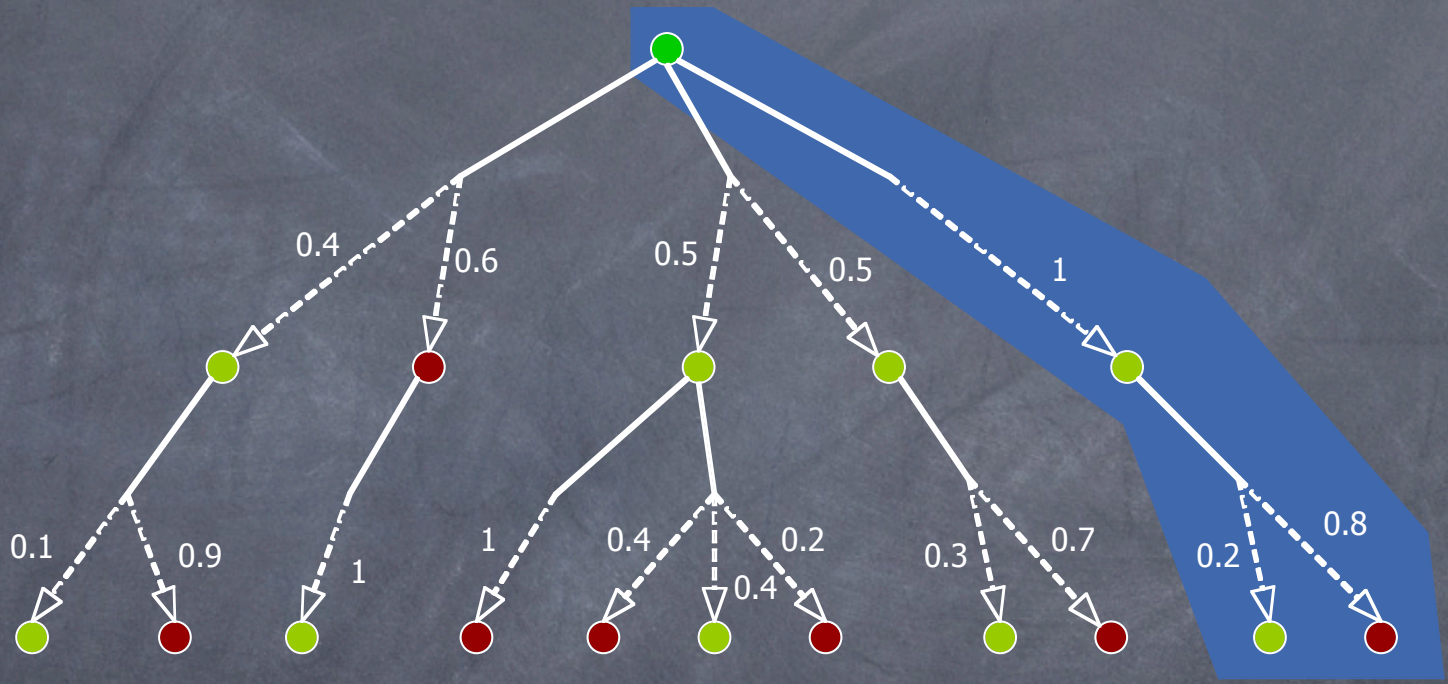


Prob(F ●) = 0.85

CONICET

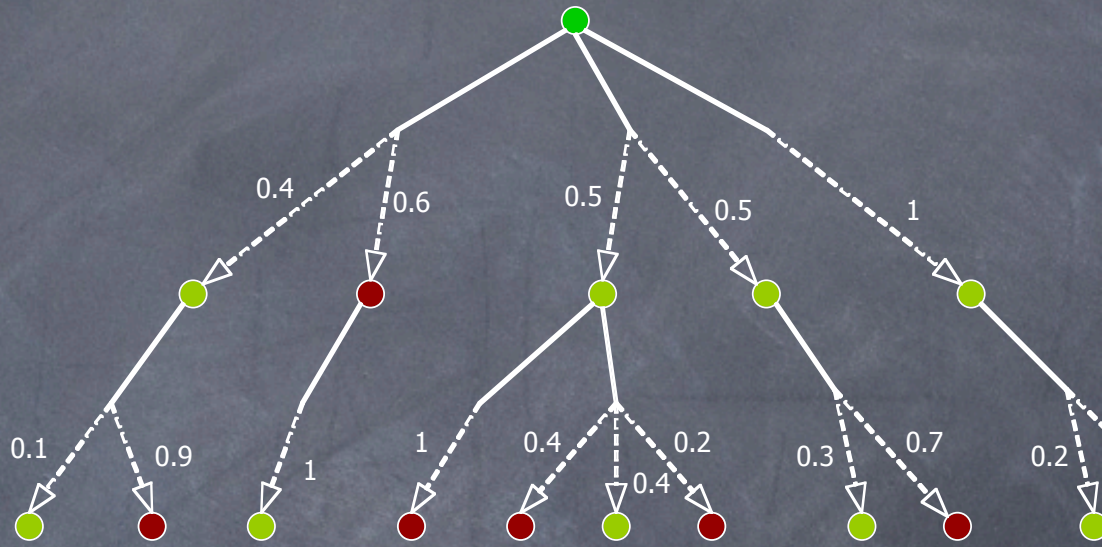
FaMAF

Pero si hay no-determinismo...



Prob(F ●) = 0.8

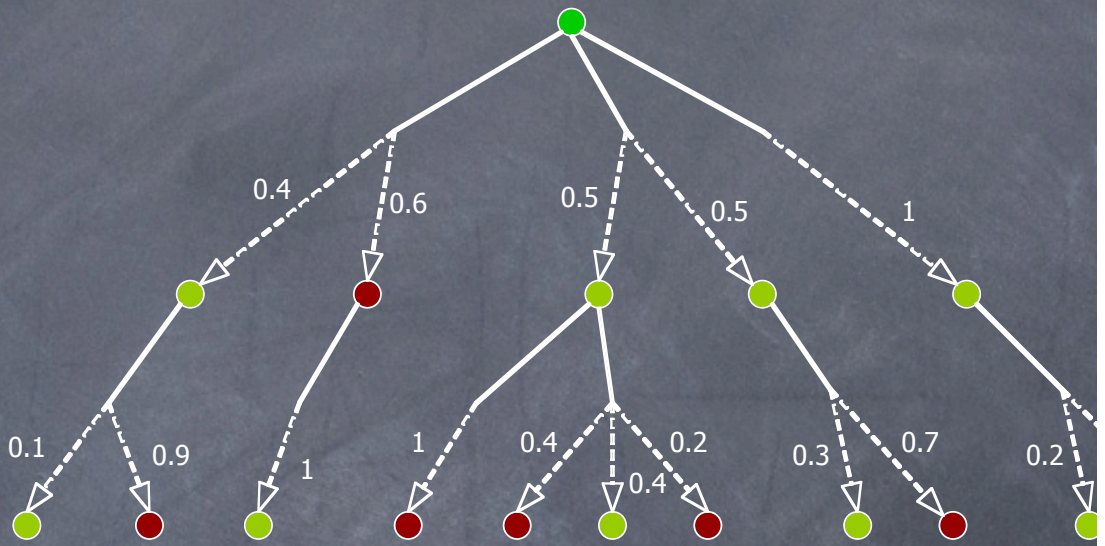
Pero si hay no-determinismo...



Pero si hay no-determinismo...

Entonces:

¿cuál es la probabilidad?



Prob(F ●) = 0.96

Prob(F ●) = 0.85

Prob(F ●) = 0.65

Prob(F ●) = 0.8

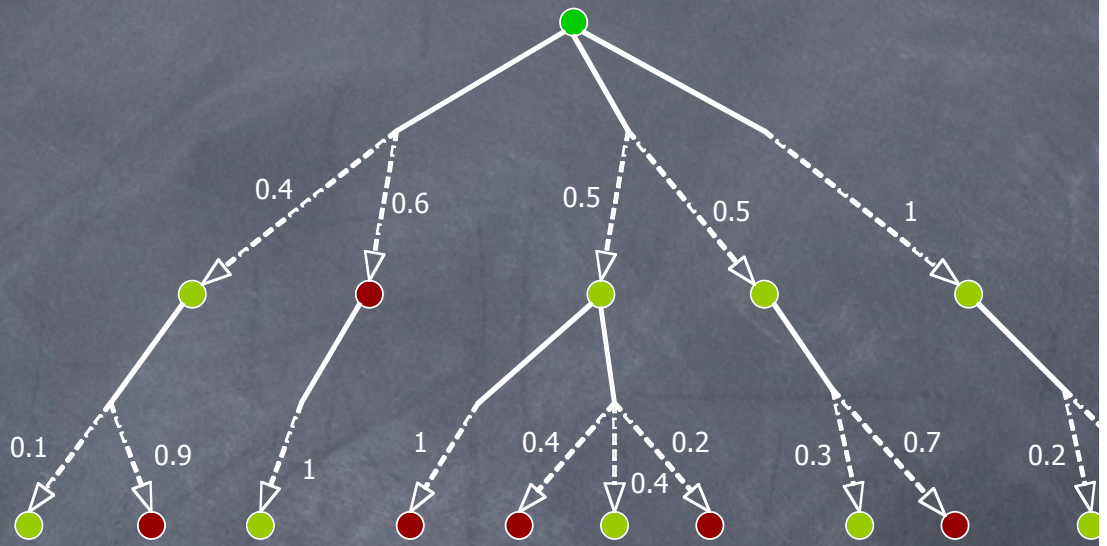
CONICET

FaMAF

Pero si hay no-determinismo...

Entonces:

¿cuál es la probabilidad?



La máxima entre todos los posibles schedulers:

$P_{max}(\ F \bullet\ ) = 0.96$

Y la mínima entre todos los posibles schedulers:

$P_{min}(\ F \bullet\ ) = 0.65$

Prob(F ●) = 0.96

Prob(F ●) = 0.85

Prob(F ●) = 0.65

Prob(F ●) = 0.8

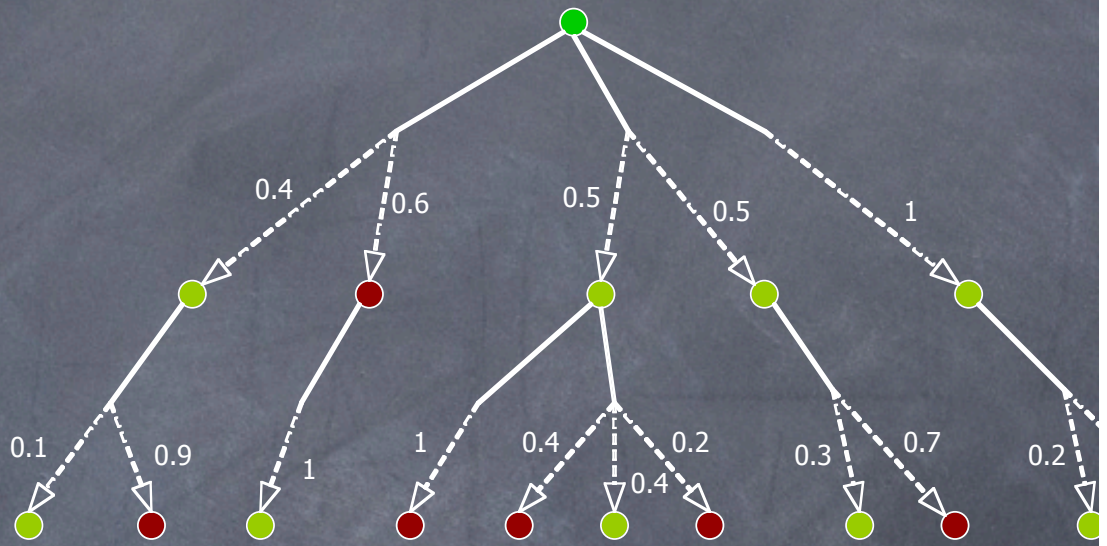
CONICET

FaMAF

Pero si hay no-determinismo...

Entonces:

¿cuál es la probabilidad?



La máxima entre todos los posibles schedulers:

$P_{max}(\ F\ \bullet\ ) = 0.96$

Y la mínima entre todos los posibles schedulers:

$P_{min}(\ F\ \bullet\ ) = 0.65$

I.e.: la interpretación de una fórmula en un sistema es un par (maxProb, minProb)

CONICET

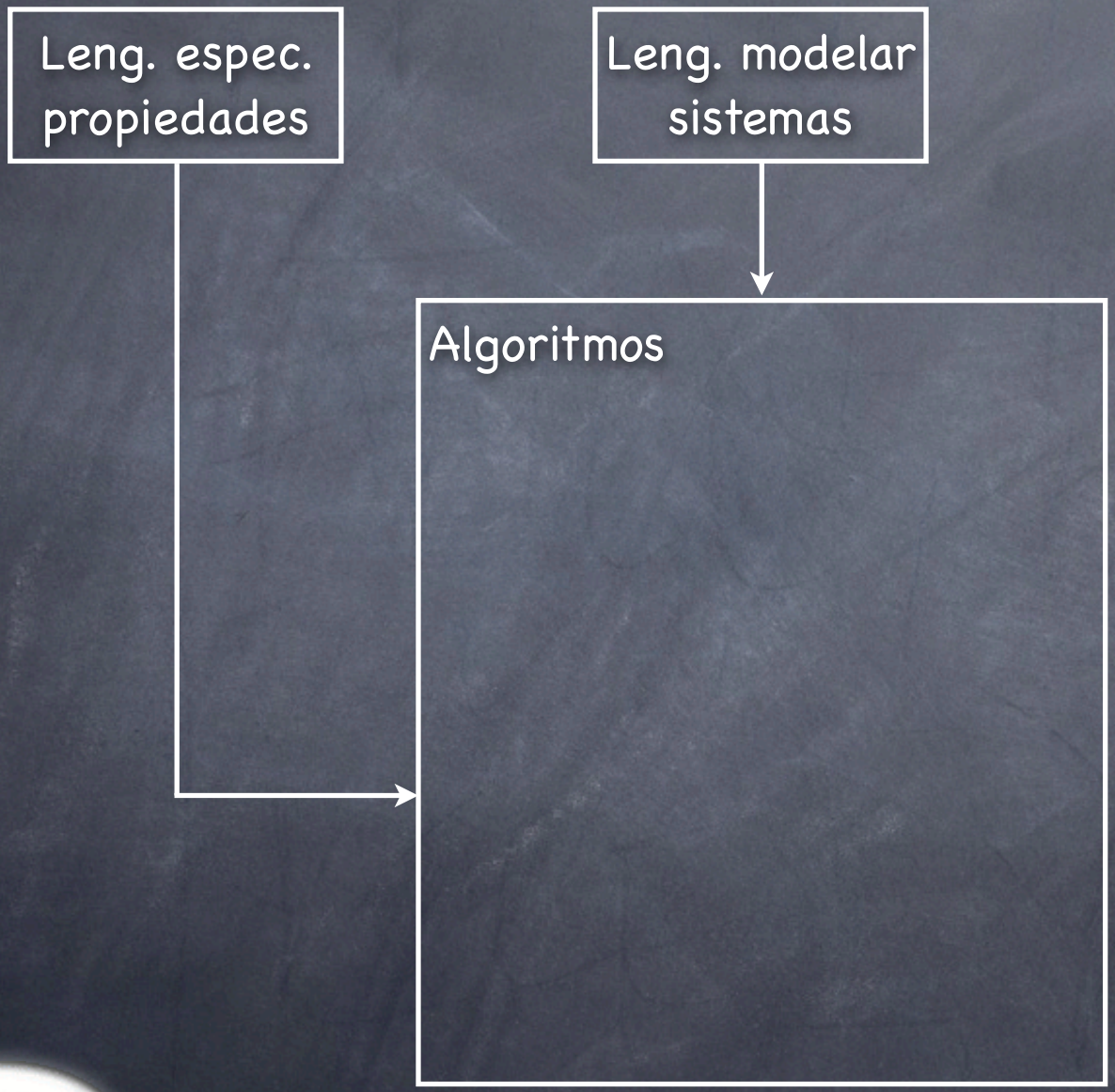
FaMAF

¿Qué estamos haciendo?

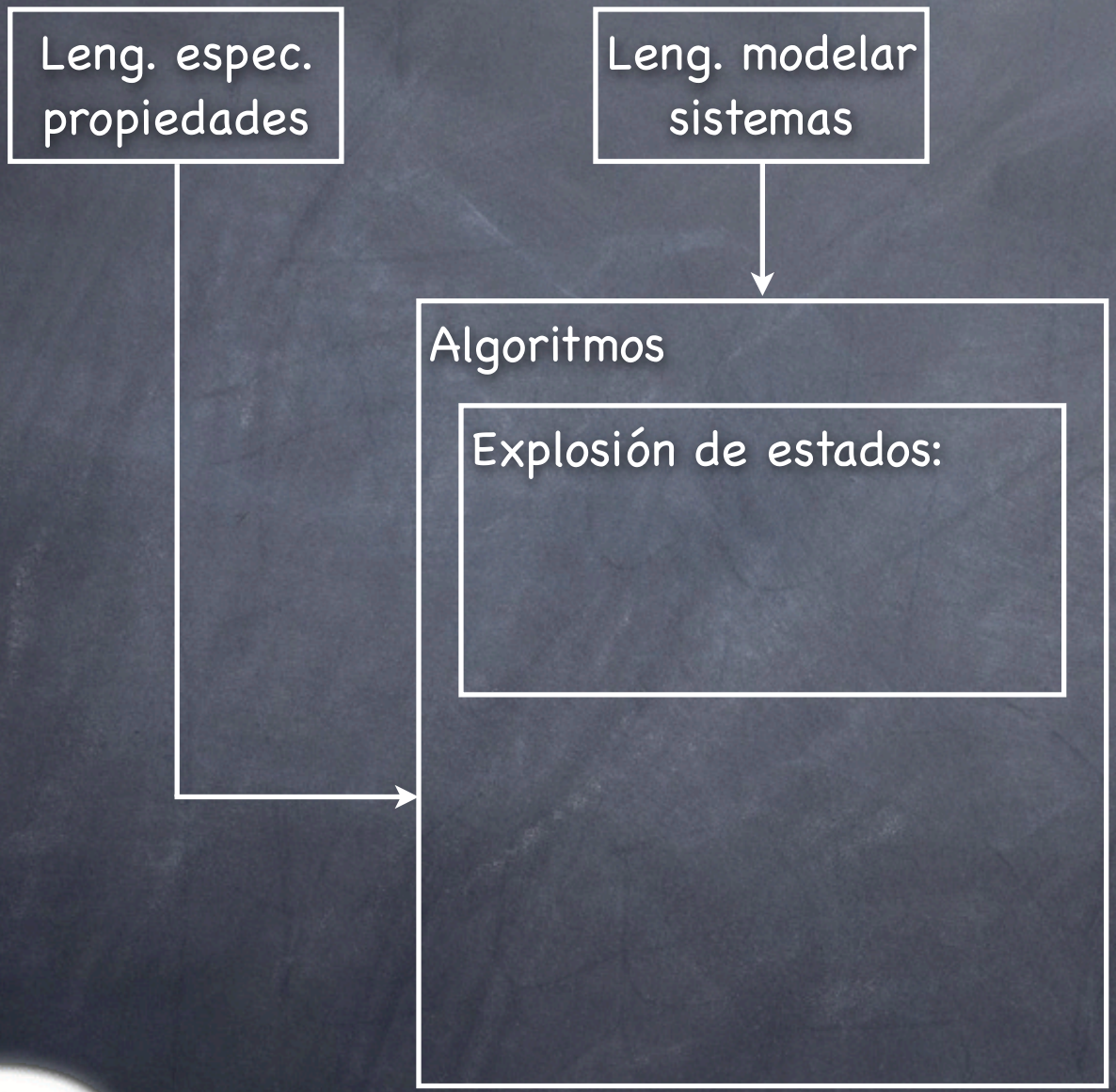
Leng. espec. propiedades

Leng. modelar sistemas

¿Qué estamos haciendo?



¿Qué estamos haciendo?



CONICET

FaMAF

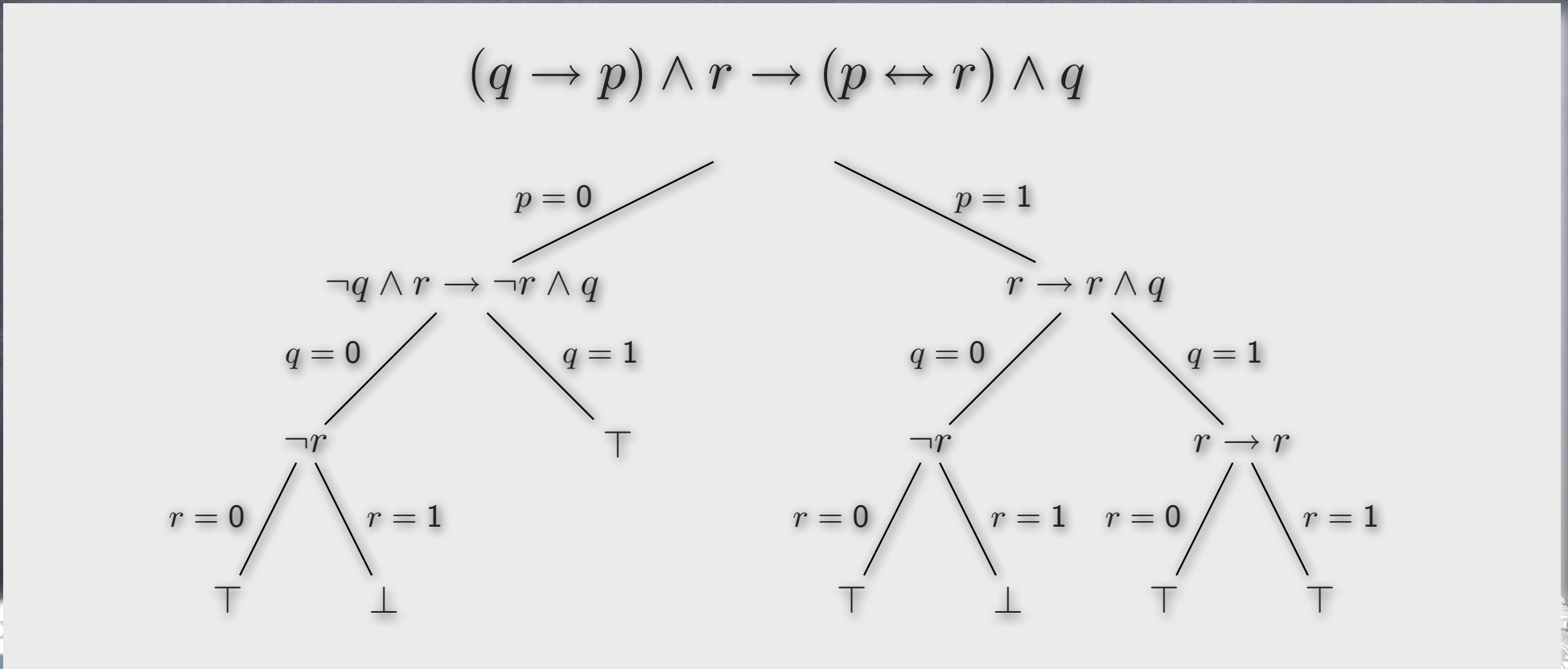
¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta

$$(q \rightarrow p) \wedge r \rightarrow (p \leftrightarrow r) \wedge q$$

¿Qué estamos haciendo?

