

# Les Automates Probabilistes (Abstrait) en tant que Théorie de Spécification

Benoît Delahaye

Université de Nantes

2013-11-8

- 1 Introduction
- 2 Theories de Specification
- 3 Automates Probabilistes Abstraits

# Automates Probabilistes à la sauce Vérif (Lynch,Segala'94)

$$P = (S, A, L, AP, V, s_0)$$

# Automates Probabilistes à la sauce Vérif (Lynch,Segala'94)

$$P = (S, A, L, AP, V, s_0)$$

- $S$  : Ensemble d'états

$s_0 \in S$  : état initial

3

2

1

4

5

# Automates Probabilistes à la sauce Vérif (Lynch,Segala'94)

$$P = (S, A, L, AP, V, s_0)$$

- $S$  : Ensemble d'états

$s_0 \in S$  : état initial

- $A$  : Ensemble d'actions

3

2

1

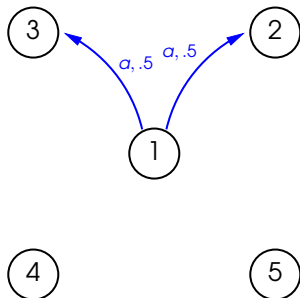
4

5

# Automates Probabilistes à la sauce Vérif (Lynch,Segala'94)

$$P = (S, A, L, AP, V, s_0)$$

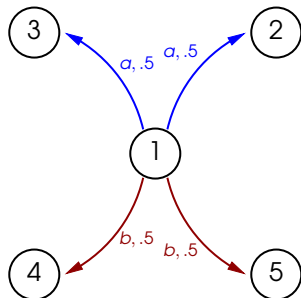
- $S$  : Ensemble d'états  
 $s_0 \in S$  : état initial
- $A$  : Ensemble d'actions
- $L \subseteq S \times A \times \text{Dist}(S)$   
Relation de transition



# Automates Probabilistes à la sauce Vérif (Lynch,Segala'94)

$$P = (S, A, L, AP, V, s_0)$$

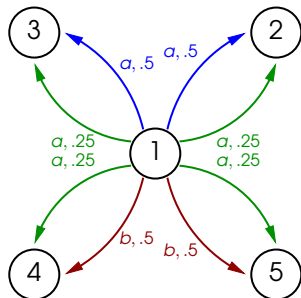
- $S$  : Ensemble d'états  
 $s_0 \in S$  : état initial
- $A$  : Ensemble d'actions
- $L \subseteq S \times A \times \text{Dist}(S)$   
Relation de transition



# Automates Probabilistes à la sauce Vérif (Lynch,Segala'94)

$$P = (S, A, L, AP, V, s_0)$$

- $S$  : Ensemble d'états  
 $s_0 \in S$  : état initial
- $A$  : Ensemble d'actions
- $L \subseteq S \times A \times \text{Dist}(S)$   
Relation de transition

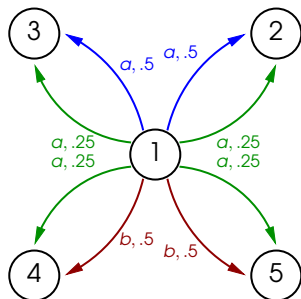




# Automates Probabilistes à la sauce Vérif (Lynch,Segala'94)

$$P = (S, A, L, AP, V, s_0)$$

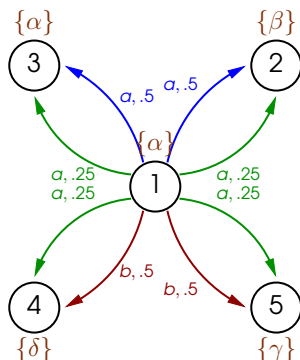
- $S$  : Ensemble d'états  
 $s_0 \in S$  : état initial
- $A$  : Ensemble d'actions
- $L \subseteq S \times A \times \text{Dist}(S)$   
Relation de transition
- $AP$  : Propositions Atomiques



# Automates Probabilistes à la sauce Vérif (Lynch,Segala'94)

$$P = (S, A, L, AP, V, s_0)$$

- $S$  : Ensemble d'états  
 $s_0 \in S$  : état initial
- $A$  : Ensemble d'actions
- $L \subseteq S \times A \times \text{Dist}(S)$   
Relation de transition
- $AP$  : Propositions Atomiques
- $V : S \rightarrow 2^{AP}$  : Labels d'états

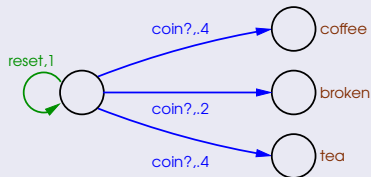


# Pour quoi faire ?

## Modélisation

Utiliser les PA pour modéliser des systèmes complexes

- Probabilistes
- Non-déterministes

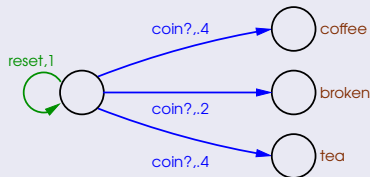


# Pour quoi faire ?

## Modélisation

Utiliser les PA pour modéliser des systèmes complexes

- Probabilistes
- Non-déterministes



## Outils

- Vérif : PCTL
- (Bi)Simulations
- Composition

$$\mathbb{P}_{>0.5}(F(\text{coffee}))$$

- 1 Introduction
- 2 Theories de Specification
- 3 Automates Probabilistes Abstraits

# Qu'est ce qu'une Théorie de Spécification ?

- Représentation **abstraite** d'une famille d'objets **de base**  
*Ex : Mots, Automates, Composants*
- Manipulation **haut-niveau**  
*Raisonnement générique*
- Design compositionnel  
*Combinaison, raffinement, abstraction*
- Algèbre  
*Propriétés formelles, opérations syntactiques*

# Une notion cruciale : l'implementation

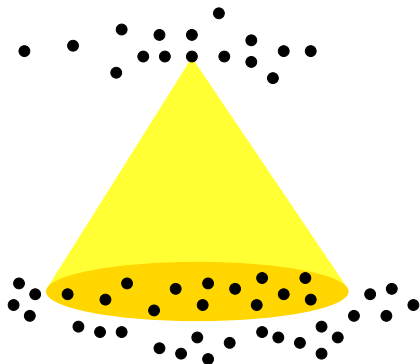


Specifications



Implementations

# Une notion cruciale : l'implementation

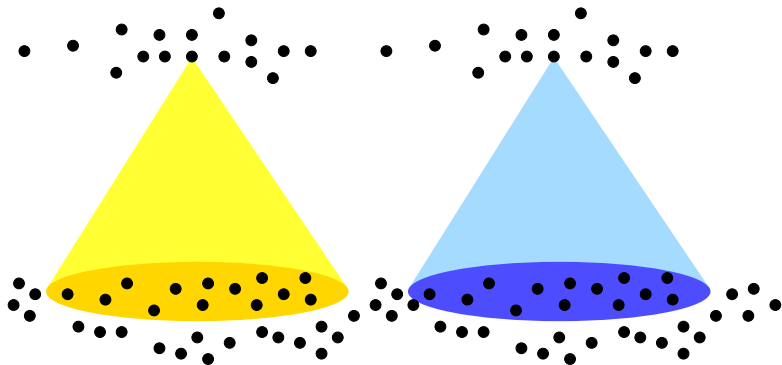


Specifications

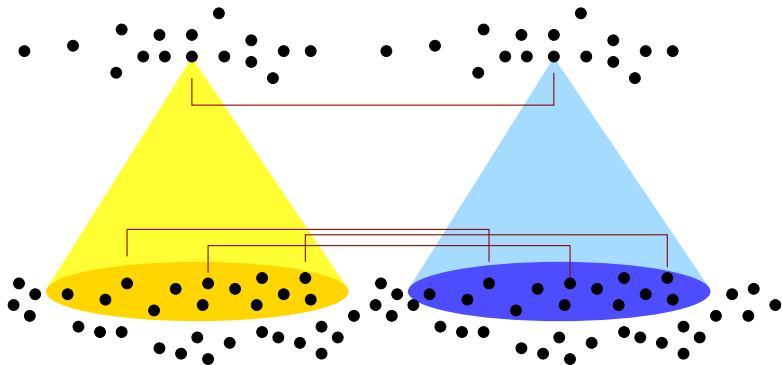
Implementations



# Une notion cruciale : l'implémentation



# Une notion cruciale : l'implémentation



## Consistence

$$S = \emptyset$$

or



## Consistence

$$S = \emptyset$$

or



## Implémentation Commune



## Consistence

$$S = \emptyset$$

or



## Implémentation Commune

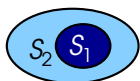


or



?

## Raffinement

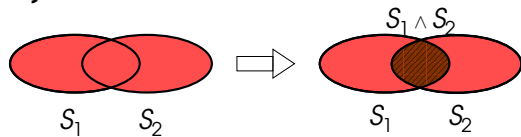


or



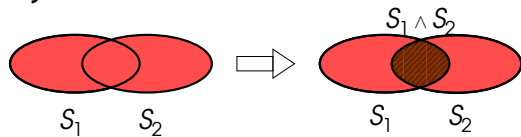
?