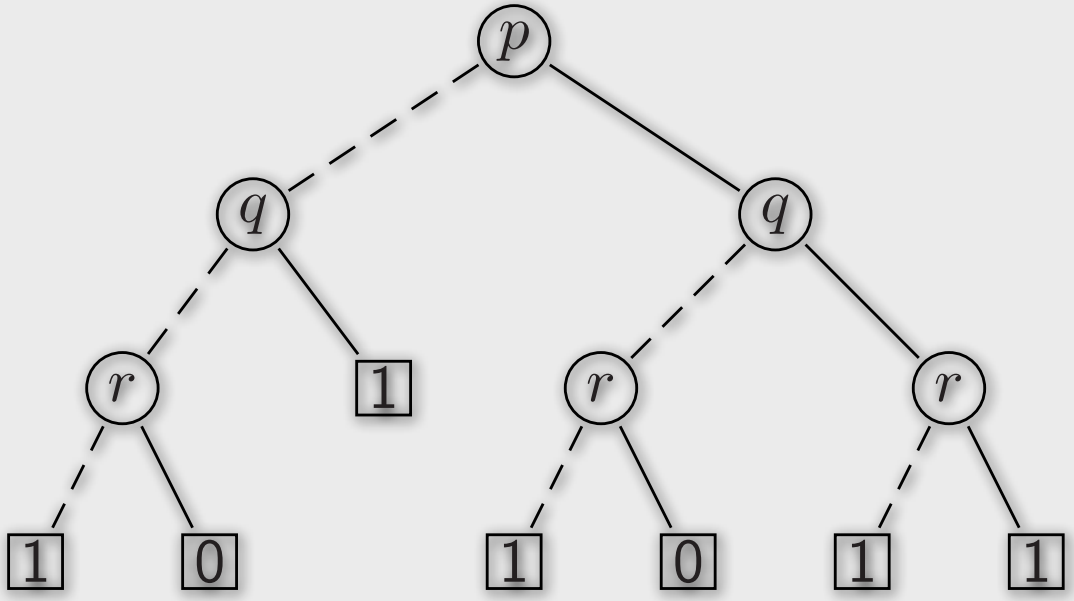
- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta



¿Qué estamos haciendo?

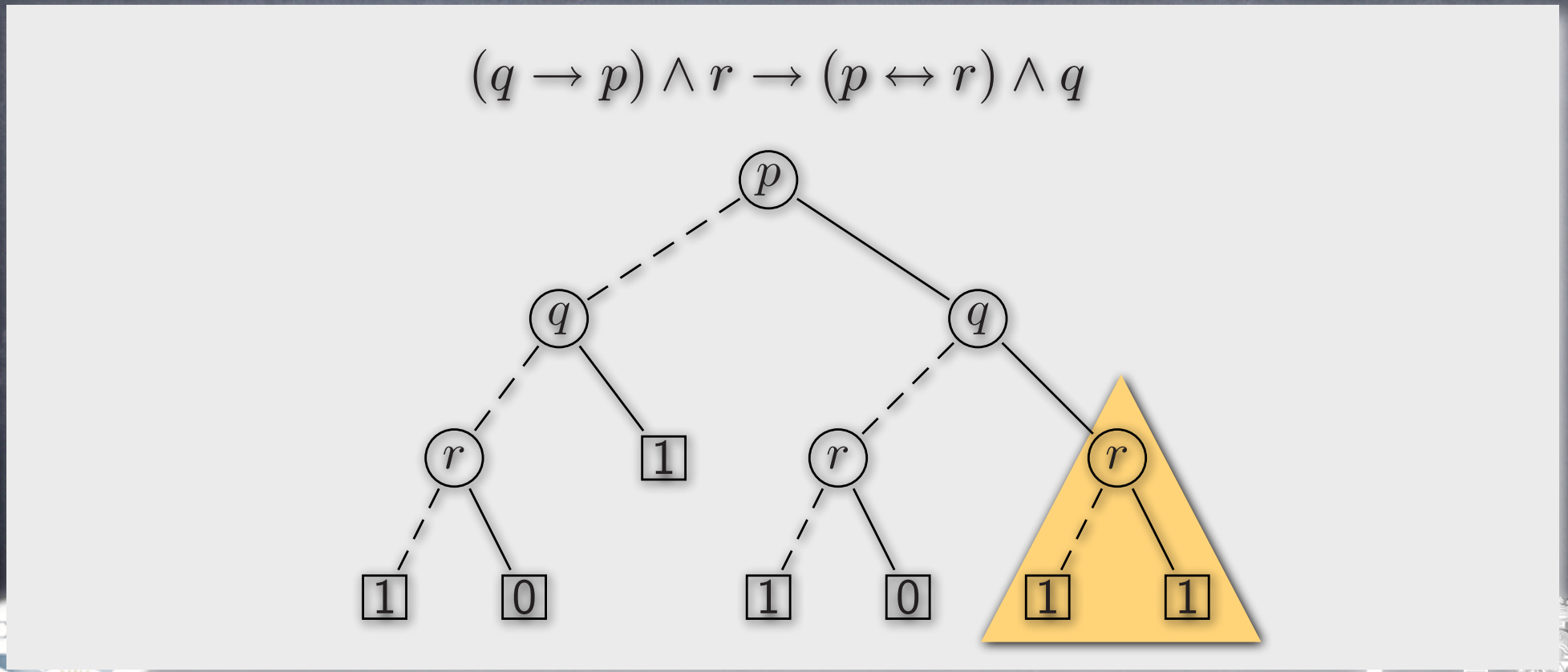
- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta

$$(q \rightarrow p) \wedge r \rightarrow (p \leftrightarrow r) \wedge q$$



¿Qué estamos haciendo?

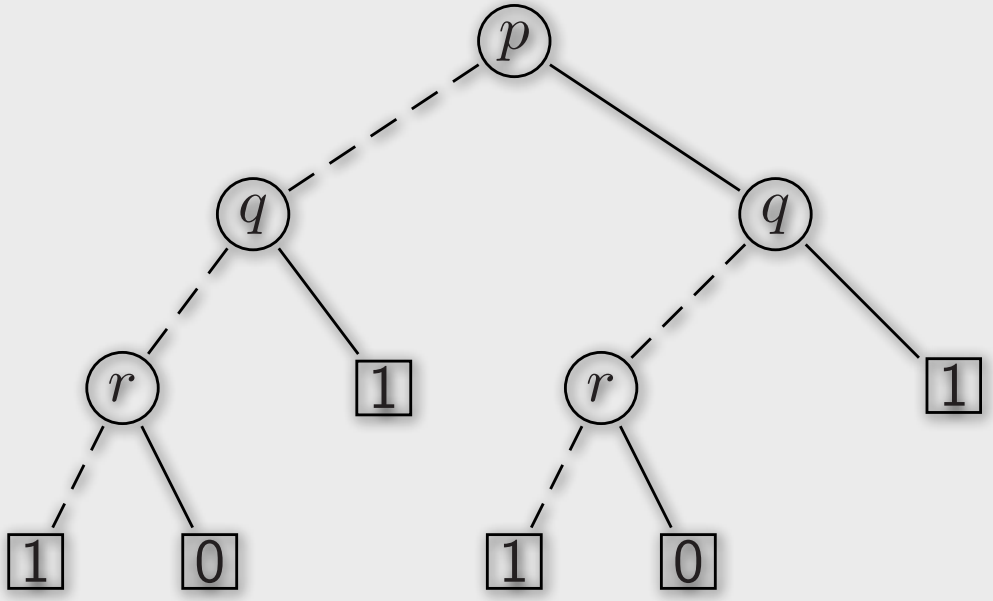
- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta



¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta

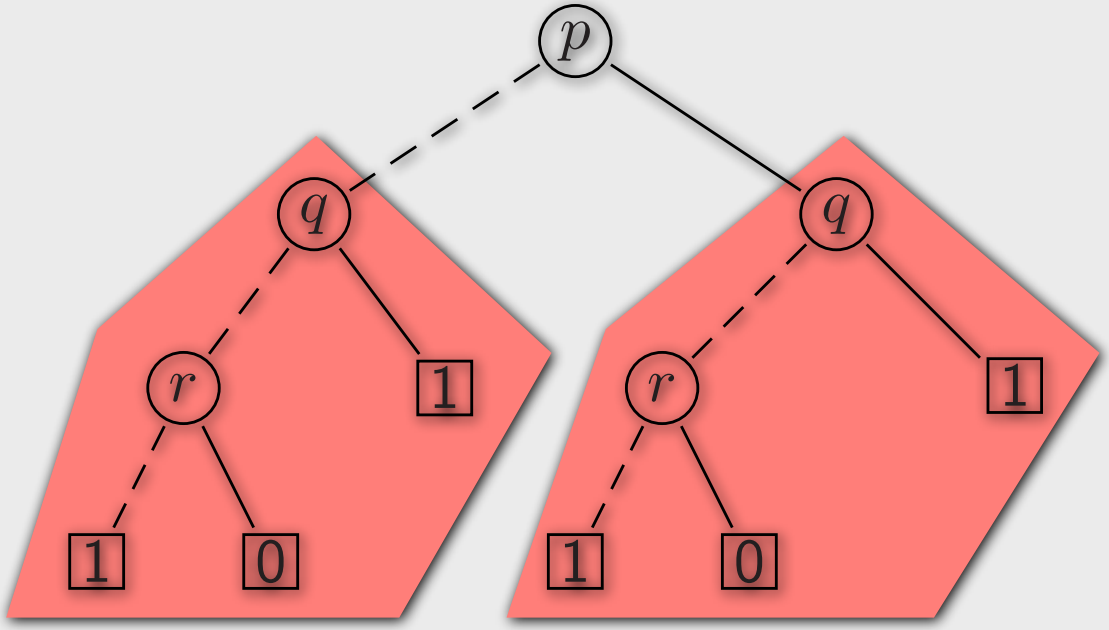
$$(q \rightarrow p) \wedge r \rightarrow (p \leftrightarrow r) \wedge q$$



¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta

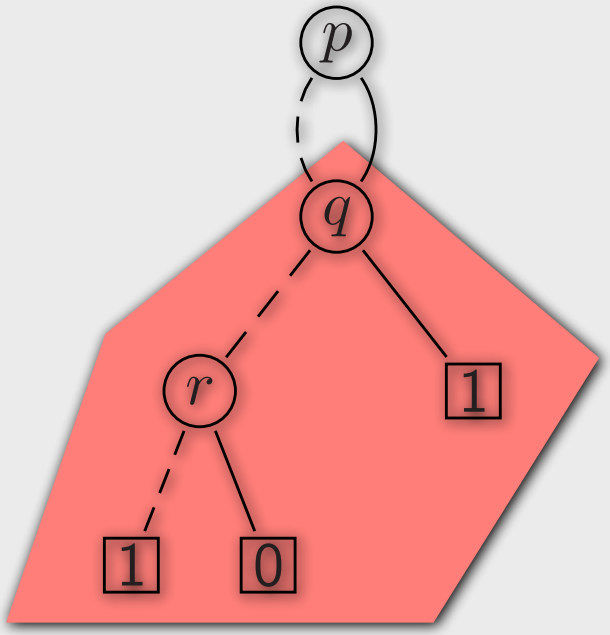
$$(q \rightarrow p) \wedge r \rightarrow (p \leftrightarrow r) \wedge q$$



¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta

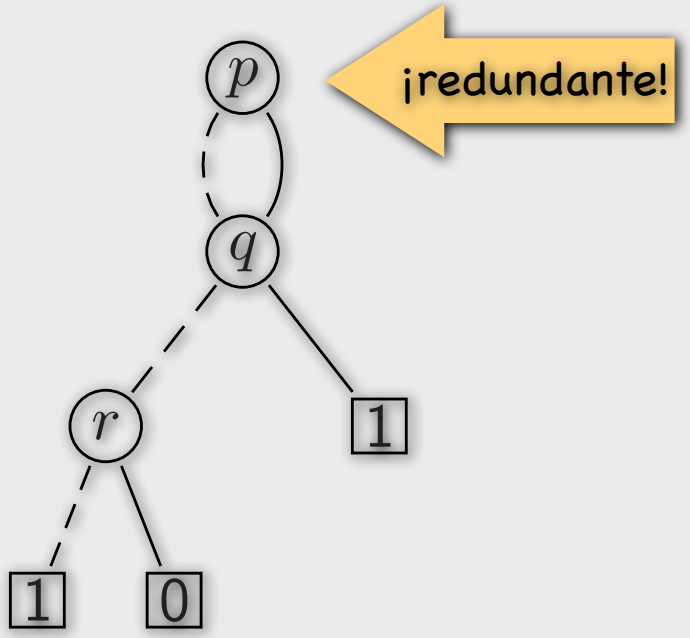
$$(q \rightarrow p) \wedge r \rightarrow (p \leftrightarrow r) \wedge q$$



¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta

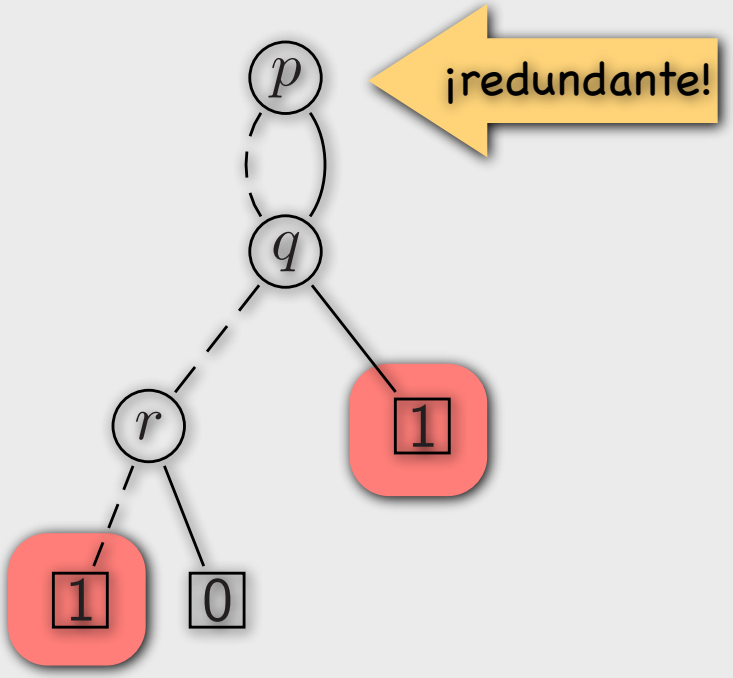
$$(q \rightarrow p) \wedge r \rightarrow (p \leftrightarrow r) \wedge q$$



¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta

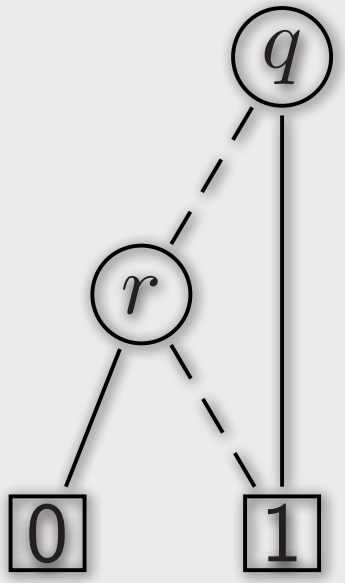
$$(q \rightarrow p) \wedge r \rightarrow (p \leftrightarrow r) \wedge q$$



¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Es inherente en model checking pero...
    - BDD es una buena herramienta

$$(q \rightarrow p) \wedge r \rightarrow (p \leftrightarrow r) \wedge q$$

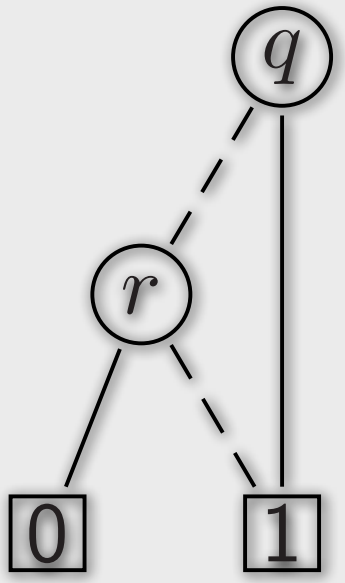


¿Qué estamos hac

- El problema de la explosión de
  - Es inherente en model chec
    - BDD es una buena herramienta

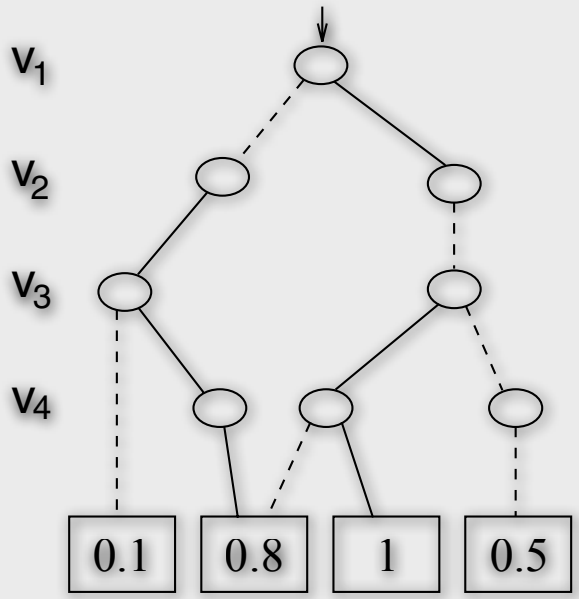
Un estado se puede ver como una tupla de booleanos.
=> un conj. de estados se puede ver como una fórmula

$$(q \rightarrow p) \wedge r \rightarrow (p \leftrightarrow r) \wedge q$$



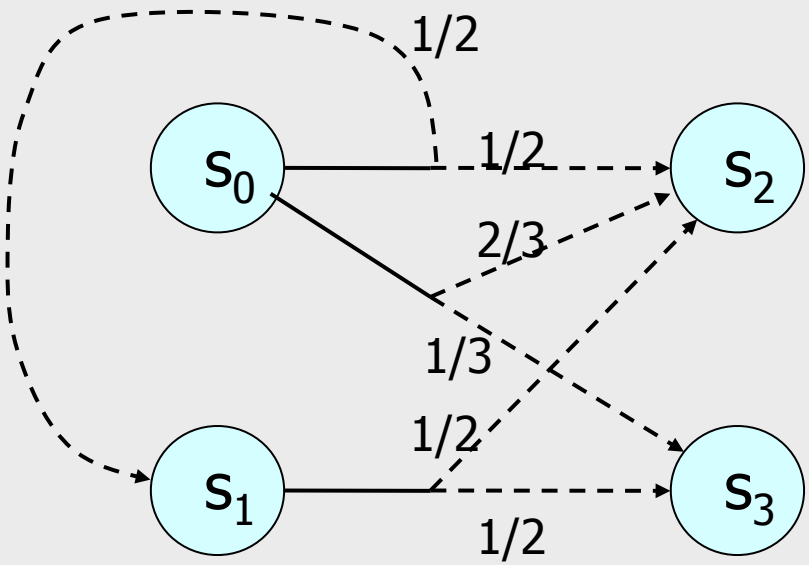
¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Se exacerba en model checking cuantitativo:
    - MTBDD es una buena herramienta... para la representación
    - pero no funciona bien en el análisis numérico



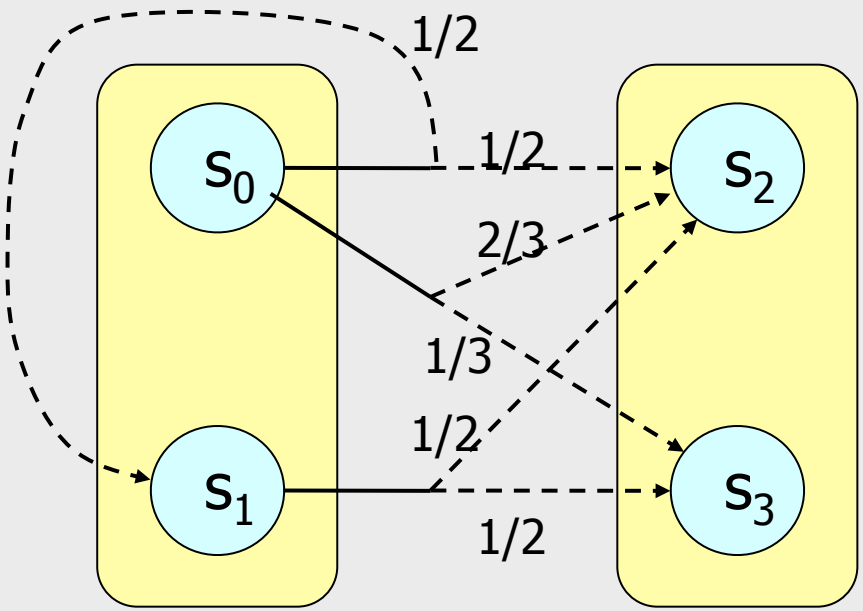
¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]



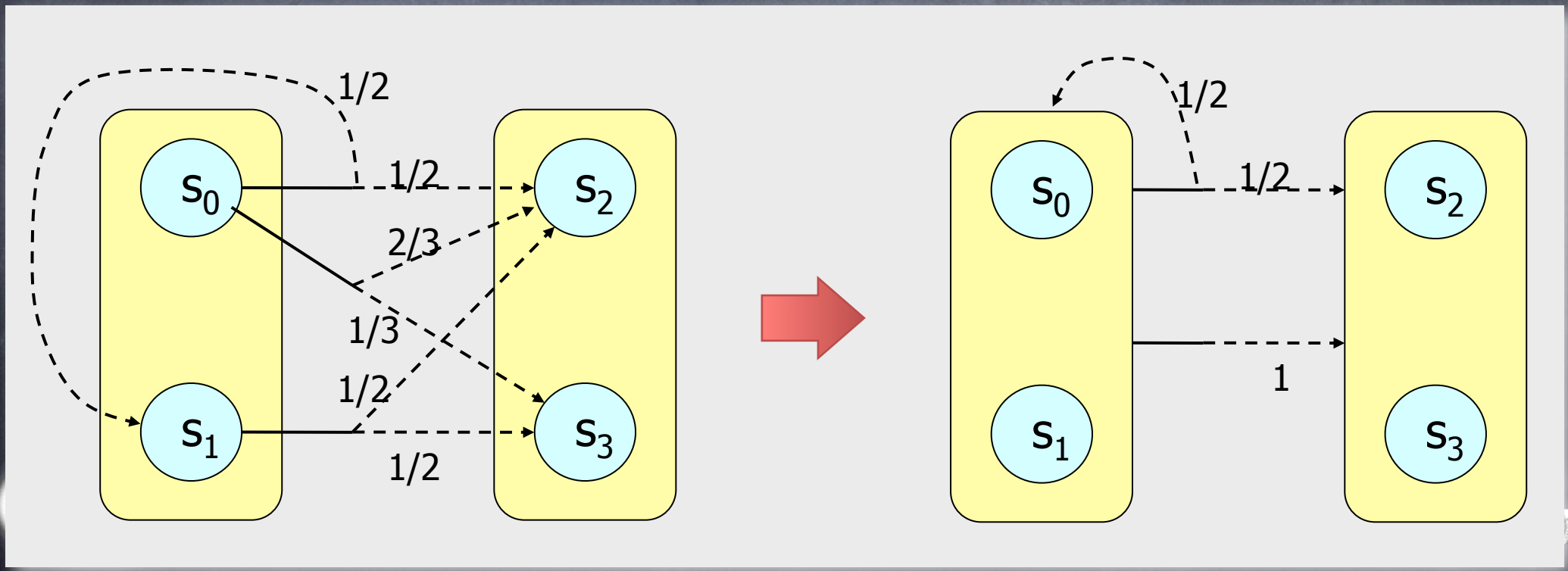
¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]



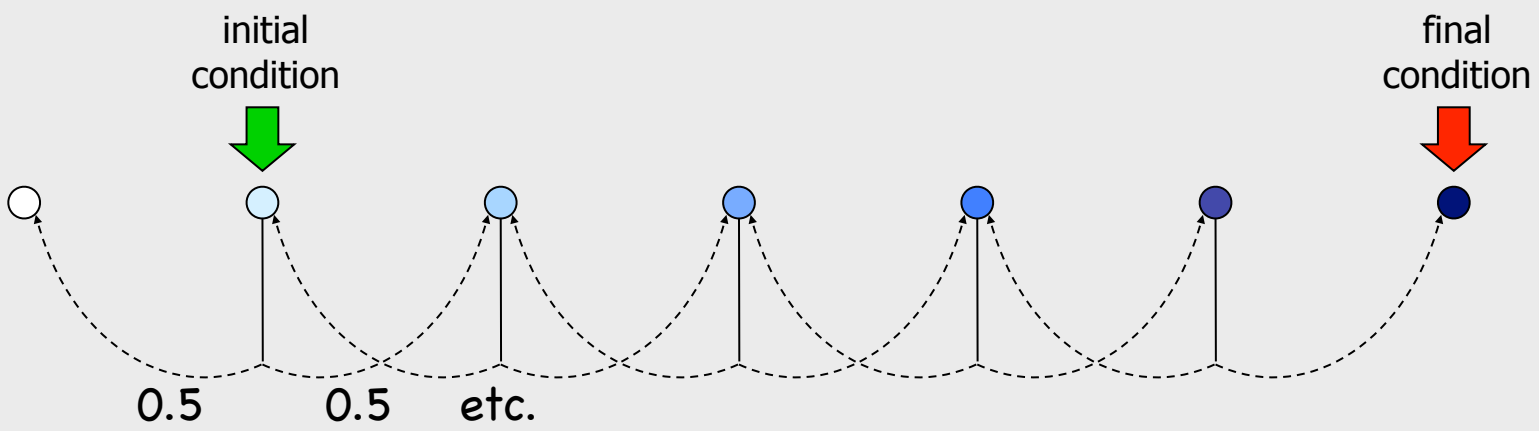
¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]



¿Qué estamos haciendo?