## Conjonction

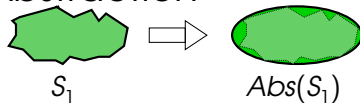


# Opérateurs à Composant Unique

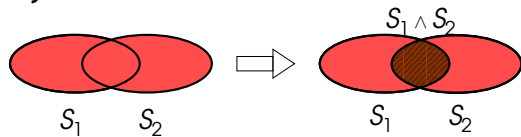
Conjonction



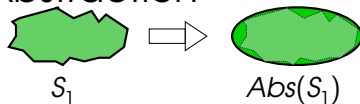
Abstraction



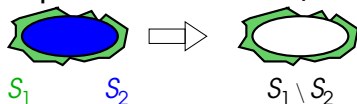
## Conjonction



## Abstraction

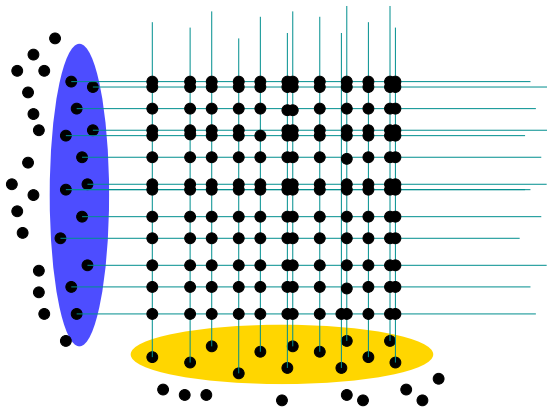


## Complémentation / Différence

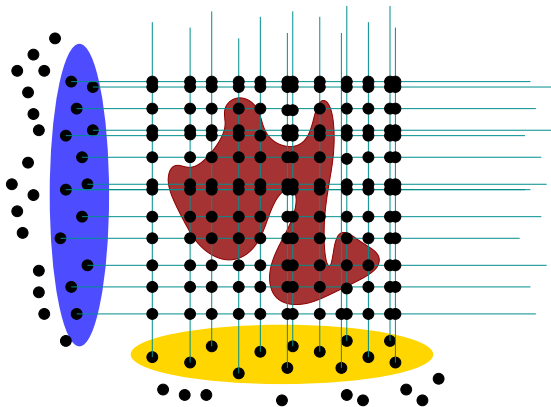




# Opérateurs à Composants Multiples



Composition Parallèle



Composition Parallèle **synchronisée**

## Raffinement

- **Correction :**
- **Complétude :**

## Raffinement

- **Correction** :  $S_1 \preceq S_2 \Rightarrow \llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket$
- **Complétude** :

## Raffinement

- **Correction** :  $S_1 \preceq S_2 \Rightarrow \llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket$
- **Complétude** :  $\llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket \Rightarrow S_1 \preceq S_2$

## Raffinement

- **Correction** :  $S_1 \preceq S_2 \Rightarrow \llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket$
- **Complétude** :  $\llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket \Rightarrow S_1 \preceq S_2$

## Conjonction

- **GLB** :
- **Intersection** :

## Raffinement



- **Correction** :  $S_1 \preceq S_2 \Rightarrow \llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket$
- **Complétude** :  $\llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket \Rightarrow S_1 \preceq S_2$

## Conjonction



- **GLB** :  $S_1 \preceq (S_2 \wedge S_3) \iff S_1 \preceq S_2 \text{ et } S_1 \preceq S_3$
- **Intersection** :

## Raffinement



- **Correction** :  $S_1 \preceq S_2 \Rightarrow \llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket$
- **Complétude** :  $\llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket \Rightarrow S_1 \preceq S_2$

## Conjonction



- **GLB** :  $S_1 \preceq (S_2 \wedge S_3) \iff S_1 \preceq S_2 \text{ et } S_1 \preceq S_3$
- **Intersection** :  $\llbracket S_1 \wedge S_2 \rrbracket = \llbracket S_1 \rrbracket \cap \llbracket S_2 \rrbracket$



## Raffinement

- **Correction** :  $S_1 \preceq S_2 \Rightarrow \llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket$
- **Complétude** :  $\llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket \Rightarrow S_1 \preceq S_2$

## Conjonction

- **GLB** :  $S_1 \preceq (S_2 \wedge S_3) \iff S_1 \preceq S_2 \text{ et } S_1 \preceq S_3$
- **Intersection** :  $\llbracket S_1 \wedge S_2 \rrbracket = \llbracket S_1 \rrbracket \cap \llbracket S_2 \rrbracket$