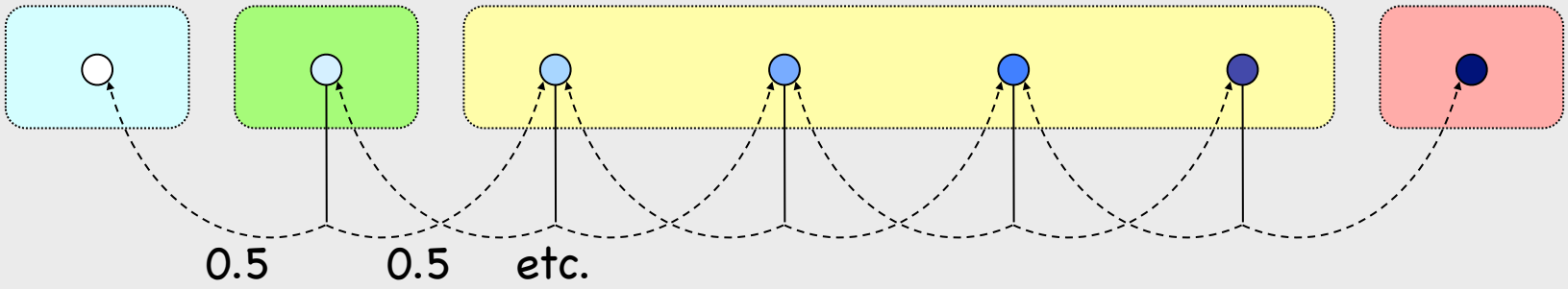
- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]



Supongamos que queremos verificar si P(,) ≤ 0.2

¿Qué estamos haciendo?

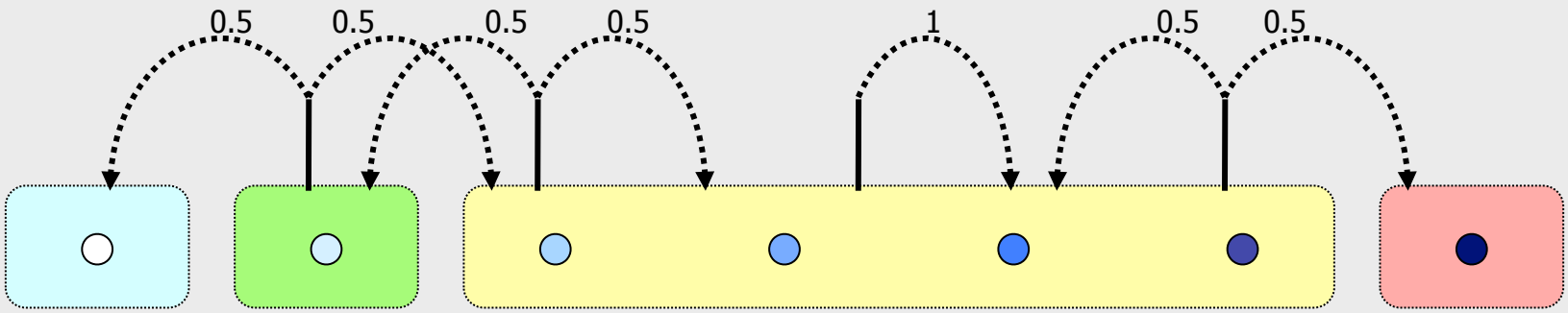
- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]



Supongamos que queremos verificar si P(,) ≤ 0.2

¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]

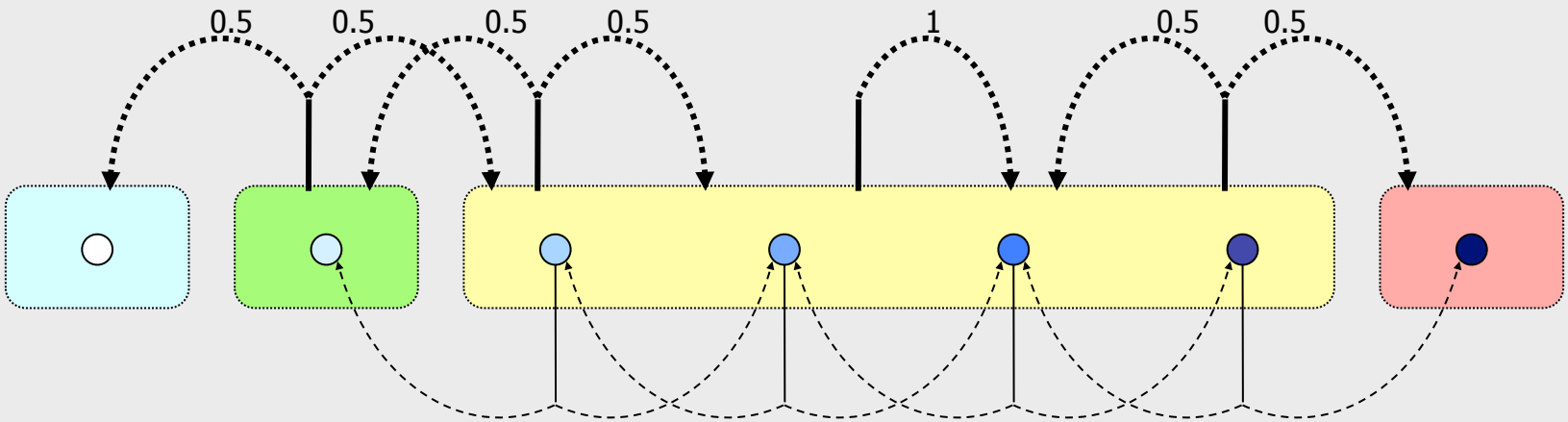


$$0 = P_0^{min} \leq P(\bullet, \bullet) \leq P_0^{max} = 0.5$$

Supongamos que queremos verificar si $P(\bullet, \bullet) \leq 0.2$

¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]

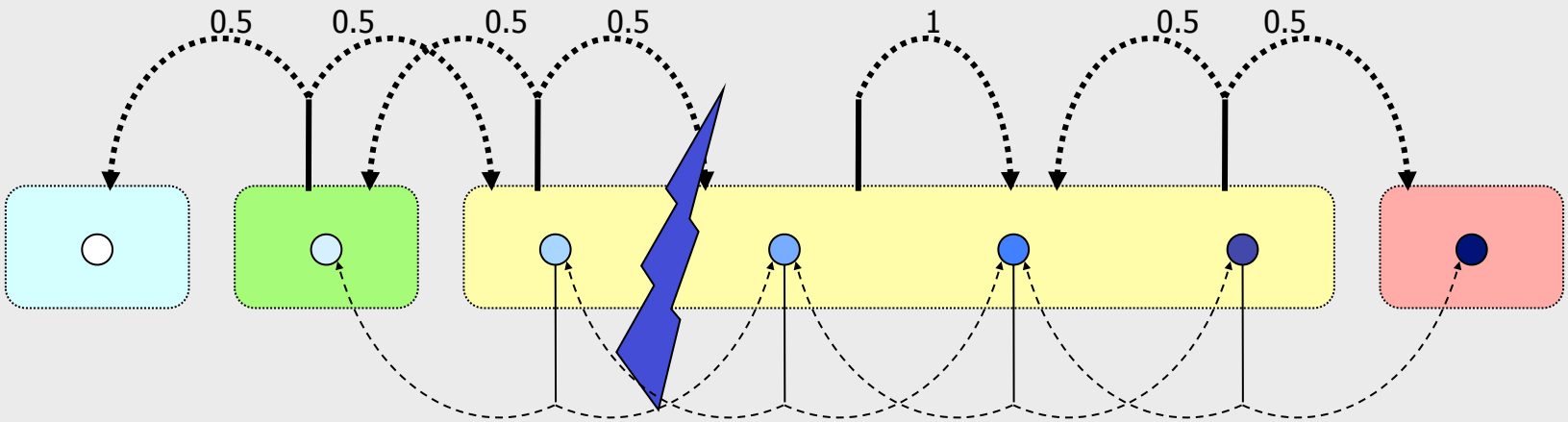


$0 = P_0^{min} \leq P(\bullet, \bullet) \leq P_0^{max} = 0.5$

Supongamos que queremos verificar si $P(\bullet, \bullet) \leq 0.2$

¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]

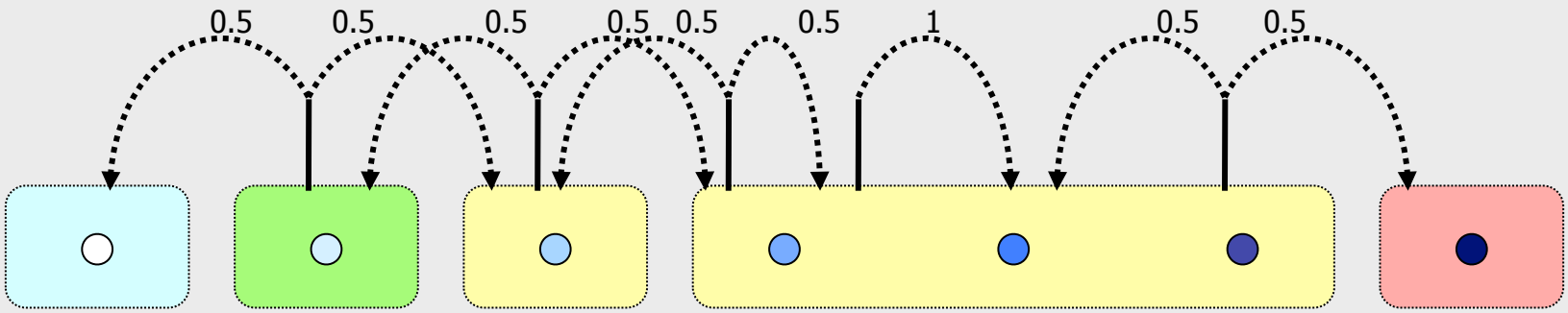


$0 = P_0^{min} \leq P(\bullet, \bullet) \leq P_0^{max} = 0.5$

Supongamos que queremos verificar si $P(\bullet, \bullet) \leq 0.2$

¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]

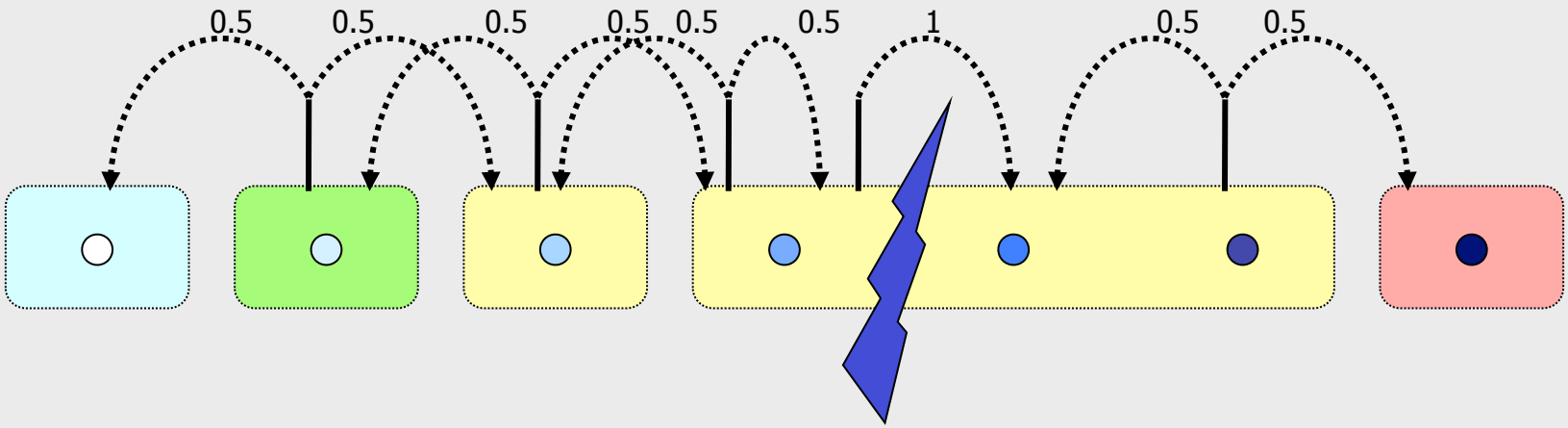


$$0 = P_1^{min} \leq P(\bullet, \bullet) \leq P_1^{max} = 0.25$$

Supongamos que queremos verificar si $P(\bullet, \bullet) \leq 0.2$

¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]

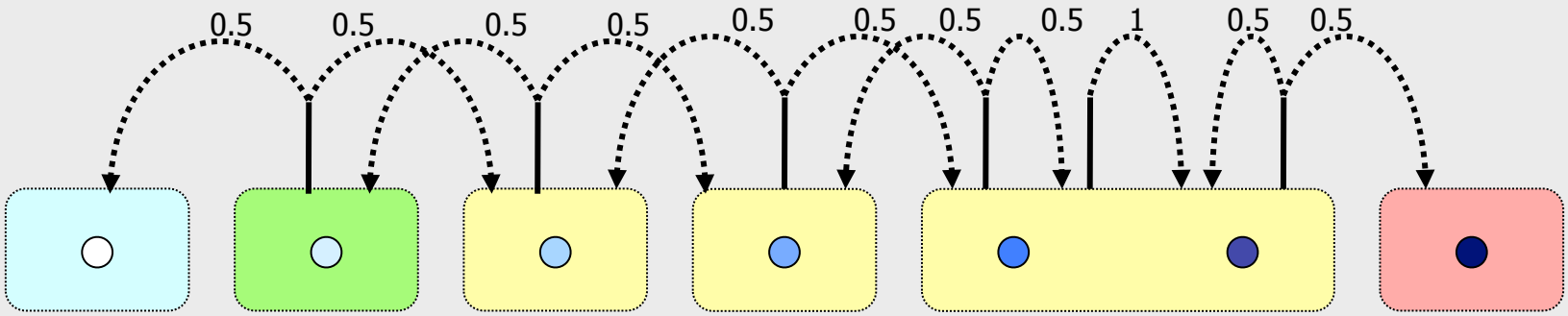


$$0 = P_1^{min} \leq P(\circ, \bullet) \leq P_1^{max} = 0.25$$

Supongamos que queremos verificar si $P(\circ, \bullet) \leq 0.2$

¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Sobre/sub aproximación mediante abstracción y refinamientos [D'Argenio, Jeannet, Larsen & Jensen, 2001 & 2002]

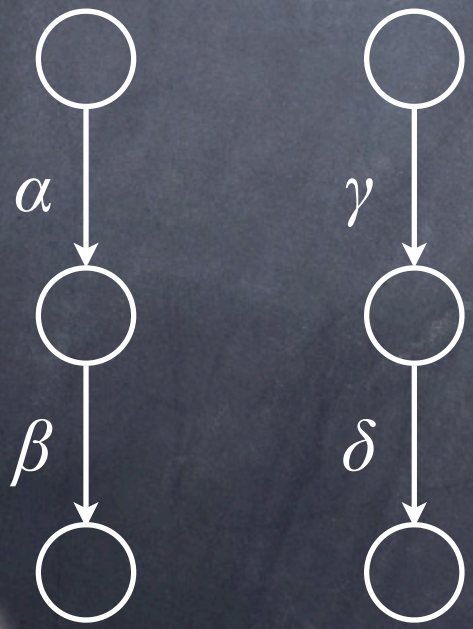


$$0 = P_2^{min} \leq P(\circ, \bullet) \leq P_2^{max} = 0.2$$

Supongamos que queremos verificar si $P(\circ, \bullet) \leq 0.2$

¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Técnicas de reducción de orden parcial [D'Argenio & Niebert, 2004] [Baier, D'Argenio & Größer, 2005-2006] [Giro, D'Argenio & Ferrer Fioriti 2009]



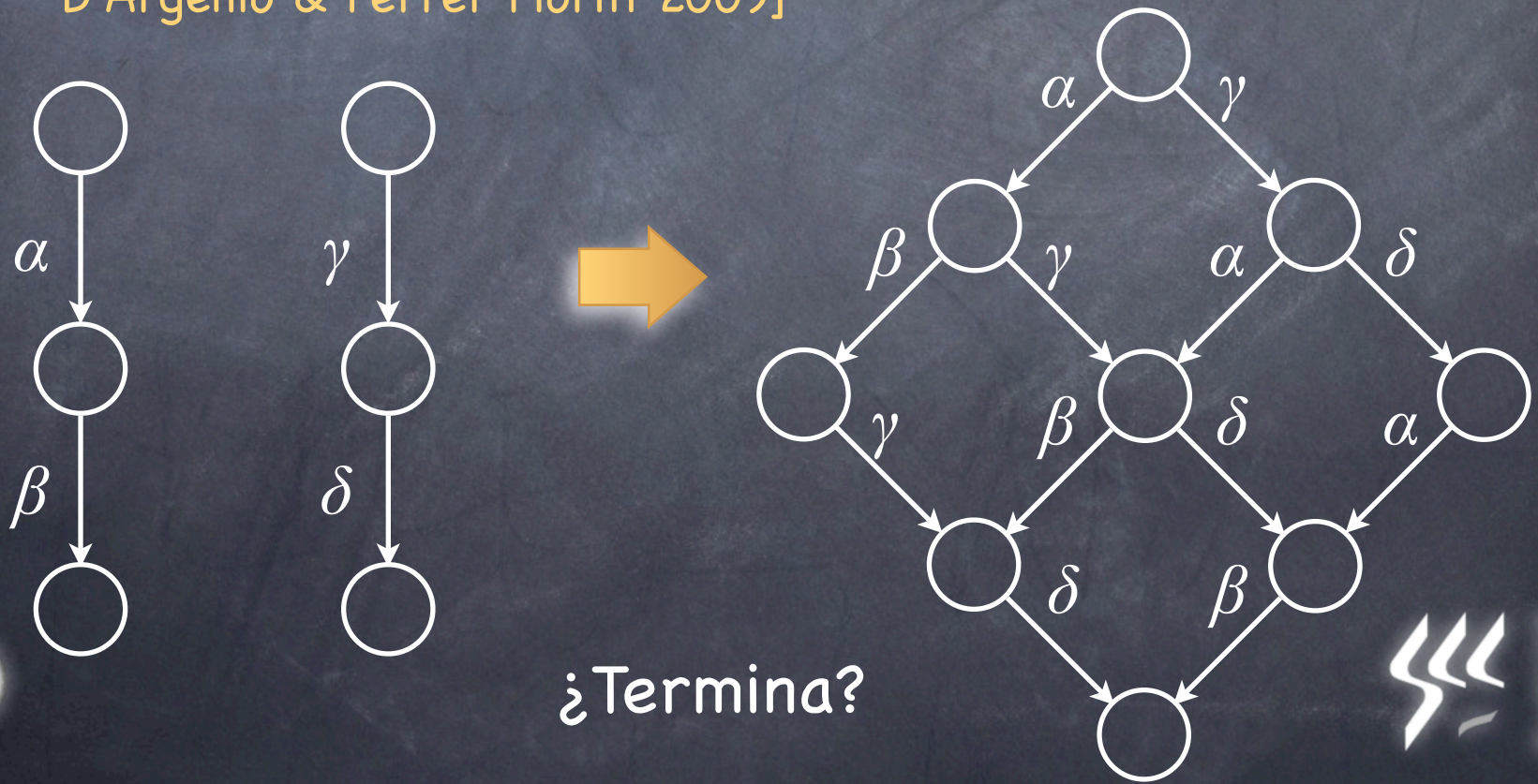
¿Termina?

CONICET

FaMAF

¿Qué estamos haciendo?

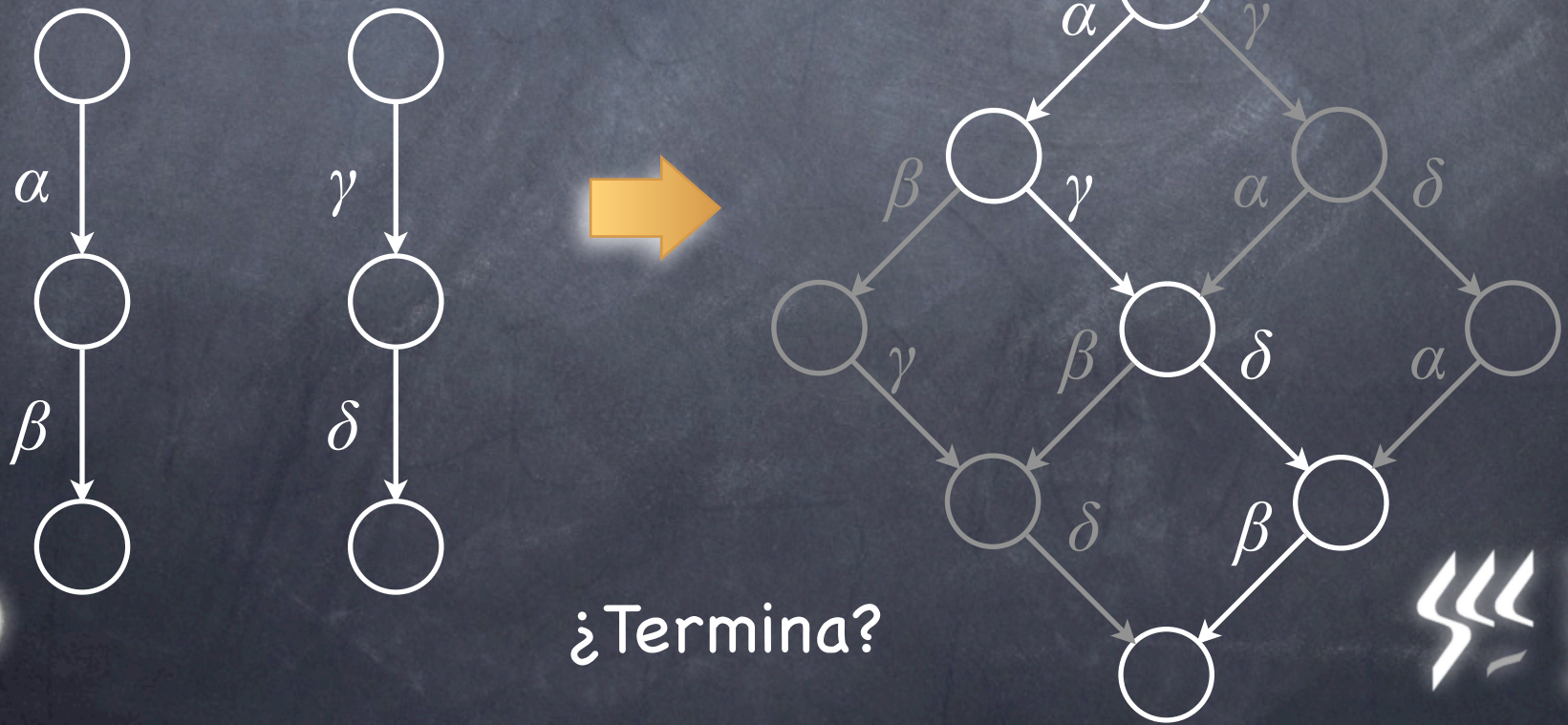
- El problema de la explosión de estados:
  - Soluciones:
  - Técnicas de reducción de orden parcial [D'Argenio & Niebert, 2004] [Baier, D'Argenio & Größer, 2005-2006] [Giro, D'Argenio & Ferrer Fioriti 2009]



¿Termina?

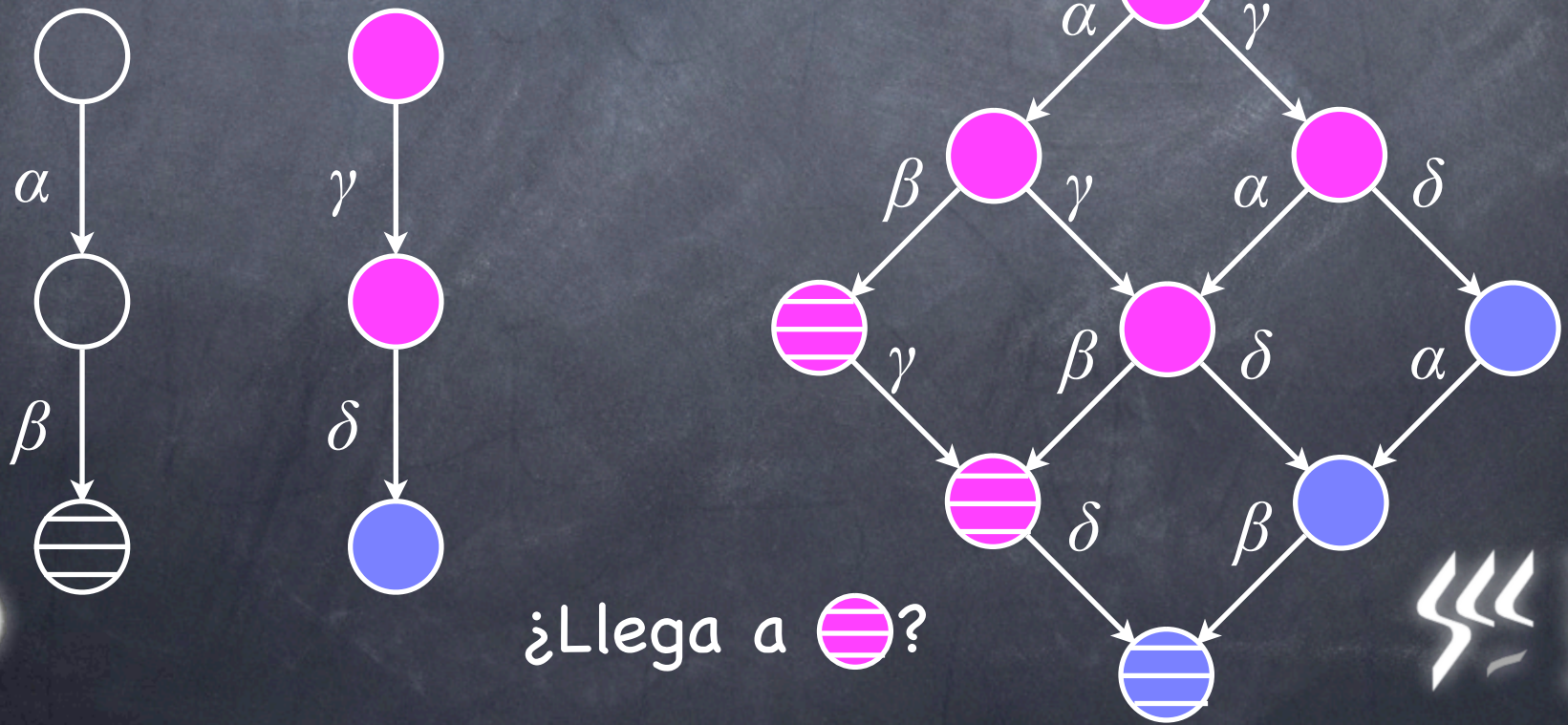
¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Técnicas de reducción de orden parcial [D'Argenio & Niebert, 2004] [Baier, D'Argenio & Größer, 2005-2006] [Giro, D'Argenio & Ferrer Fioriti 2009]



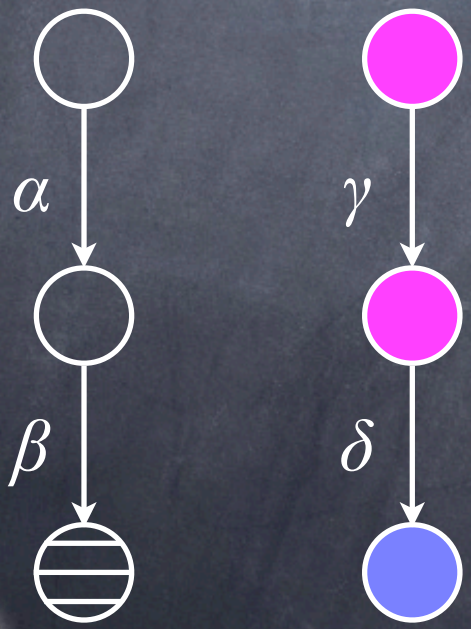
¿Qué estamos haciendo?

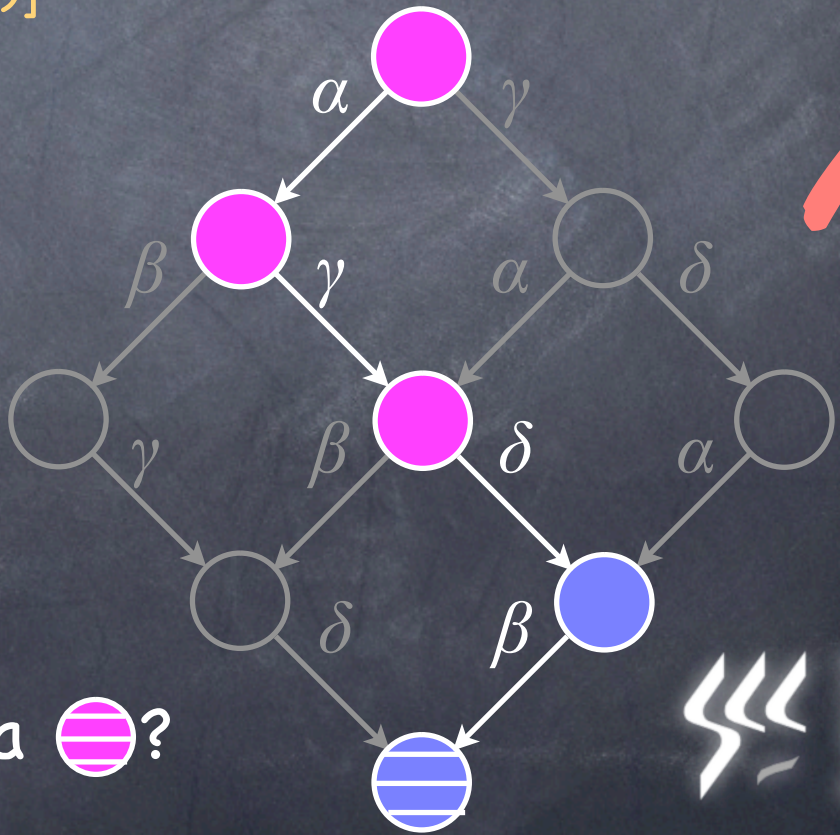
- El problema de la explosión de estados:
  - Soluciones:
  - Técnicas de reducción de orden parcial [D'Argenio & Niebert, 2004] [Baier, D'Argenio & Größer, 2005-2006] [Giro, D'Argenio & Ferrer Fioriti 2009]



¿Qué estamos haciendo?

- El problema de la explosión de estados:
  - Soluciones:
  - Técnicas de reducción de orden parcial [D'Argenio & Niebert, 2004] [Baier, D'Argenio & Größer, 2005-2006] [Giro, D'Argenio & Ferrer Fioriti 2009]

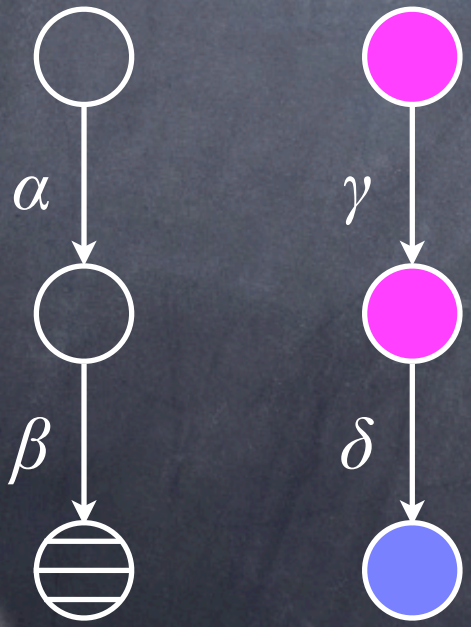


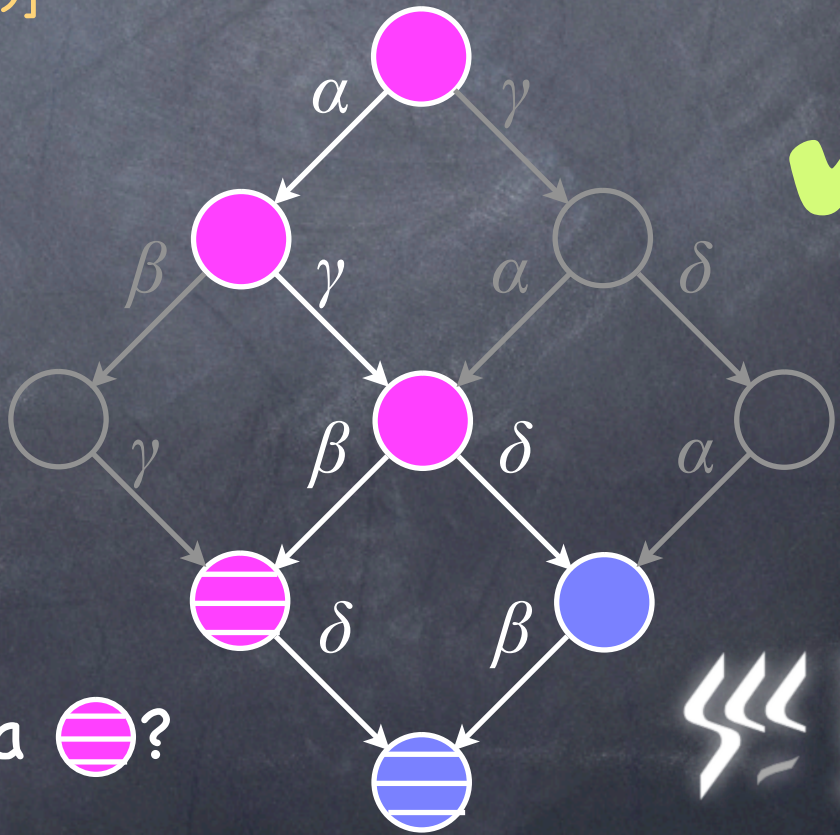


¿Llega a ▤?

¿Qué estamos haciendo?

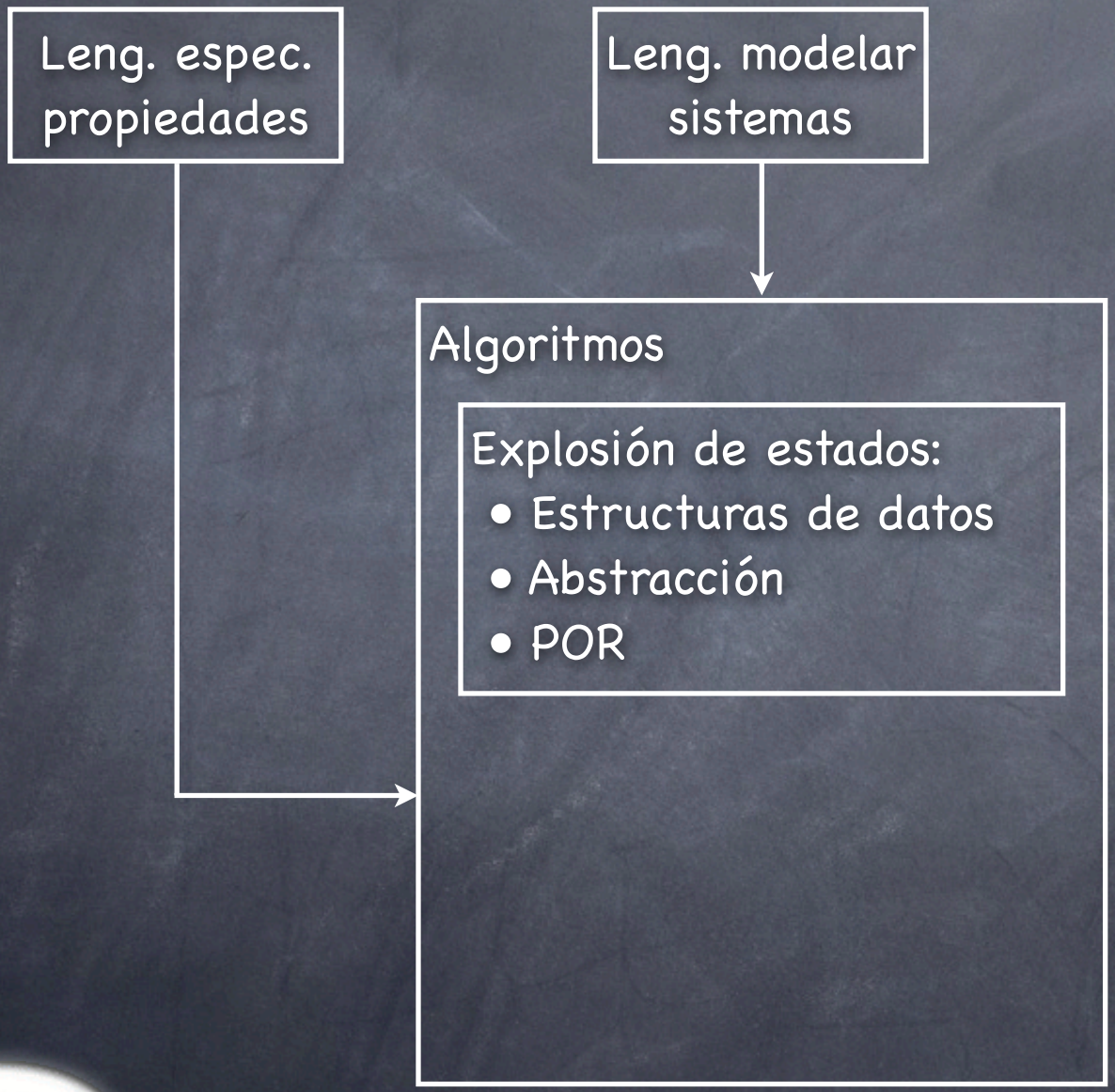
- El problema de la explosión de estados:
  - Soluciones:
  - Técnicas de reducción de orden parcial [D'Argenio & Niebert, 2004] [Baier, D'Argenio & Größer, 2005-2006] [Giro, D'Argenio & Ferrer Fioriti 2009]





¿Llega a ☰?

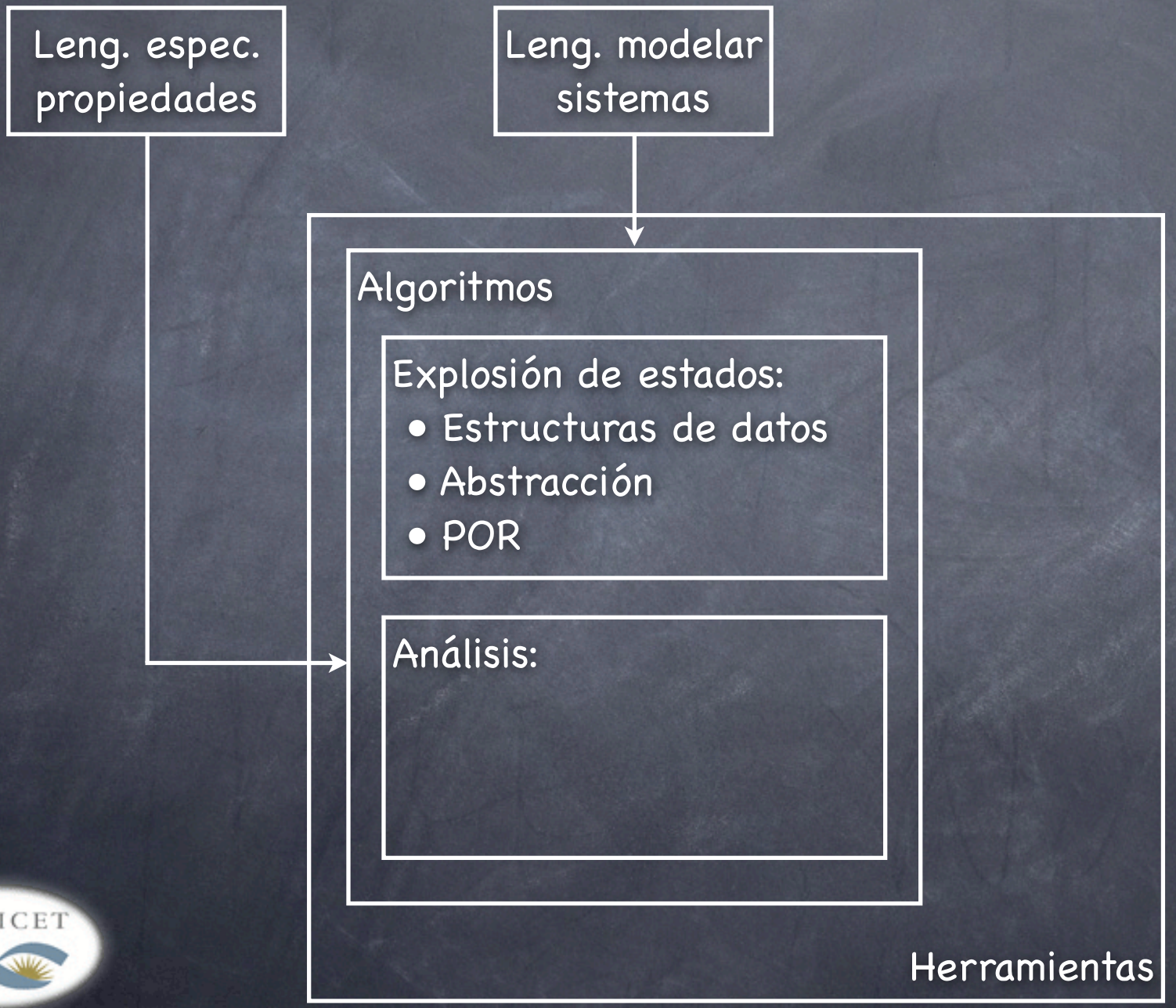
¿Qué estamos haciendo?



CONICET

FaMAF

¿Qué estamos haciendo?



¿Qué estamos haciendo?

- Desarrollo de model checker cuantitativos
  - RAPTURE: un MCC para análisis de alcanzabilidad [D'Argenio, Jeannet & Larsen, 2002]
  - RAPTURE front end para MCC de propiedades en LTL [Combina & Lee, 2006]
  - Extensión del motor de PRISM para MCC de propiedades en LTL [Bederián, 2008, Incluido en la distro de PRISM]
  - POR implementado en PRISM [Giro, D'Argenio & Ferrer Fioriti 2009] [Ferrer Fioriti 2010]
  - Paralelización de los algoritmos de cálculo numérico en PRISM [Dal Lago, 2011?]

¿Qué estamos

RAPTURE es obsoleta.
=> estamos llevando técnicas de RAPTURE a PRISM [Zandarin 2010?]

- Desarrollo de model check[illegible] cuantitativos
  - RAPTURE: un MCC para análisis de alcanzabilidad [D'Argenio, Jeannet & Larsen, 2002]
  - RAPTURE front end para MCC de propiedades en LTL [Combina & Lee, 2006]
  - Extensión del motor de PRISM para MCC de propiedades en LTL [Bederián, 2008, Incluido en la distro de PRISM]
  - POR implementado en PRISM [Giro, D'Argenio & Ferrer Fioriti 2009] [Ferrer Fioriti 2010]
  - Paralelización de los algoritmos de cálculo numérico en PRISM [Dal Lago, 2011?]

CONICET

FaMAF

¿Qué estamos haciendo?

- POR implementado en PRISM [Giro, D'Argenio & Ferrer Fioriti 2009] [Ferrer Fioriti 2010]

Model	Full	**A1-A4** reduct.		**A1-A3** reduct.		
n / N / 2^K	size	size	% full	size	% full	% **A4**
4 / 3 / 4	532326	191987	36.07	126629	23.79	65.96
5 / 3 / 4	13866186	2752750	19.85	1690227	12.19	61.40
6 / 3 / 4	357387872	36974560	10.35	21771724	6.09	58.88
4 / 3 / 8	3020342	913379	30.24	604457	20.01	66.18
5 / 3 / 8	115442928	18569442	16.09	11585347	10.04	62.39
6 / 3 / 8	4318481408	353075296	8.18	212917856	4.93	60.30

Binary exponential backoff (size comparison)

¿Qué estamos haciendo?