## Composition

- **Correction** :
  
- **Précongruence** :

## Raffinement

- **Correction** :  $S_1 \preceq S_2 \Rightarrow \llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket$
- **Complétude** :  $\llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket \Rightarrow S_1 \preceq S_2$

## Conjonction

- **GLB** :  $S_1 \preceq (S_2 \wedge S_3) \iff S_1 \preceq S_2 \text{ et } S_1 \preceq S_3$
- **Intersection** :  $\llbracket S_1 \wedge S_2 \rrbracket = \llbracket S_1 \rrbracket \cap \llbracket S_2 \rrbracket$

## Composition

- **Correction** :  
 $P_1 \models S_1 \text{ et } P_2 \models S_2 \Rightarrow P_1 \parallel P_2 \models S_1 \parallel S_2$
- **Précongruence** :

## Raffinement

- **Correction** :  $S_1 \preceq S_2 \Rightarrow \llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket$
- **Complétude** :  $\llbracket S_1 \rrbracket \subseteq \llbracket S_2 \rrbracket \Rightarrow S_1 \preceq S_2$

## Conjonction

- **GLB** :  $S_1 \preceq (S_2 \wedge S_3) \iff S_1 \preceq S_2 \text{ et } S_1 \preceq S_3$
- **Intersection** :  $\llbracket S_1 \wedge S_2 \rrbracket = \llbracket S_1 \rrbracket \cap \llbracket S_2 \rrbracket$

## Composition

- **Correction** :  
 $P_1 \models S_1 \text{ et } P_2 \models S_2 \Rightarrow P_1 \parallel P_2 \models S_1 \parallel S_2$
- **Précongruence** :  
 $S_1 \preceq S'_1 \text{ et } S_2 \preceq S'_2 \Rightarrow S_1 \parallel S_2 \preceq S'_1 \parallel S'_2$

- 1 Introduction
- 2 Theories de Specification
- 3 Automates Probabilistes Abstraits**

Comment représenter un *ensemble* de PAs ?

Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

Valuations

Distributions

Transitions

Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

Valuations

$$2^{AP} \Rightarrow 2^{2^{AP}}$$

Distributions

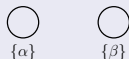
Transitions



Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

Valuations

$$2^{AP} \Rightarrow 2^{2^{AP}}$$



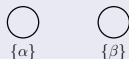
Distributions

Transitions

Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

## Valuations

$$2^{AP} \Rightarrow 2^{2^{AP}}$$



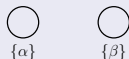
## Distributions

## Transitions

Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

## Valuations

$$2^{AP} \Rightarrow 2^{2^{AP}}$$



## Distributions

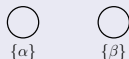
$$Dist(S) \Rightarrow \mathcal{P}(Dist(S))$$

## Transitions

Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

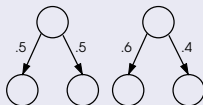
## Valuations

$$2^{AP} \Rightarrow 2^{2^{AP}}$$



## Distributions

$$Dist(S) \Rightarrow \mathcal{P}(Dist(S))$$

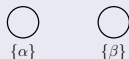


## Transitions

Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

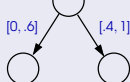
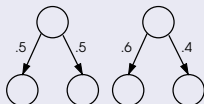
## Valuations

$$2^{AP} \Rightarrow 2^{2^{AP}}$$



## Distributions

$$\text{Dist}(S) \Rightarrow \mathcal{P}(\text{Dist}(S))$$

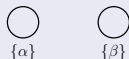


## Transitions

Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

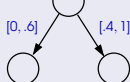
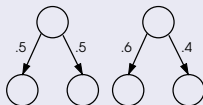
## Valuations

$$2^{AP} \Rightarrow 2^{2^{AP}}$$



## Distributions

$$\text{Dist}(S) \Rightarrow \mathcal{P}(\text{Dist}(S))$$



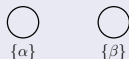
## Transitions

$$\mathbb{B}_2 \Rightarrow \mathbb{B}_3$$

Comment représenter un *ensemble* de PAs ?  
(en conservant une représentation graphique *finie*)

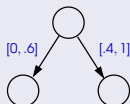
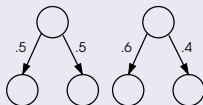
## Valuations

$$2^{AP} \Rightarrow 2^{2^{AP}}$$



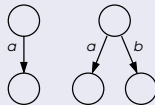
## Distributions

$$Dist(S) \Rightarrow \mathcal{P}(Dist(S))$$



## Transitions

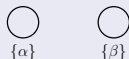
$$\mathbb{B}_2 \Rightarrow \mathbb{B}_3$$