- POR implementado en PRISM [Giro, D'Argenio & Ferrer Fioriti 2009] [Ferrer Fioriti 2010]

Model	Full	**A1-A4** reduct.		**A1-A3** reduct.		
n / N / 2^K	size	size	% full	size	% full	% **A4**
4 / 3 / 4	532326	191987	36.07	126629	23.79	65.96
5 / 3 / 4	13866186	2752750	19.85	1690227	12.19	61.40
6 / 3 / 4	357387872	36974560	10.35	21771724	6.09	58.88
4 / 3 / 8	3020342	913379	30.24	604457	20.01	66.18
5 / 3 / 8	115442928	18569442	16.09	11585347	10.04	62.39
6 / 3 / 8	$4.3 * 10^9$	$3.5 * 10^8$	8.18	$2.1 * 10^8$	4.93	60.30

Binary exponential backoff (size comparison)

¿Qué estamos haciendo?

- POR implementado en PRISM [Giro, D'Argenio & Ferrer Fioriti 2009] [Ferrer Fioriti 2010]

Model	Full			**A1-A3** reduct.		
n / N / 2^K	size				% full	% **A4**
4 / 3 / 4	532326			629	23.79	65.96
5 / 3 / 4	13866186			0227	12.19	61.40
6 / 3 / 4	357387872			24	6.09	58.88
4 / 3 / 8	3020342	913379	30.24	604457	20.04	66.18
5 / 3 / 8	115442928	18569442	16.09	11585347	4.93	2.39
6 / 3 / 8	4.3 * 10^9	3.5 * 10^8	8.18	2.1 * 10		.30

El espacio de estado es 20 veces menor que el original.

Binary exponential backoff (size comparison)

¿Qué estamos haciendo?

- POR implementado en PRISM [Giro, D'Argenio & Ferrer Fioriti 2009] [Ferrer Fioriti 2010]

Model	Full		**A1-A4** reduct.		**A1-A3** reduct.	
n / N / 2^K	constr.	total	constr.	total	constr.	total
4 / 3 / 4	0m01.39	1m04.27	0m18.96	1m22.98	0m18.02	1m13.36
5 / 3 / 4	0m03.49	11m32.99	1m16.82	8m15.60	1m14.53	6m50.12
6 / 3 / 4	0m07.55	5h03m39.81	4m00.95	1h13m11.39	5m15.06	53m35.43
4 / 3 / 8	0m02.05	3m33.62	0m23.85	3m01.88	0m22.78	2m28.50
5 / 3 / 8	0m05.41	1h21m13.54	1m36.41	30m42.82	1m41.18	22m09.23
6 / 3 / 8	0m13.30	—	5m14.95	12h31m57.39	6m44.82	7h45m46.75

Binary exponential backoff (time comparison)

¿Qué estamos haciendo?

- POR implementado en PRISM [Giro, D'Argenio & Ferrer Fioriti 2009] [Ferrer Fioriti 2010]

Model	Full		**A1-A4** reduct.		**A1-A3** reduct.	
n / N / 2^K	constr.	total	constr.		constr.	total
4 / 3 / 4	0m01.39	1m04.27			02	1m13.36
5 / 3 / 4	0m03.49	11m32.99			53	6m50.12
6 / 3 / 4	0m07.55	5h03m39.81	4m00.95		15.06	53m35.43
4 / 3 / 8	0m02.05	3m33.62	0m23.85	3m01.88	0m22.[illegible]	2m28.59
5 / 3 / 8	0m05.41	1h21m13.54	1m36.41	30m42.82	1m41.18	22m09.23
6 / 3 / 8	0m13.30	—	5m14.95	12h31m57.39	6m44.82	7h45m46.75

4 veces más veloz

Binary exponential backoff (time comparison)

CONICET

FaMAF

¿Qué estamos haciendo?

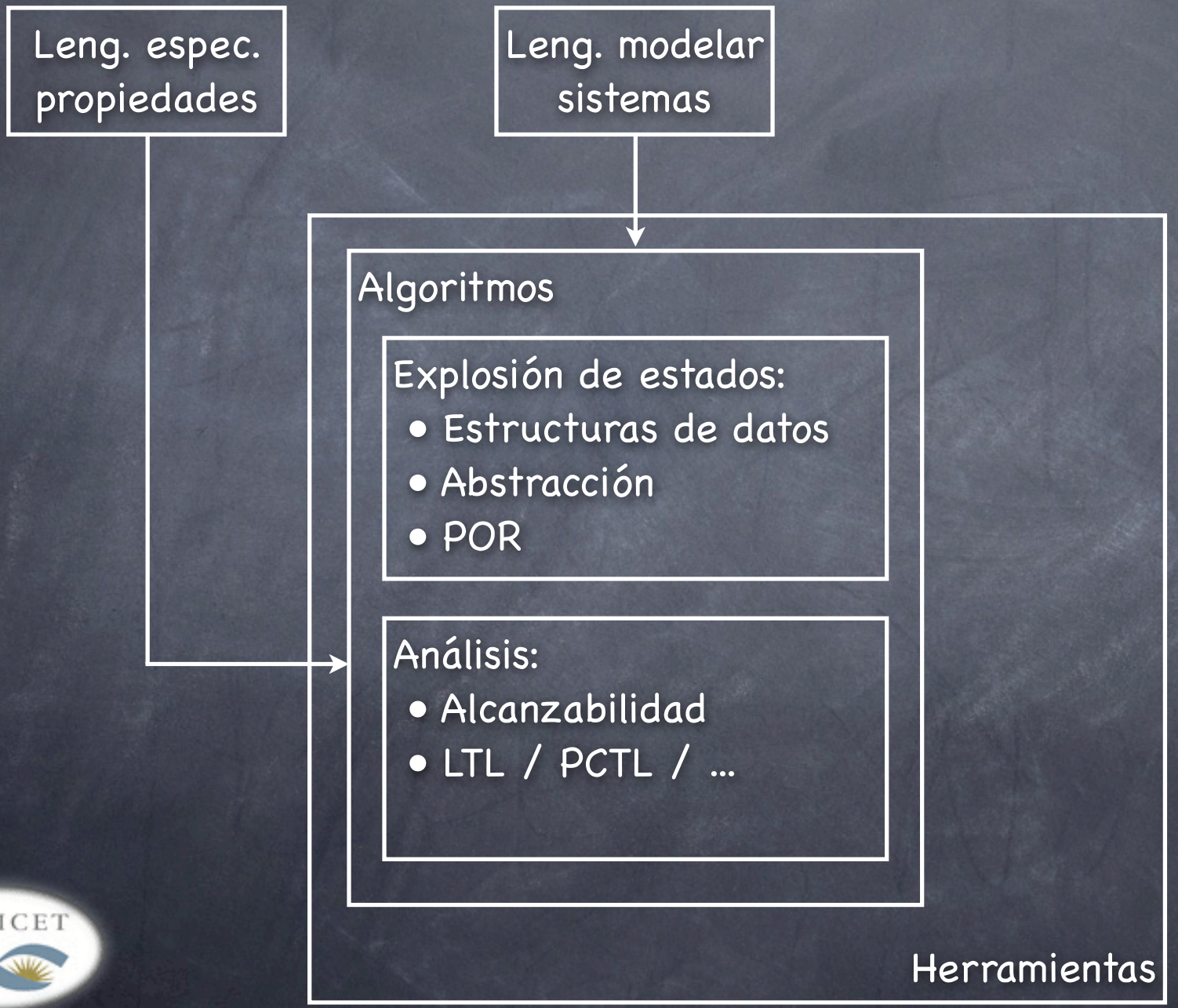
- POR implementado en PRISM [Giro, D'Argenio & Ferrer Fioriti 2009] [Ferrer Fioriti 2010]

Model	Full		**A1-A4** reduct.		**A1-A3** reduct.	
n / N / 2^K	constr.	total	constr.	total	constr.	total
4 / 3 / 4	0m01.39	1m04.27	0m18.02		0m18.02	1m13.36
5 / 3 / 4	0m03.49	11m32.99			1m41.53	6m50.12
6 / 3 / 4	0m07.55	5h03m39.81			3m06.06	53m35.43
4 / 3 / 8	0m02.05	3m33.62	0m23.85		0m22.78	2m28.50
5 / 3 / 8	0m05.41	1h21m13.54	1m36.41	30m42.82	1m41.[illegible]	22m09.23
6 / 3 / 8	0m13.30	☹	5m14.95	12h31m57.39	6m44.82	7h45m46.75

Realizable!!

Binary exponential backoff (time comparison)

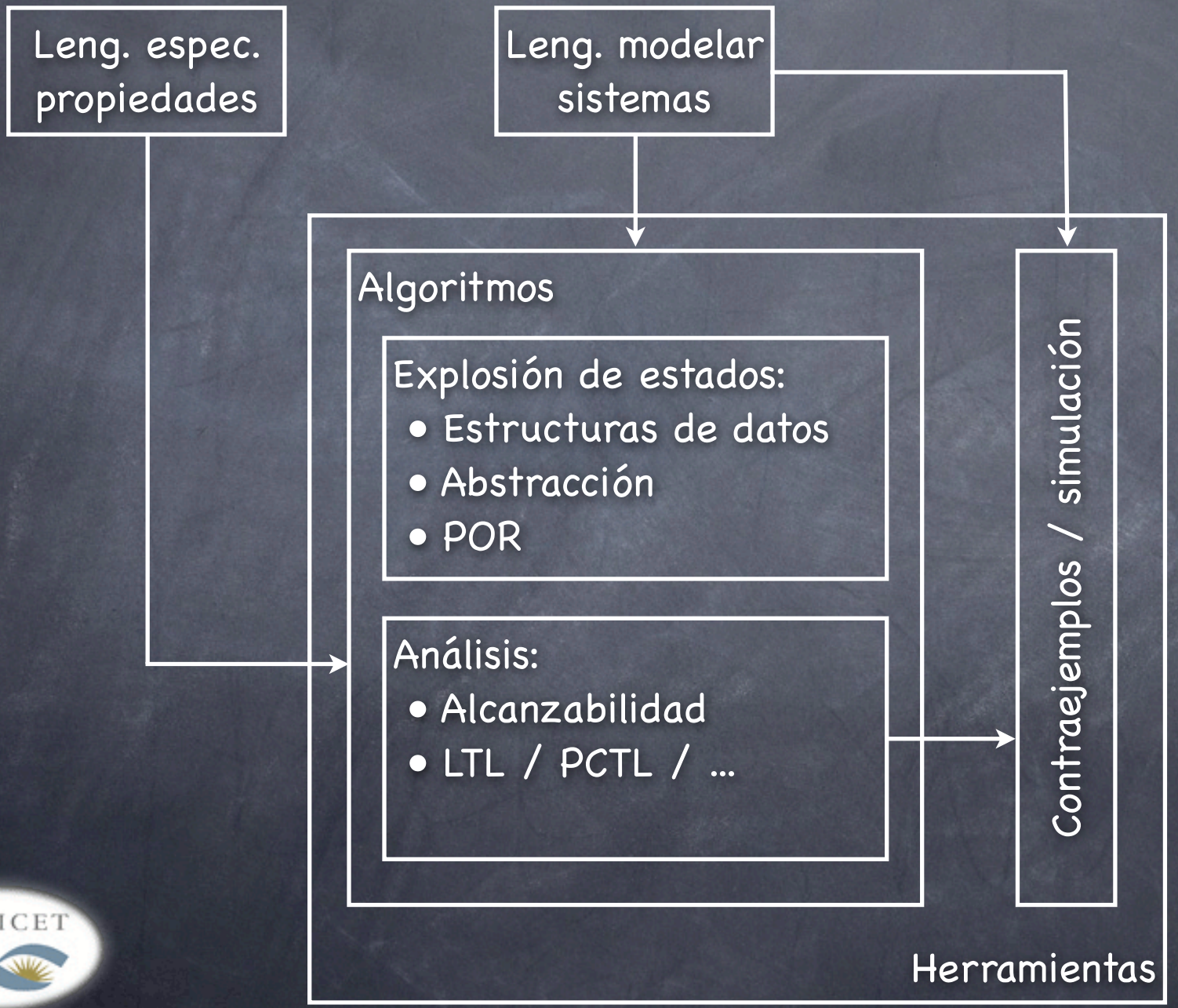
¿Qué estamos haciendo?



CONICET

FaMAF

¿Qué estamos haciendo?



CONICET

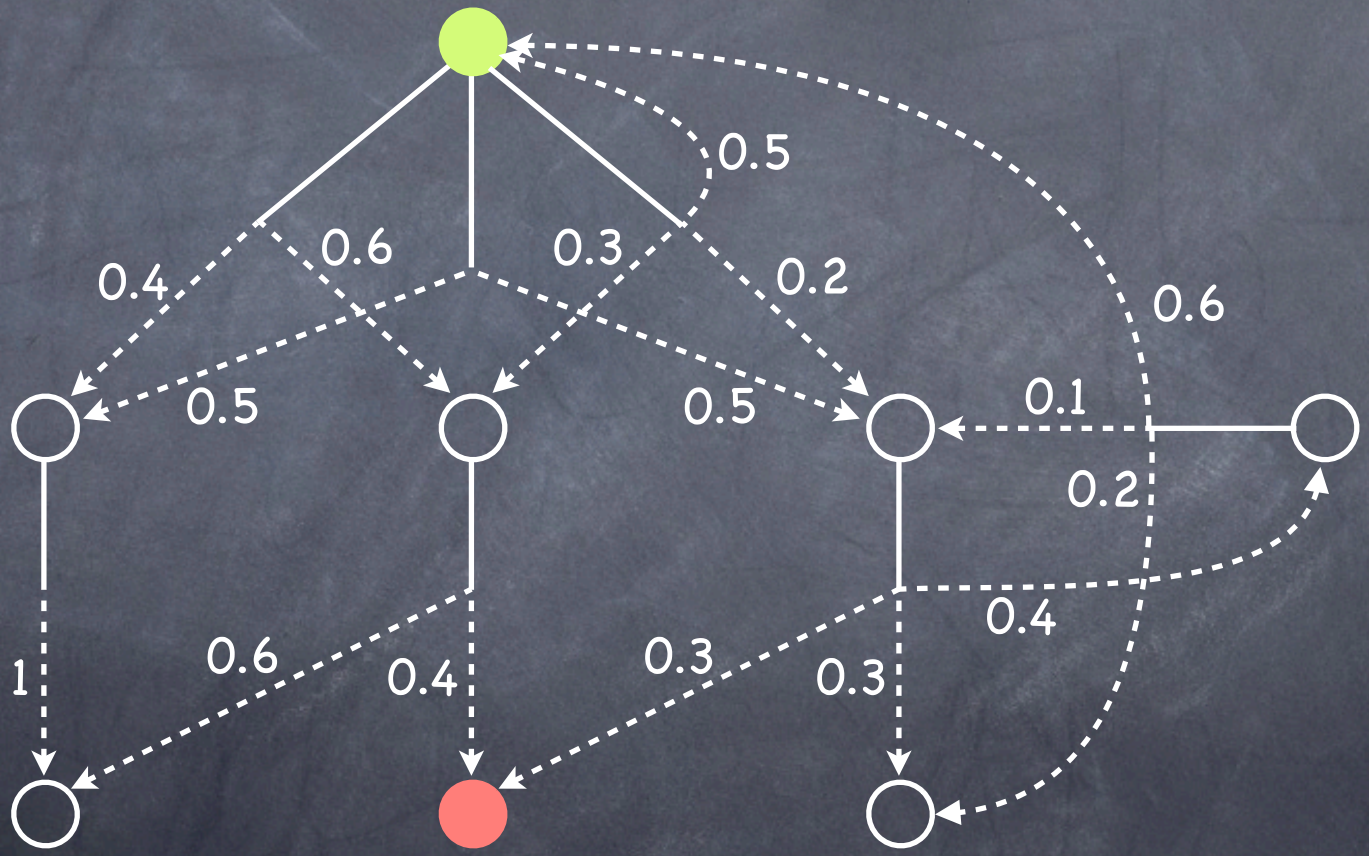
FaMAF

¿Qué estamos haciendo?

- Generación de contraejemplos
  - Lo más importante en MC no es probar verdadera una propiedad.
  - Sino: dar una justificación en el caso de que no se satisfaga:
    - Contraejemplos / trazas de diagnóstico.
  - Pero: ¿qué es un contraejemplo en MCC?
  - Solución: [Andrés, 2006] [Andrés, D'Argenio & van Rossum, 2009] [Marenchino 2011?]

¿Qué estamos haciendo?

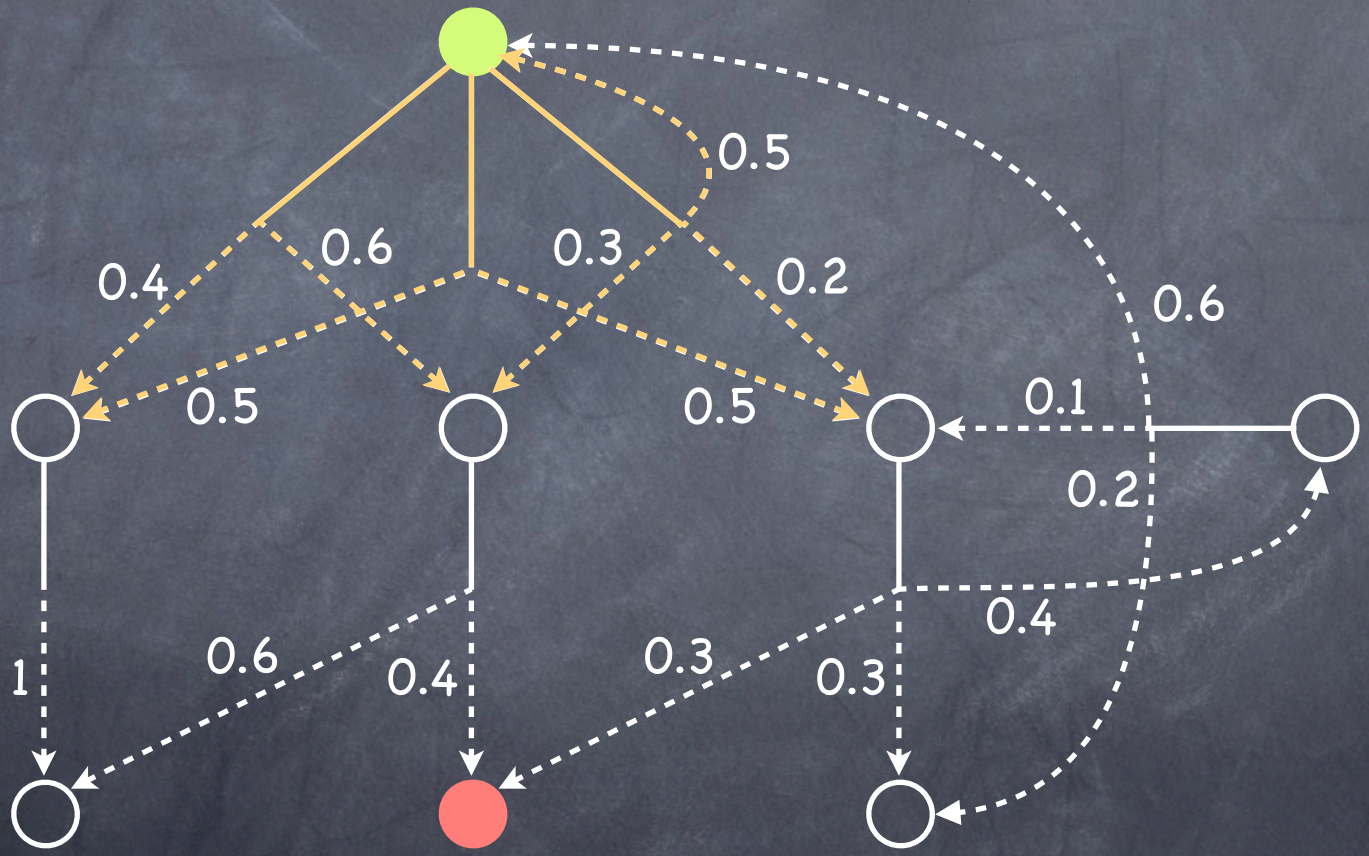
- Generación de contraejemplos



Prob(F●) ≤ 0.4

¿Qué estamos haciendo?

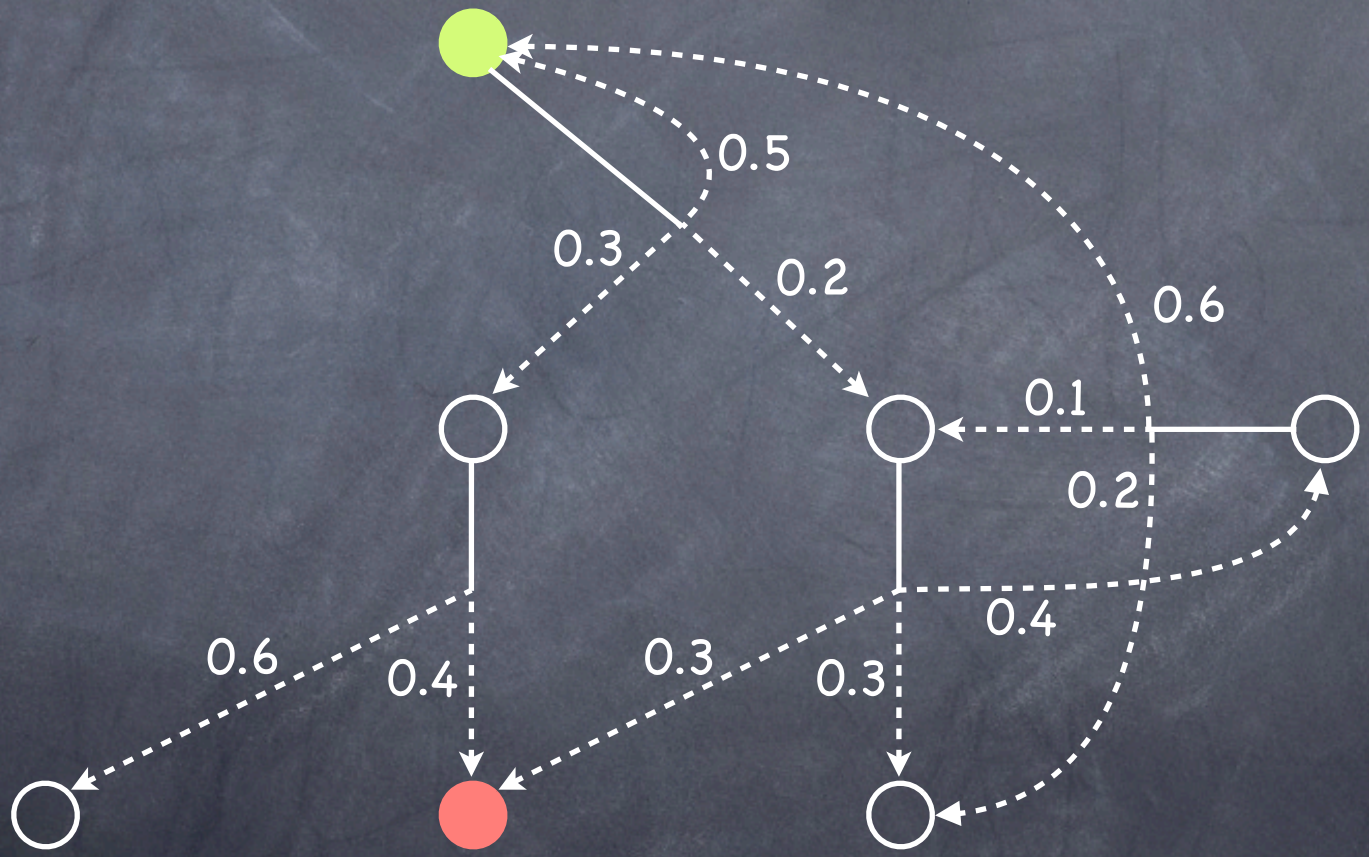
- Generación de contraejemplos



Prob(F●) ≤ 0.4

¿Qué estamos haciendo?