## Comment représenter un *ensemble* de PAs ? (en conservant une représentation graphique *finie*)

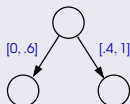
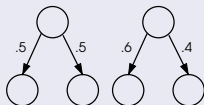
### Valuations

$$2^{AP} \Rightarrow 2^{2^{AP}}$$



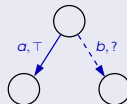
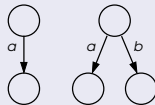
### Distributions

$$Dist(S) \Rightarrow \mathcal{P}(Dist(S))$$



### Transitions

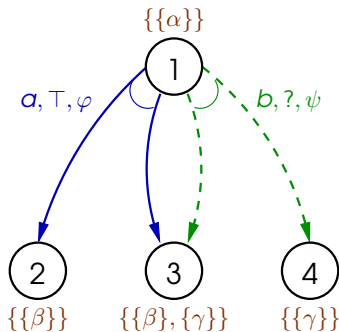
$$\mathbb{B}_2 \Rightarrow \mathbb{B}_3$$





# Abstract Probabilistic Automata

$$N = (S, A, \mathcal{L}, AP, \mathcal{V}, S_0)$$



$$\mu \in \varphi \iff (\mu(1) = \mu(4) = 0) \wedge (\mu(2) > .6)$$

$$\nu \in \psi \iff (\nu(1) = \nu(2) = 0) \wedge (\frac{\nu(3)}{\nu(4)} > 2)$$



## Composition

**Composition**

**Consistence**

**Composition**

**Conjonction**

**Consistence**

**Composition**

**Conjonction**

**Consistence**

**Correction**

**Composition**

**Conjonction**

**Consistence**

**Différence**

**Correction**

**Composition**

**Conjonction**

**Raffinement**

**Consistence**

**Différence**

**Correction**



**Composition**

**Déterminisation**

**Conjonction**

**Raffinement**

**Consistence**

**Différence**

**Correction**

**Composition**

**Déterminisation**

**Conjonction**

**Raffinement**

**Consistence**

**Complétude**

**Différence**

**Correction**

**Composition**

**Déterminisation**

**Conjonction**

**Logique**

**Raffinement**

**Consistence**

**Complétude**

**Différence**

**Correction**

**Composition**

**Déterminisation**

**Conjonction**

**Logique**

**Implémentation commune**

**Raffinement**

**Consistence**

**Complétude**

**Différence**

**Correction**

**Composition**

**Déterminisation**

**Conjonction**

**Logique**

**Abstraction**

**Implémentation commune**

**Raffinement**

**Consistence**

**Complétude**

**Différence**

**Correction**

**Composition**

**Déterminisation**

**Conjonction**

**Logique**

**Abstraction**

**Implémentation commune**

**Raffinement**

**Consistence**

**Complétude**

**Différence**

**Correction**

**Déterminisme**

**Composition**                      **Déterminisation**

**Conjonction**                      **Logique**

**Abstraction**                      **Implémentation commune**

**Raffinement**                      **Consistence**

**Complétude**                      **Différence**

**Correction**                      **Déterminisme**

**Stuttering**

**Composition**                      **Déterminisation**

**Conjonction**                      **Logique**

**Abstraction**                      **Implémentation commune**

**Raffinement**                      **Consistence**

**Complétude**                      **Différence**

**Correction**                      **Déterminisme**

**Stuttering**

**Outil**



**Composition**                      **Déterminisation**

**Conjonction**                      **Logique**

**Abstraction**                      **Implémentation commune**

**Raffinement**                      **Consistence**

**Complétude**                      **Différence**

**Correction**                      **Déterminisme**

**Stuttering**

**Outil**                      **Complexité**

Composition                      Déterminisation

Conjonction                      Logique

Abstraction                      Implémentation commune

**Applications**                      Consistance

Raffinement

Complétude                      Différence

Correction                      Déterminisme

Outil                      Stuttering

Complexité

Composition                      Déterminisation

Conjonction                      Logique

Abstraction                      Implémentation commune

**Applications**                      Consistance

Raffinement                      **Quotient**

Complétude                      Différence

Correction                      Déterminisme

Outil                      Stuttering

Complexité

(TCS'11) **Constraint Markov Chains.** *B. Caillaud, B. Delahaye, K.G. Larsen, A. Legay, M.L. Pedersen, A. Wasowski*

(I&C'13/14) **Abstract Probabilistic Automata.** *B. Delahaye, J.P. Katoen, K.G. Larsen, A. Legay, M.L. Pedersen, F. Sher, A. Wasowski*