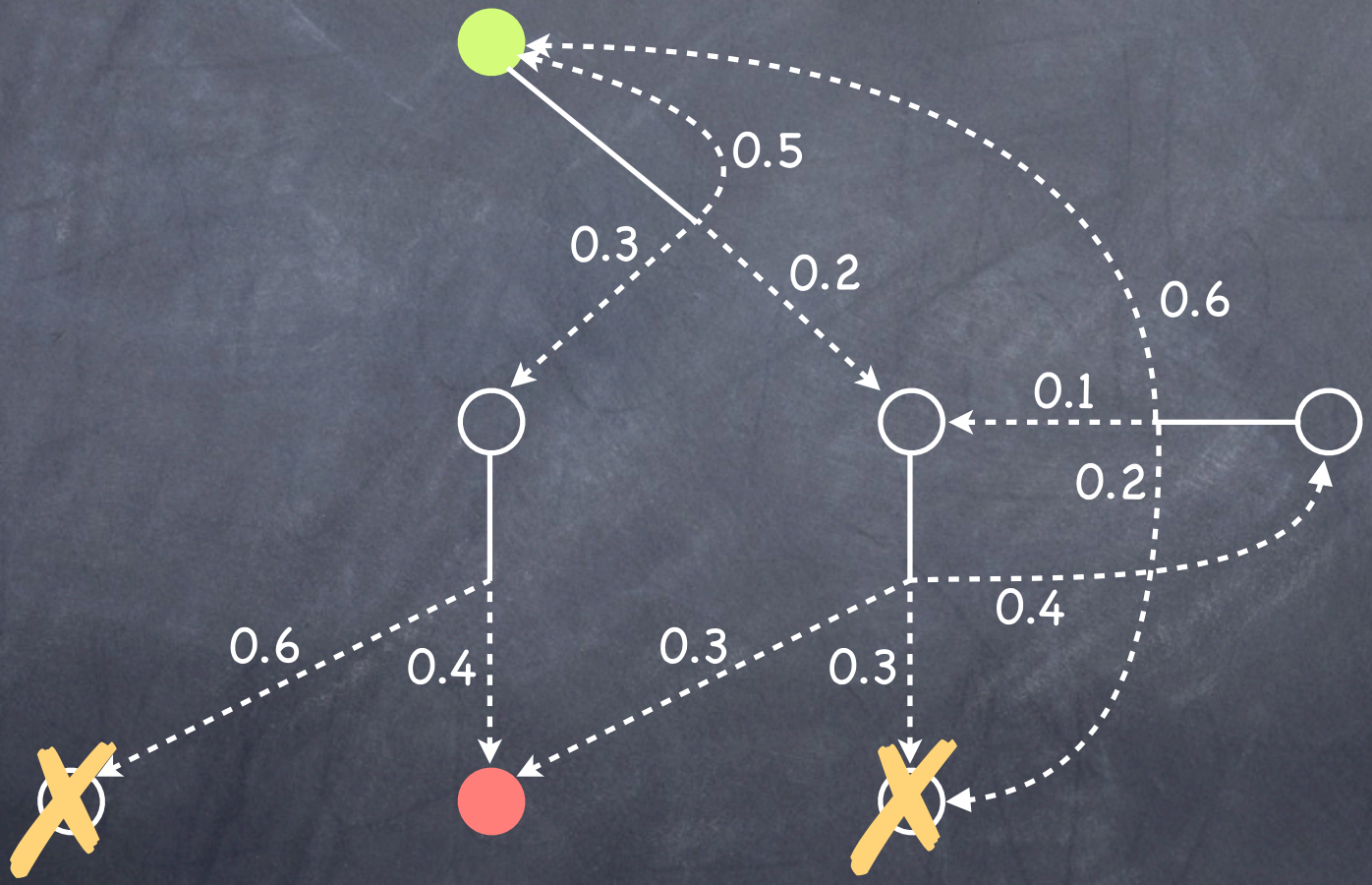
- Generación de contraejemplos



Prob(F●) ≤ 0.4

¿Qué estamos haciendo?

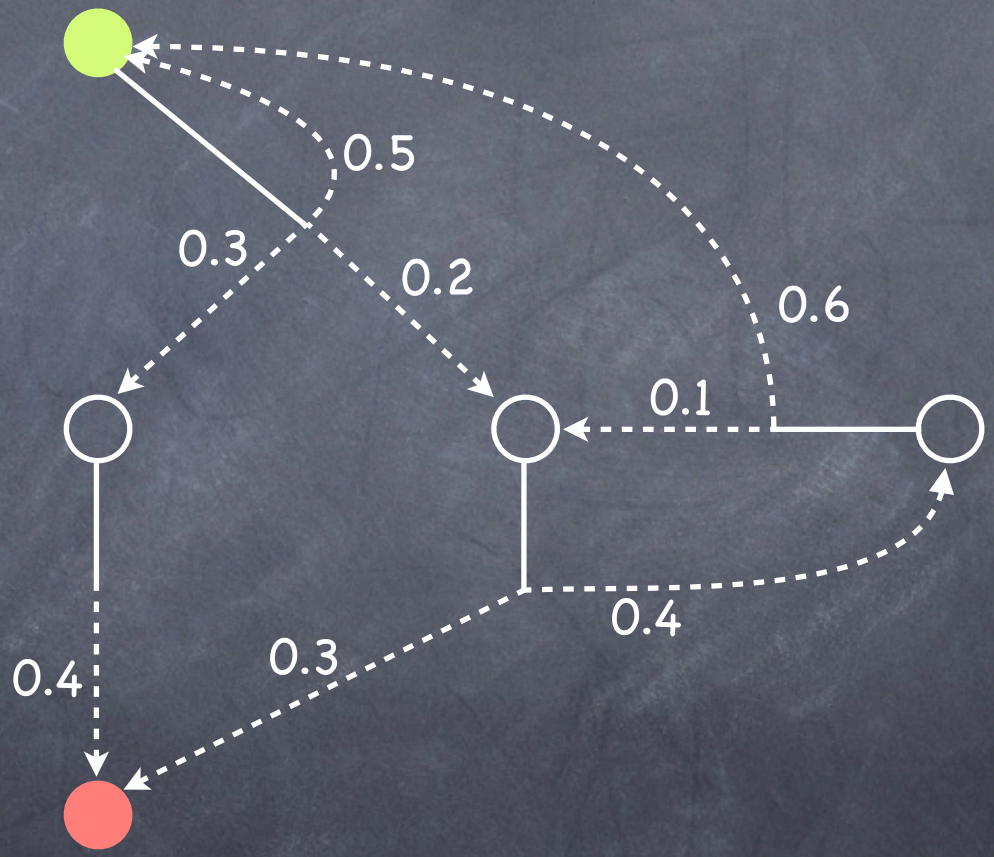
- Generación de contraejemplos



Prob(F●) ≤ 0.4

¿Qué estamos haciendo?

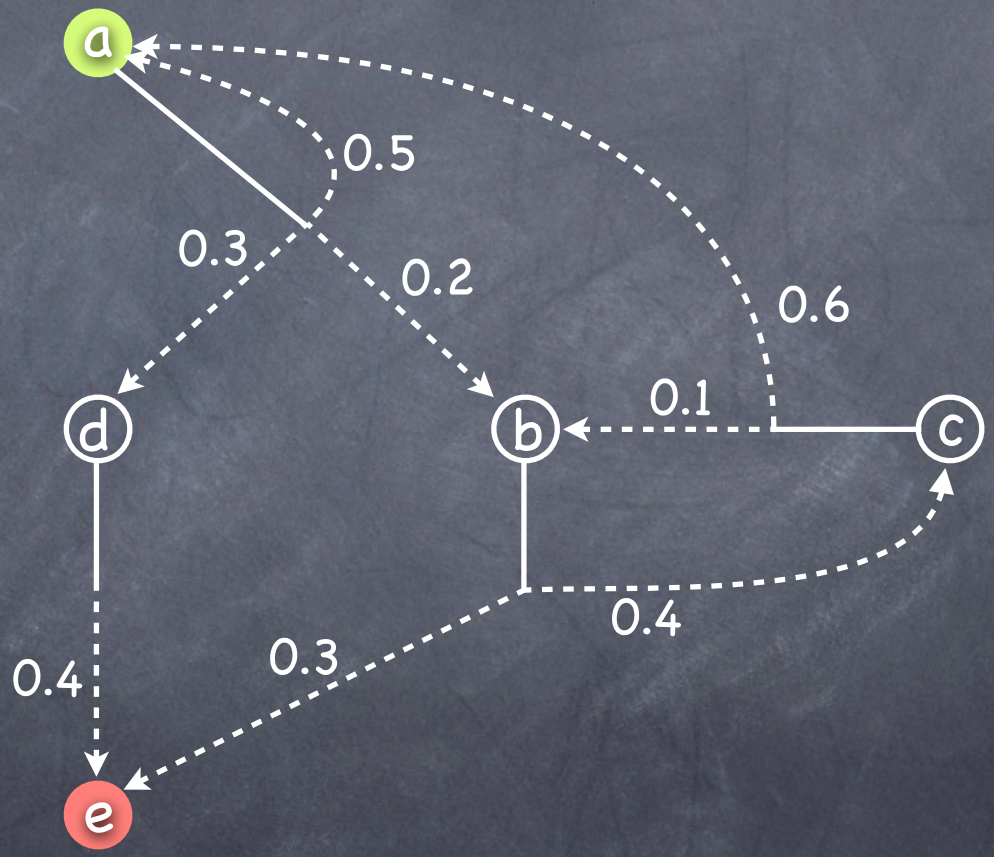
- Generación de contraejemplos



Prob(F●) ≤ 0.4

¿Qué estamos haciendo?

- Generación de contraejemplos

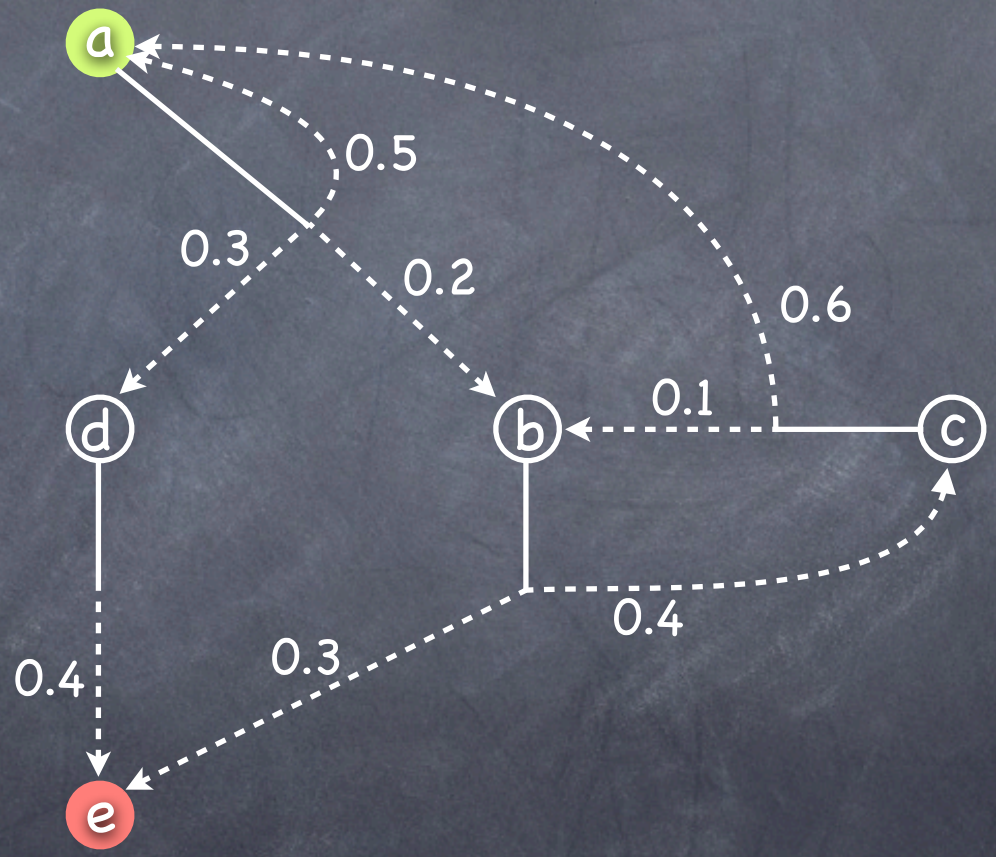


Prob(F●) ≤ 0.4

¿Qué estamos haciendo?

- Generación de contraejemplos

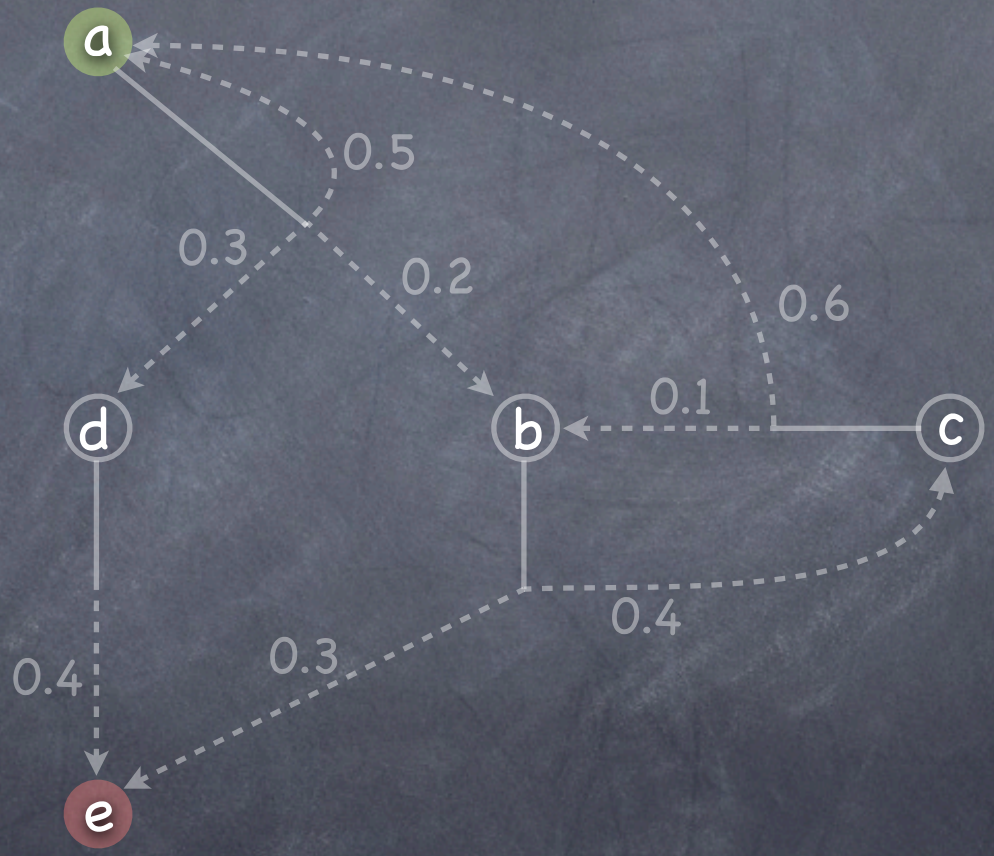
ade	0.12
aade	0.06
aaade	0.03
...	
abe	0.06
abcabe	0.00288
abcaabe	0.00144
aabcaaabcbe	1.44E-05
...	



Prob(F●) ≤ 0.4

¿Qué estamos haciendo?

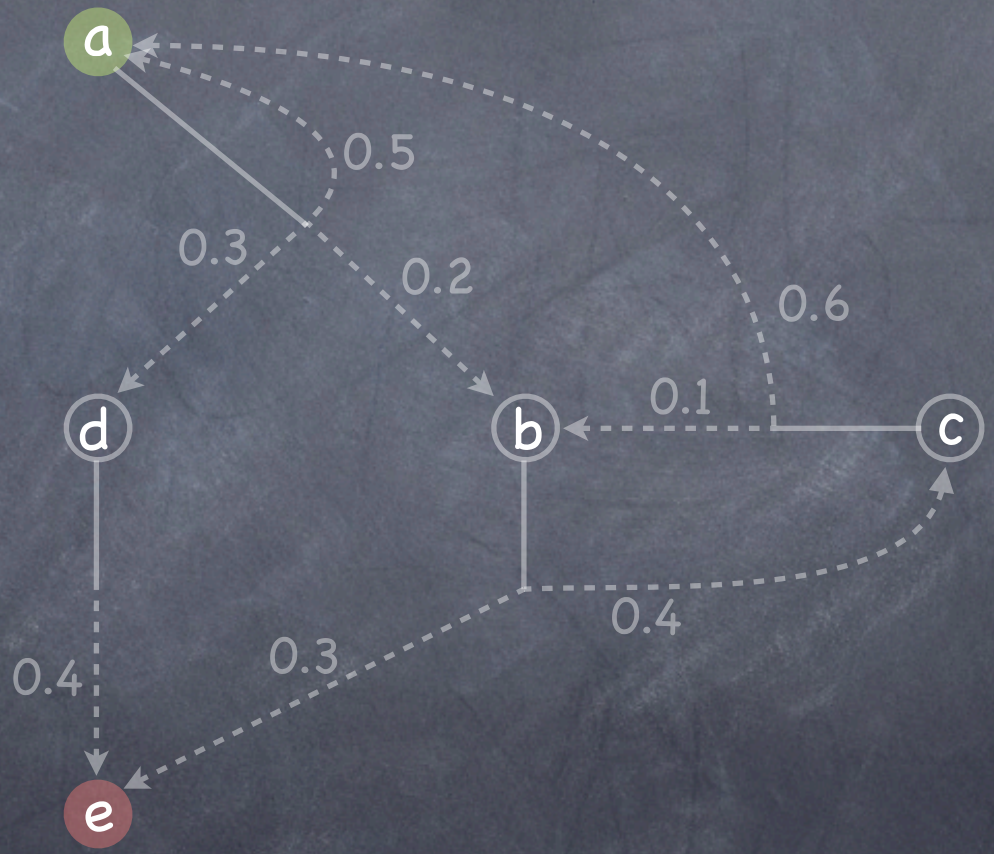
- Generación de contraejemplos



Prob(F●) ≤ 0.4

¿Qué estamos haciendo?

- Generación de contraejemplos

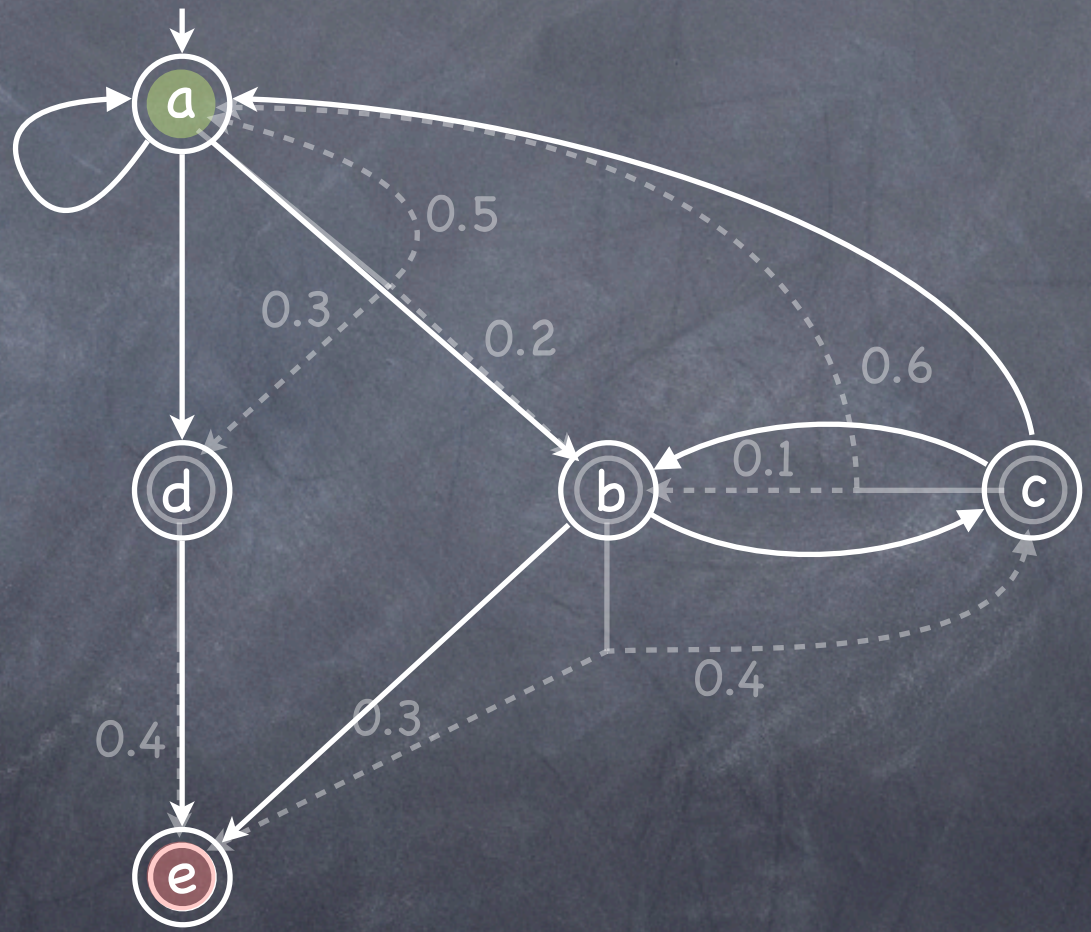


CONICET

FaMAF

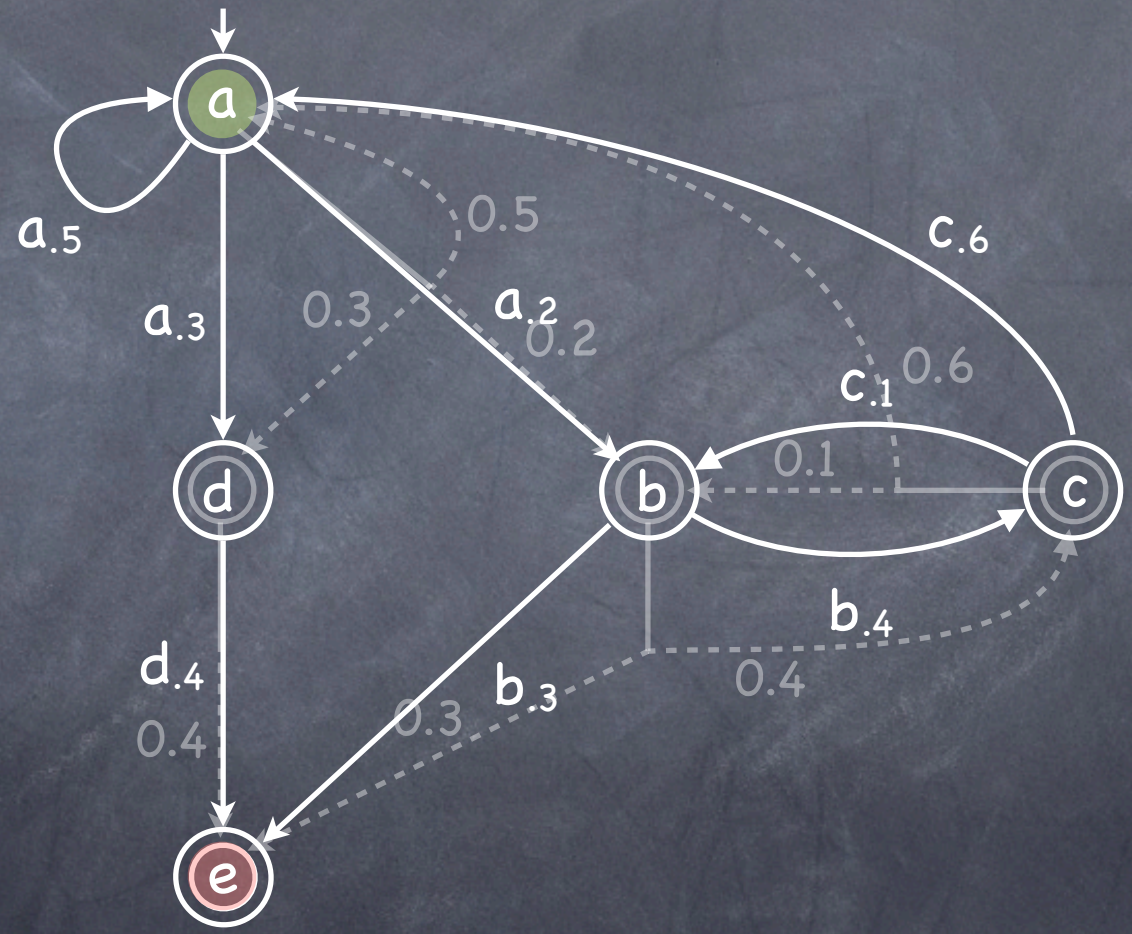
¿Qué estamos haciendo?

- Generación de contraejemplos



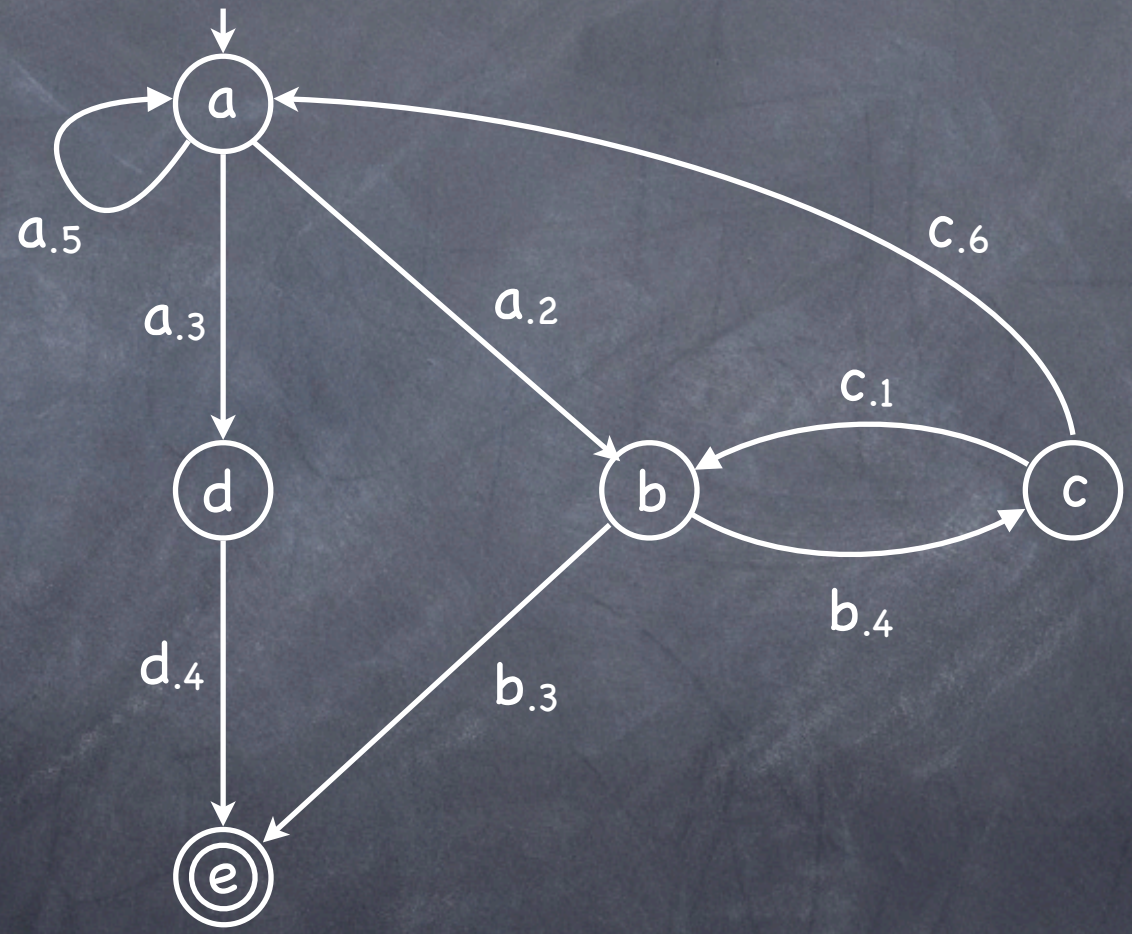
¿Qué estamos haciendo?

- Generación de contraejemplos



¿Qué estamos haciendo?

- Generación de contraejemplos



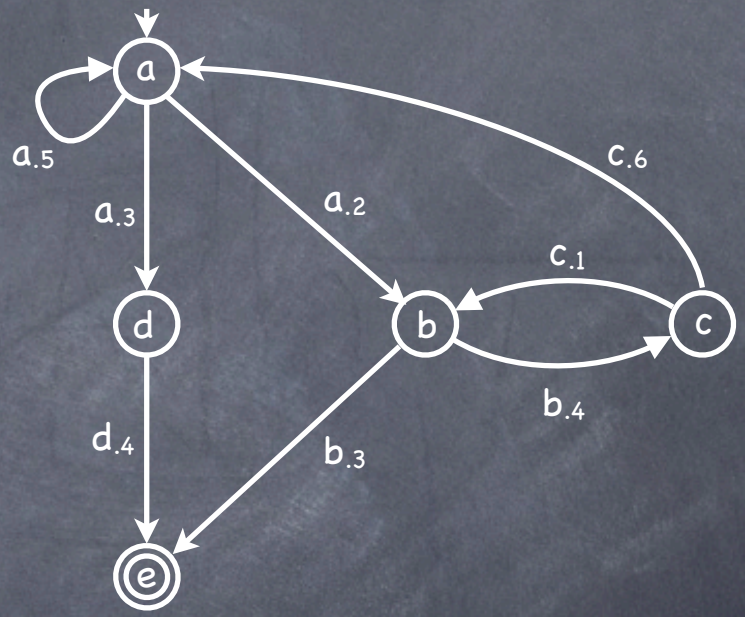
CONICET

FaMAF

¿Qué estamos haciendo?

- Generación de contraejemplos

$(a_{.5}+a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*(a_{.2}(b_{.4}c_{.1})^*b_{.3}+a_{.3}d_{.4})$

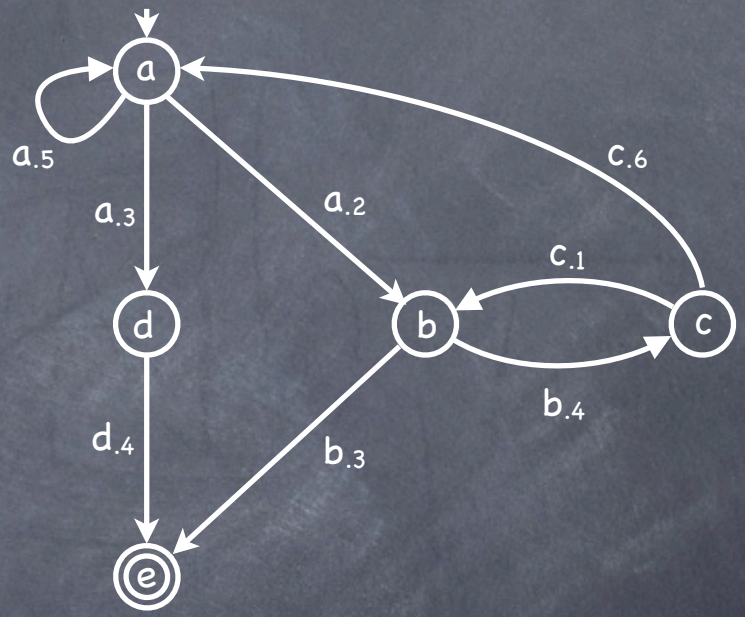


¿Qué estamos haciendo?

- Generación de contraejemplos

$(a_{.5}+a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*(a_{.2}(b_{.4}c_{.1})^*b_{.3}+a_{.3}d_{.4})$

$(a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.2}(b_{.4}c_{.1})^*b_{.3}$
$+ (a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.3}d_{.4}$



CONICET

FaMAF

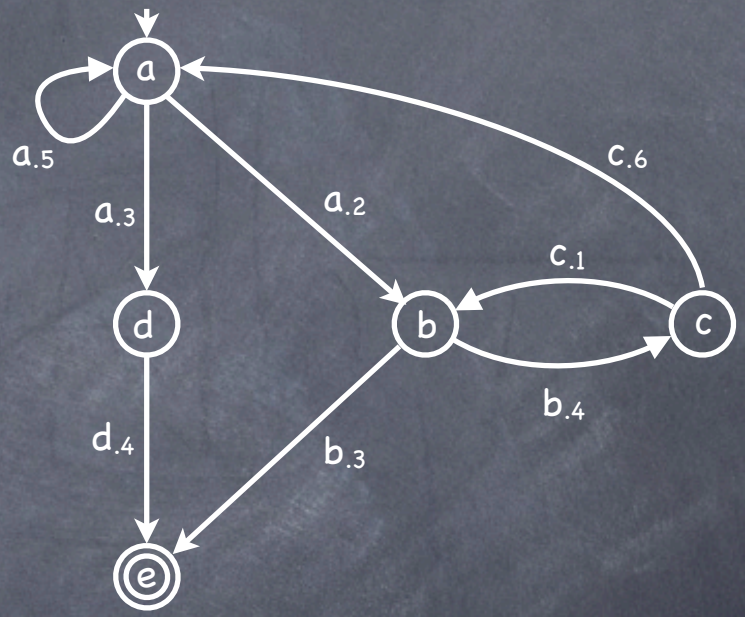
¿Qué estamos haciendo?

- Generación de contraejemplos

$(a_{.5}+a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*(a_{.2}(b_{.4}c_{.1})^*b_{.3}+a_{.3}d_{.4})$

$(a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.2}(b_{.4}c_{.1})^*b_{.3}$

$(a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.3}d_{.4}$



CONICET

FaMAF

¿Qué estamos haciendo?

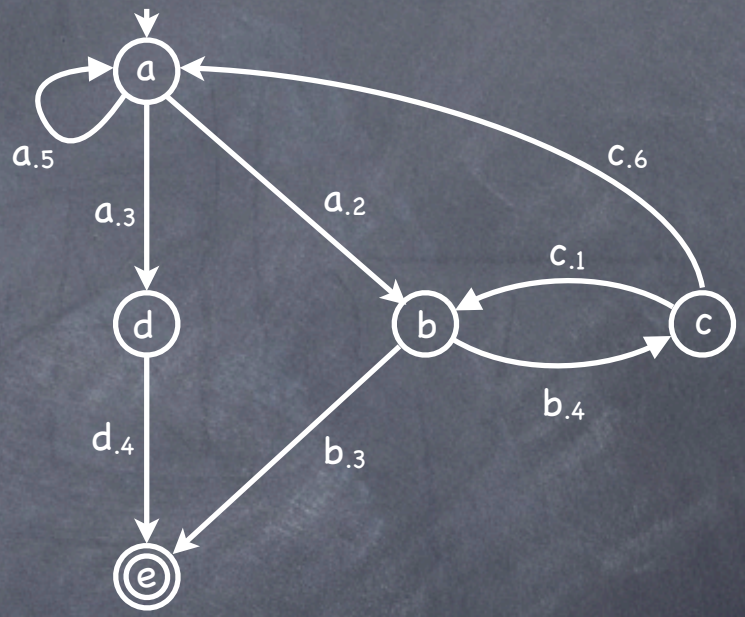
- Generación de contraejemplos

$(a_{.5}+a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*(a_{.2}(b_{.4}c_{.1})^*b_{.3}+a_{.3}d_{.4})$

$(a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.2}(b_{.4}c_{.1})^*b_{.3}$

$$\frac{1}{1-\left(0.5\cdot 0.2\cdot \frac{1}{1-0.4\cdot 0.1}\cdot 0.4\cdot 0.6\right)}\cdot 0.2\cdot \frac{1}{1-0.4\cdot 0.1}\cdot 0.3$$

$(a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.3}d_{.4}$



¿Qué estamos haciendo?

- Generación de contraejemplos

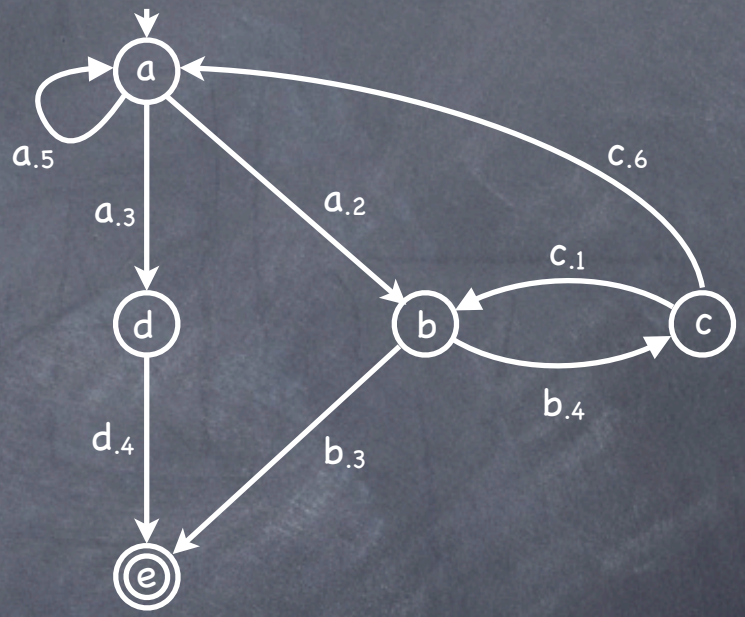
$(a_{.5}+a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*(a_{.2}(b_{.4}c_{.1})^*b_{.3}+a_{.3}d_{.4})$

$(a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.2}(b_{.4}c_{.1})^*b_{.3}$

0.138888... (a*a(bc)*bc)*a(bc)*be

$(a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.3}d_{.4}$

0.266666... (a*a(bc)*bc)*ade



CONICET

FaMAF

¿Qué estamos haciendo?

- Generación de contraejemplos

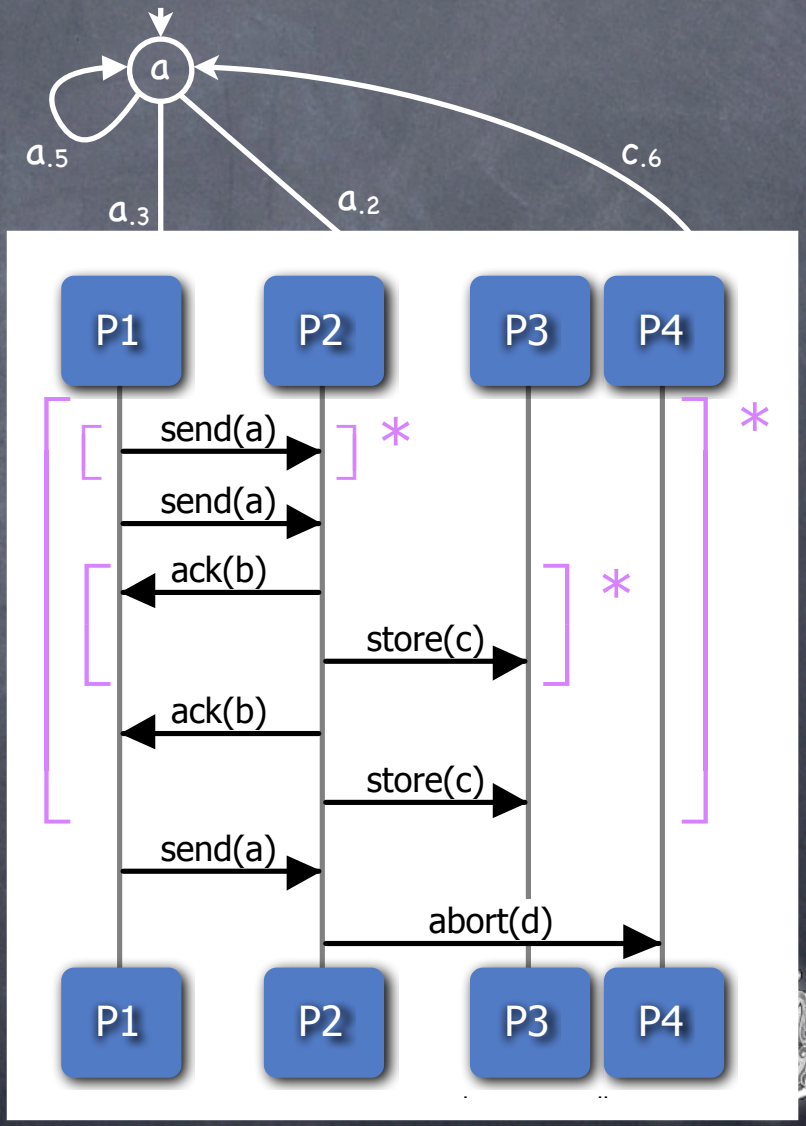
$(a_{.5}+a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*(a_{.2}(b_{.4}c_{.1})^*b_{.3}+a_{.3}d_{.4})$

$(a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.2}(b_{.4}c_{.1})^*b_{.3}$

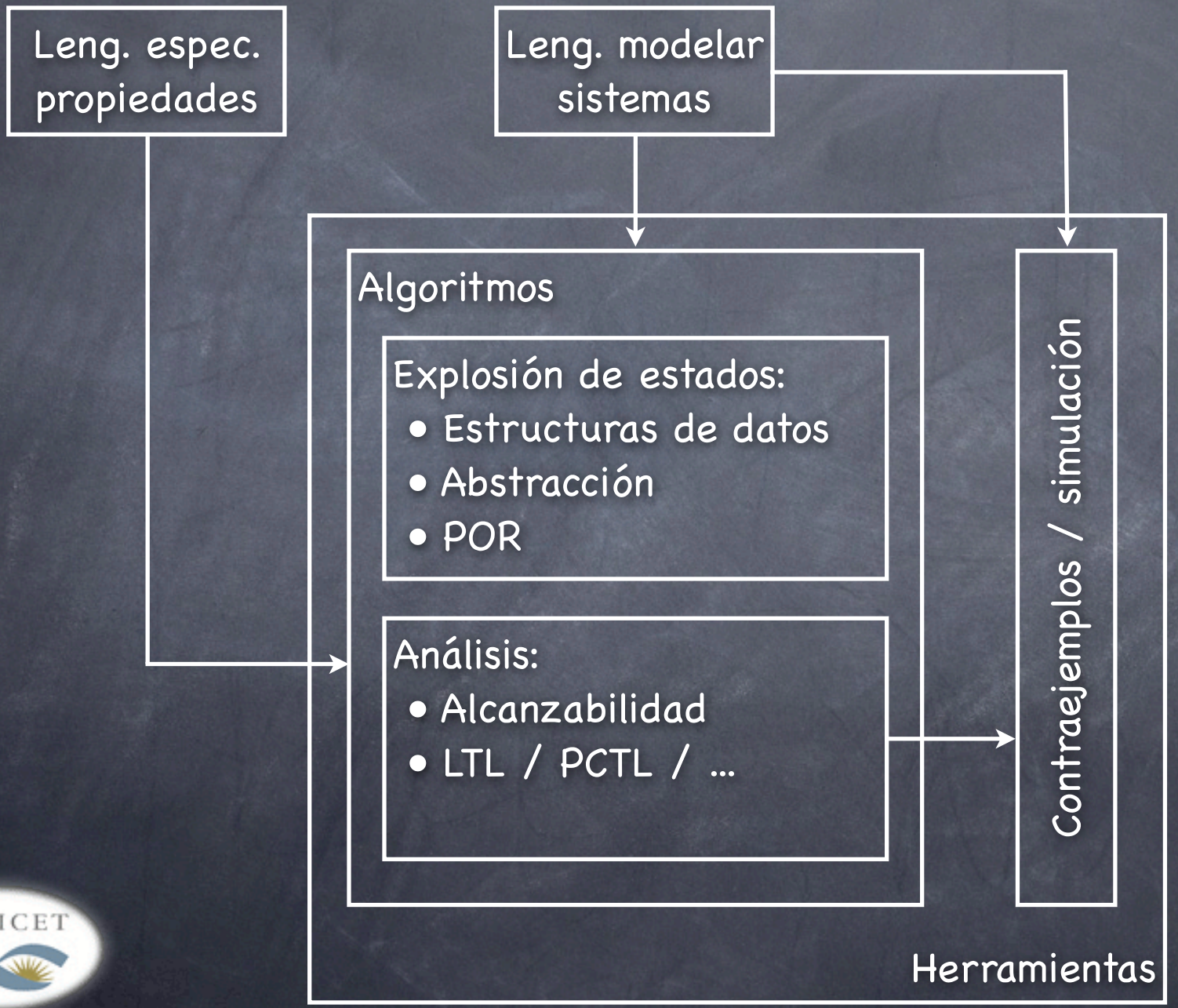
0.138888... (a*a(bc)*bc)*a(bc)*be

$(a_{.5}{}^*a_{.2}(b_{.4}c_{.1})^*b_{.4}c_{.6})^*a_{.3}d_{.4}$

0.266666... (a*a(bc)*bc)*ade



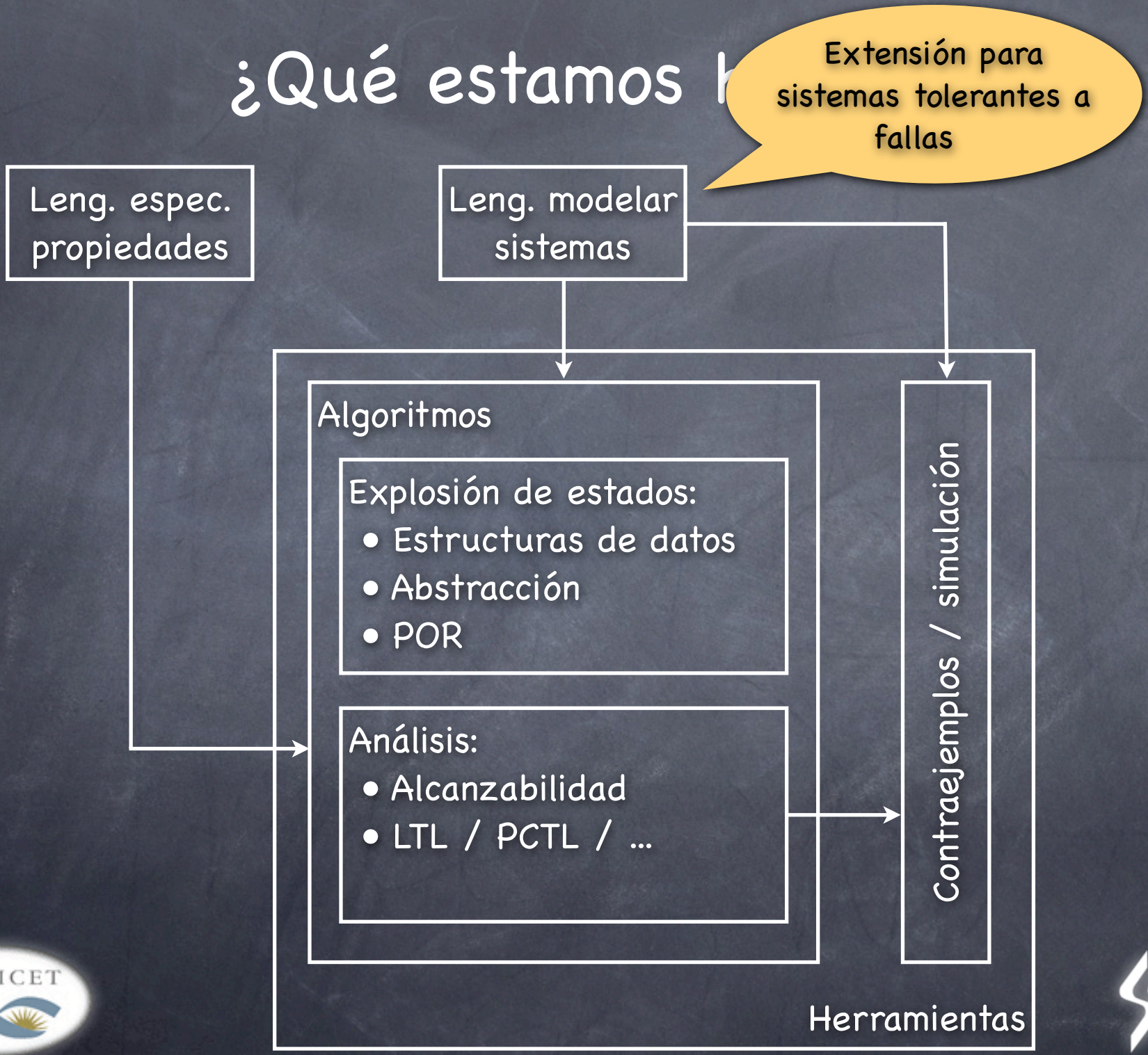
¿Qué estamos haciendo?



CONICET

FaMAF

¿Qué estamos h



CONICET

FaMAF

¿Qué estamos haciendo?

- Desarrollo de model checker cuantitativos
  - Modelado declarativo de fallas para el análisis de sistemas tolerantes a fallas

```
MODULE FailStopProcessor
FAULT FailStopFault
  pre(state = Operational);
  effect(state = Stopped);
  restores(0);
VAR
  b : boolean;
  state : {Operational, Stopped};
ASSIGN
  init(b) := 0;
  next(b) :=
    case
      state = Operational : !b;
      1                   : b;
    esac;
  init(state) := Operational;
  next(state) := state;
```

Falluto: no-probabilista, extiende NuSMV [Hames 2009]. Próximamente también en PRISM (prob +tiempo) [Bordenabe 2011?].

CONICET

FaMAF

¿Qué estamos haciendo?

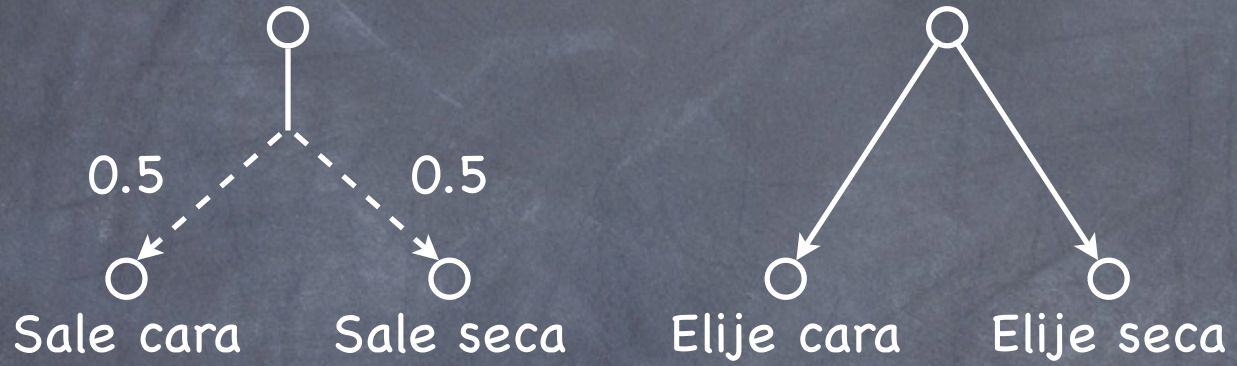
- Desarrollo de model checker cuantitativos
  - Modelado declarativo de fallas para el análisis de sistemas tolerantes a fallas

```
MODULE counter
FAULT crash
  pre(1);
  effect();
  restores(0);
VAR
  i : 0..4;
ASSIGN
  init(i) := 0;
  next(i) :=
    case
      i < 4 : i + 1 disabled_by {crash};
      i = 4 : 0 disabled_by {crash};
    esac;
```

Falluto: no-probabilista, extiende NuSMV [Hames 2009]. Próximamente también en PRISM (prob +tiempo) [Bordenabe 2011?].

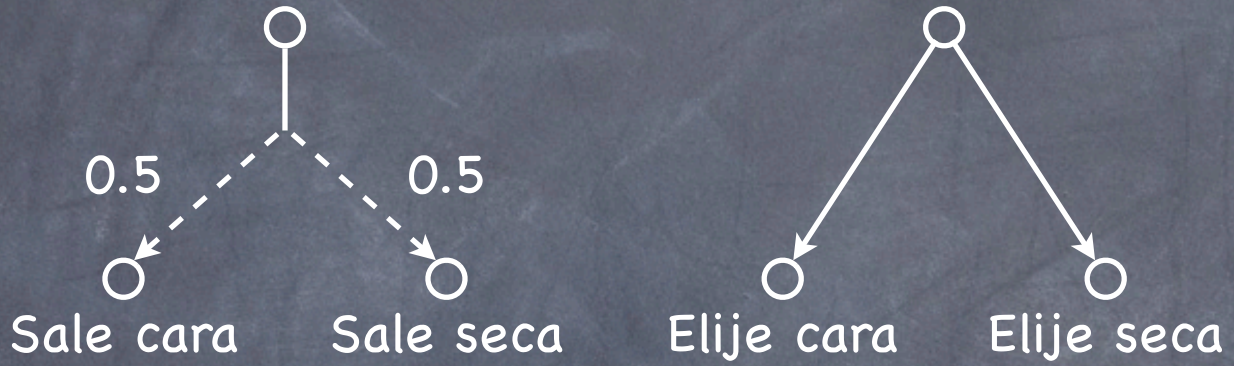
¿Qué estamos haciendo?

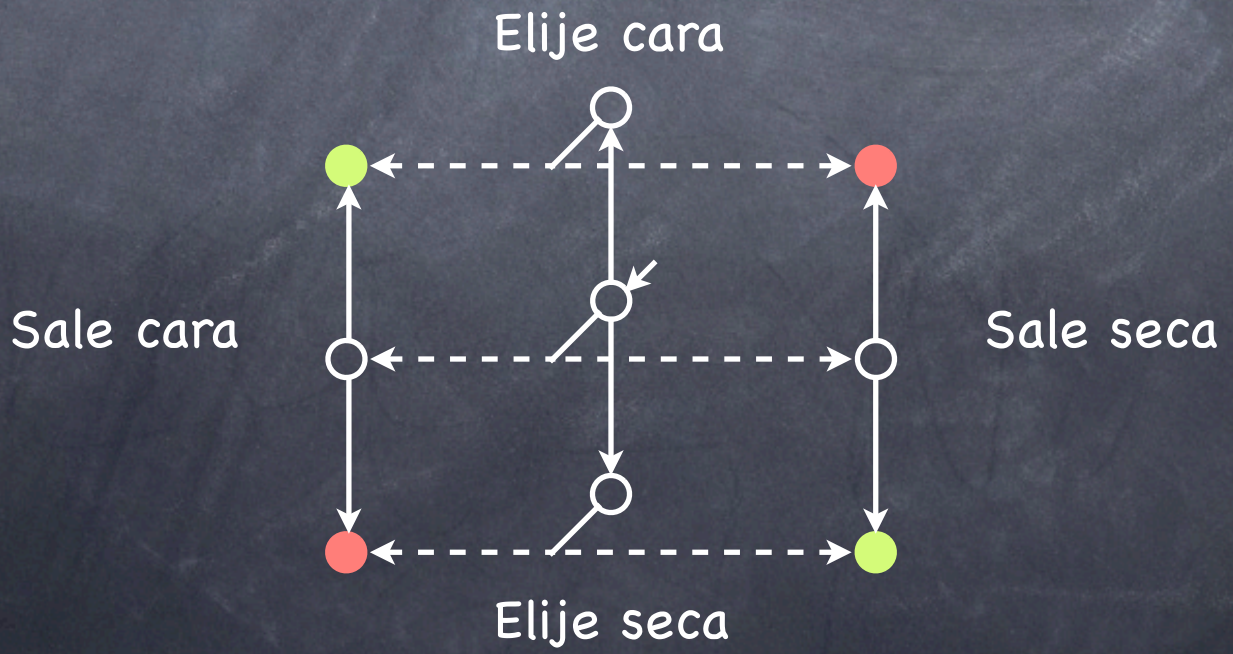
- Sist. distribuidos: todos los schedulers son muchos:



¿Qué estamos haciendo?

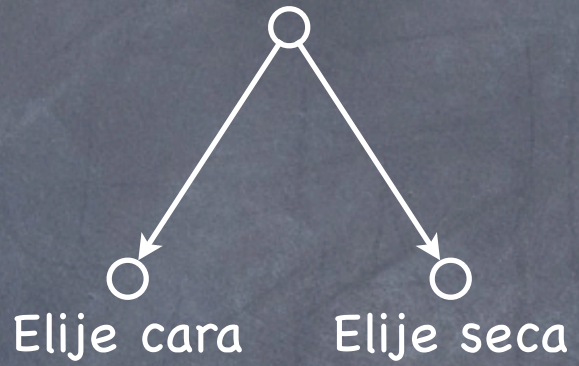
- Sist. distribuidos: todos los schedulers son muchos:



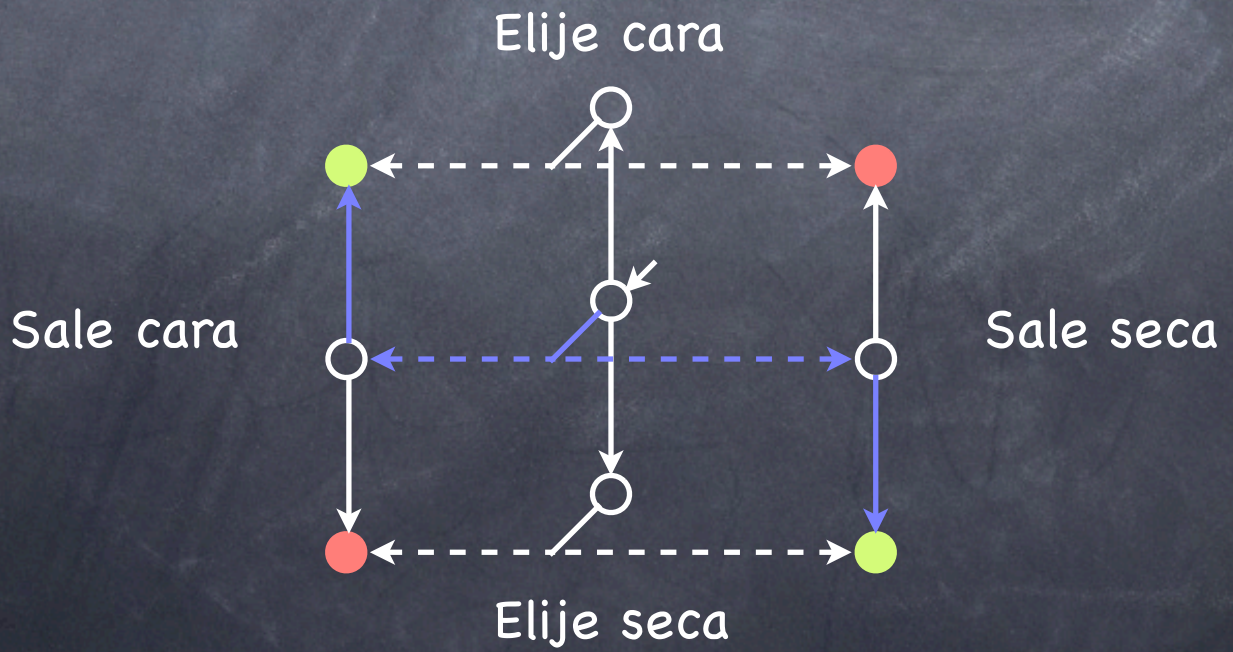


¿Qué estamos haciendo?

- Sist. distribuidos: todos los schedulers son muchos:

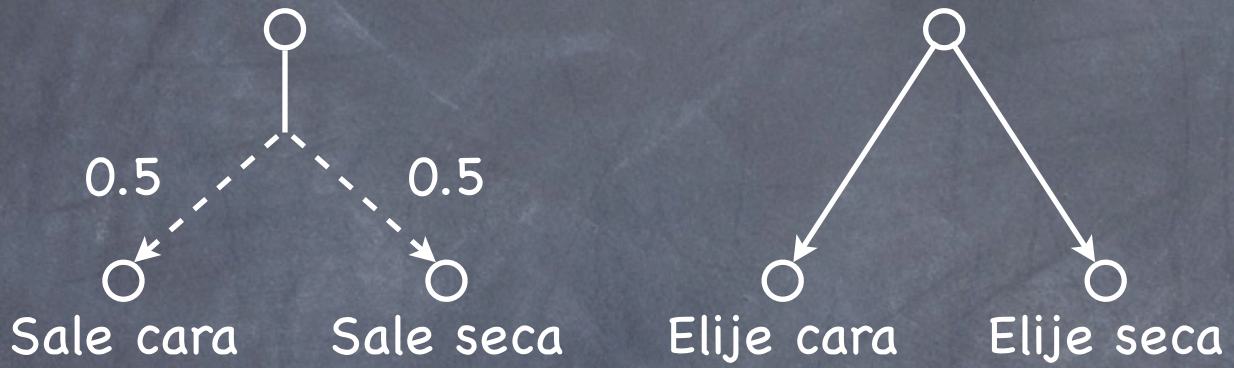


La máxima probabilidad de adivinar es 1 !!!!



¿Qué estamos haciendo?

- Sist. distribuidos: todos los schedulers son muchos:



La máxima probabilidad de adivinar es 1 !!!!

- Solución:
  - Considerar sólo los schedulers que respetan la elecciónes locales.
  - Desafortunadamente el problema de MCC es indecidible [Giro & D'Argenio, 2007] [Giro 2009]

¿Qué estamos haciendo?

- Sist. distribuidos: todos los schedulers son muchos y los que necesitamos no permiten MCC:
- Solución (o algo así):
  - Buscar un conjunto que "se parezca" y sea decidible ☹
  - Buscar cotas seguras:
    - Algoritmos específicos [Giro & D'Argenio, 2009]
    - Algoritmos basados en reducción de orden parcial [Giro, D'Argenio & Ferrer Fioriti, 2009]

¿Qué estamos haciendo?

- Todos los schedulers son muchos y los que necesitamos no permiten MCC:
- **ES** decidible para el caso finito:
  - Se reduce a problemas de optimización no lineal [Calin, Crouzen, D'Argenio, Hahn & Zhang 2010]
  - Aplicación:
    - propiedades de alcanzabilidad acotada,
    - protocolos de seguridad.

¿Qué estamos haciendo?

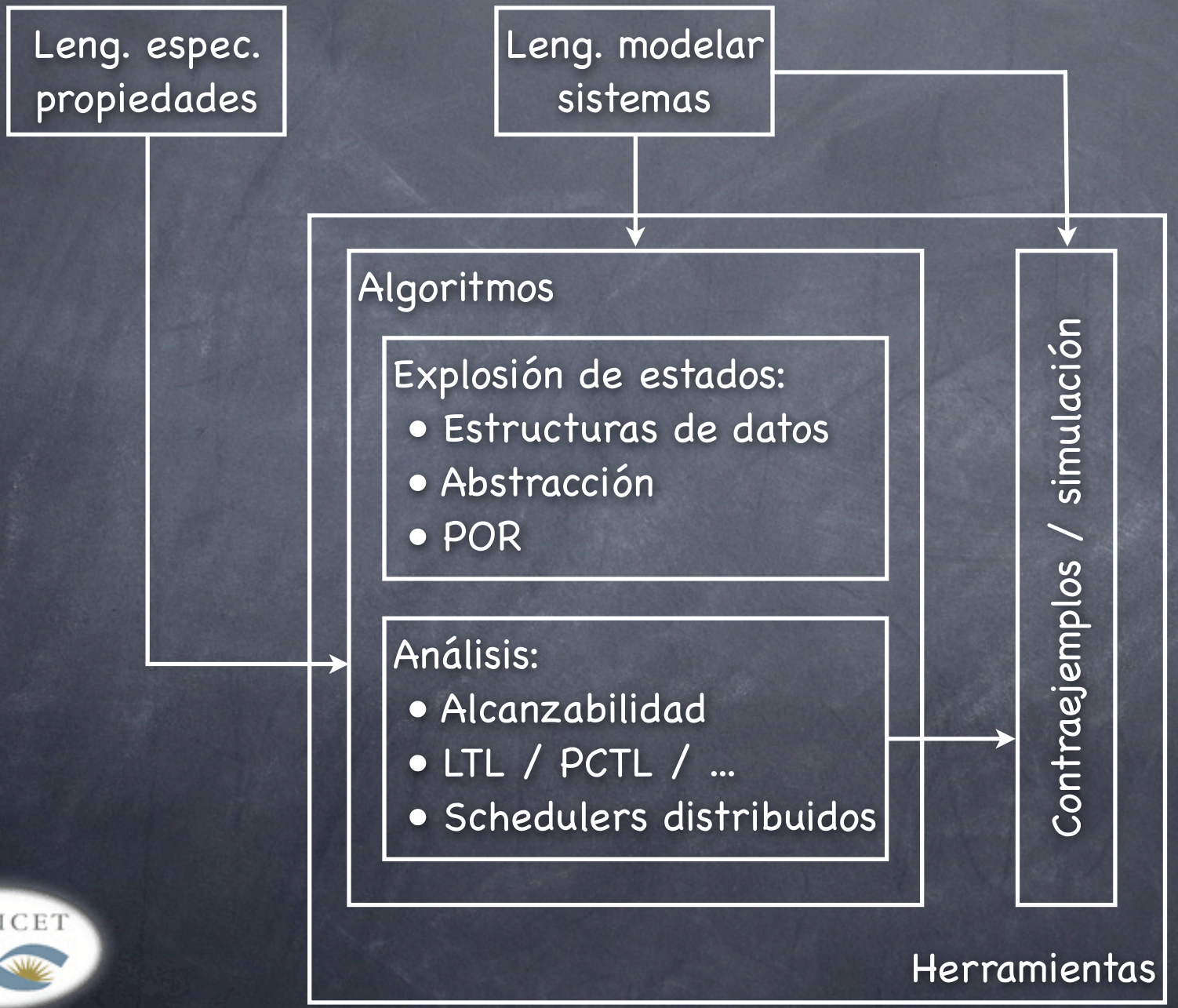
- Todos los schedulers son muchos y los que necesitamos no permiten MCC:
- **ES** decidible para el caso finito:
  - Se reduce a problemas de optimización no lineal [Calin, Crouzen, D'Argenio, Hahn & Zhang 2010]
  - Aplicación:
    - propiedades de alcanzabilidad acotada,
    - protocolos de seguridad.

Necesita algunos ajustes aún

CONICET

FaMAF

¿Qué estamos haciendo?



CONICET

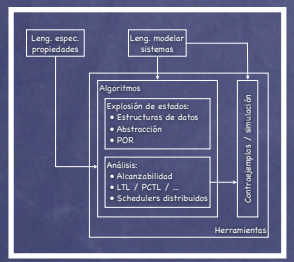
FaMAF

¿Qué estamos haciendo?

Prob. Discretas

MCC

DTMDP



CONICET

FaMAF

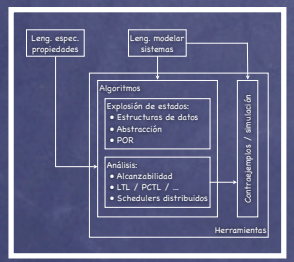
¿Qué estamos haciendo?

Prob. Continuas

Prob. Discretas

MCC

DTMDP



CONICET

FaMAF

¿Qué estamos haciendo?

Leng. de especificación:
- Propiedades
- Modelos de Sistemas

Herramientas

Semántica Simbólica

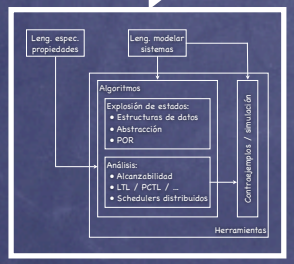
- Abstracciones
- Sobre / sub aprox. en modelos discretos.

Simulación por eventos discretos

Prob. Continuas

Prob. Discretas

MCC
DTMDP



Otros MC:
- Spin/SMV/...
- Uppaal/Zeus/...

CONICET

FaMAF

¿Qué estamos haciendo?

- Y el tiempo como variable estocástica:
  - Autómatas estocásticos y álgebras de procesos ♤ [D'Argenio & Katoen, 2005] [Bravetti & D'Argenio, 2004]
  - MoDeST: un lenguaje para la descripción de sistemas estocásticos y temporizados [Bohnenkamp, D'Argenio, Hermanns & Katoen, 2006]
  - Abstracción de probabilidades [D'Argenio, 2003] [Gebremichael & D'Argenio, 2005] [D'Argenio & Wolovick, 2011?]
  - Optimización de tests para sist. de tiempo real [Wolovick, D'Argenio & Qu, 2009] [Miretti 2010?]

¿Qué estamos haciendo?

- Y si todo es continuo? (probabilidades, no determinismo, estados...)
  - Estudio fundamental: Procesos de Markov etiquetados no determinsitas (NLMP) / bisimulaciones / Lógicas [D'Argenio, Wolovick, Sánchez Terraf, Celayes 2009] [Celayes, 2006] [D'Argenio, Wolovick, Sánchez Terraf 2011?] [Sánchez Terraf 2011?]
  - Schedulers sobre NLMP [Wolovick, 2011?]

Verificación de Sistemas con Probabilidad y Nodeterminismo

Pedro R. D'Argenio
FaMAF, UNC - CONICET

http://www.cs.famaf.unc.edu.ar/~dargenio/
dargenio@famaf.unc.edu.ar