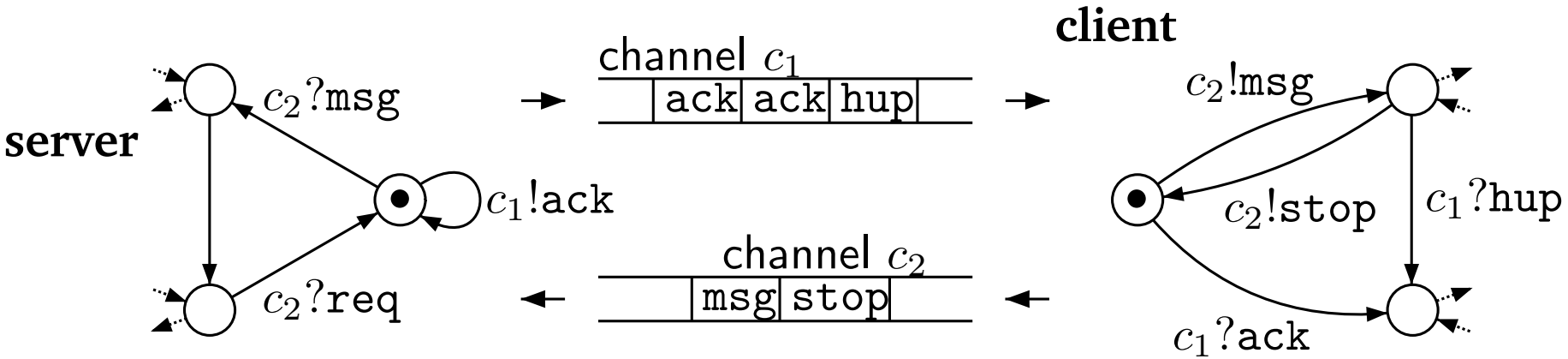
Approche probabiliste pour la vérification de propriétés de vivacité dans les *Lossy Channel Systems*

Ph. Schnoebelen & N. Bertrand

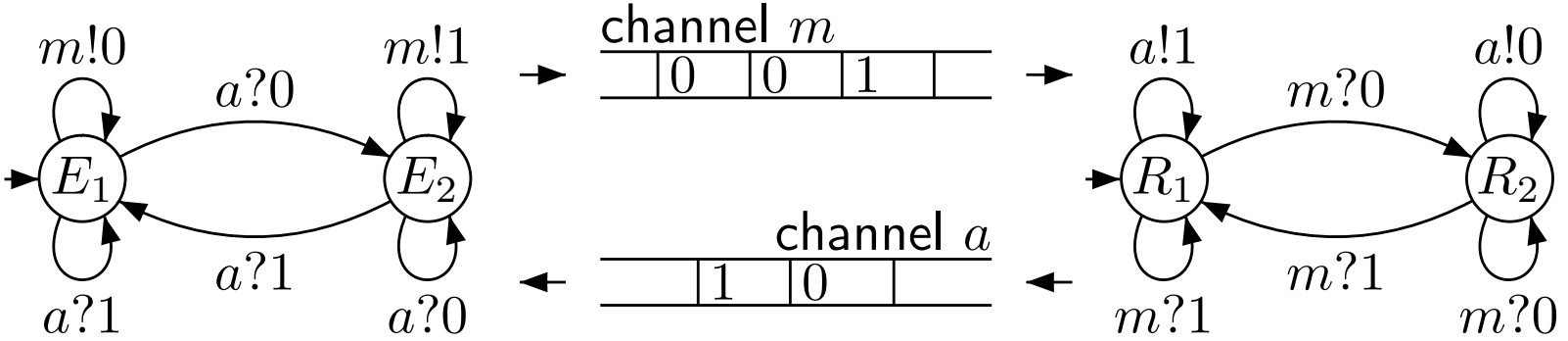
Channel systems

These are processes communicating via unbounded FIFO channels

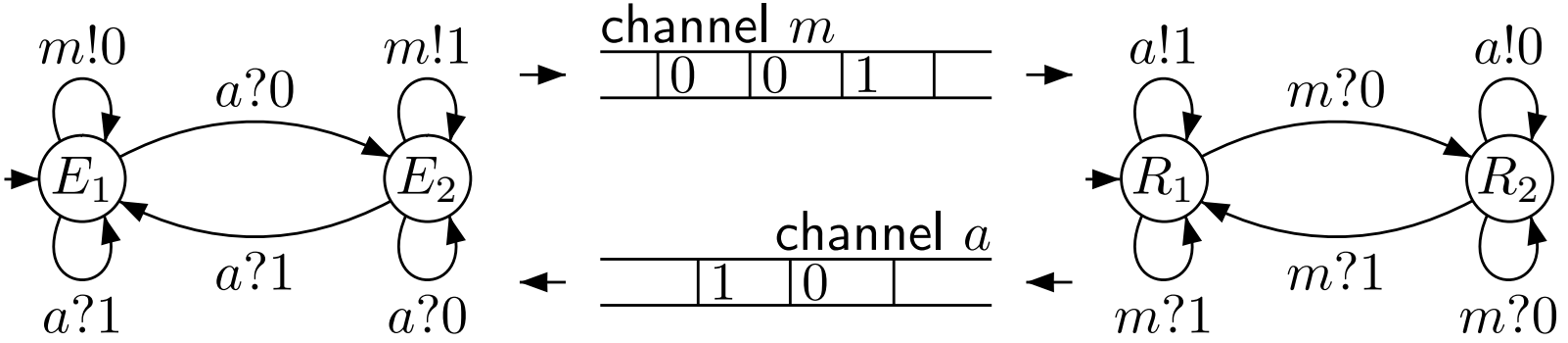


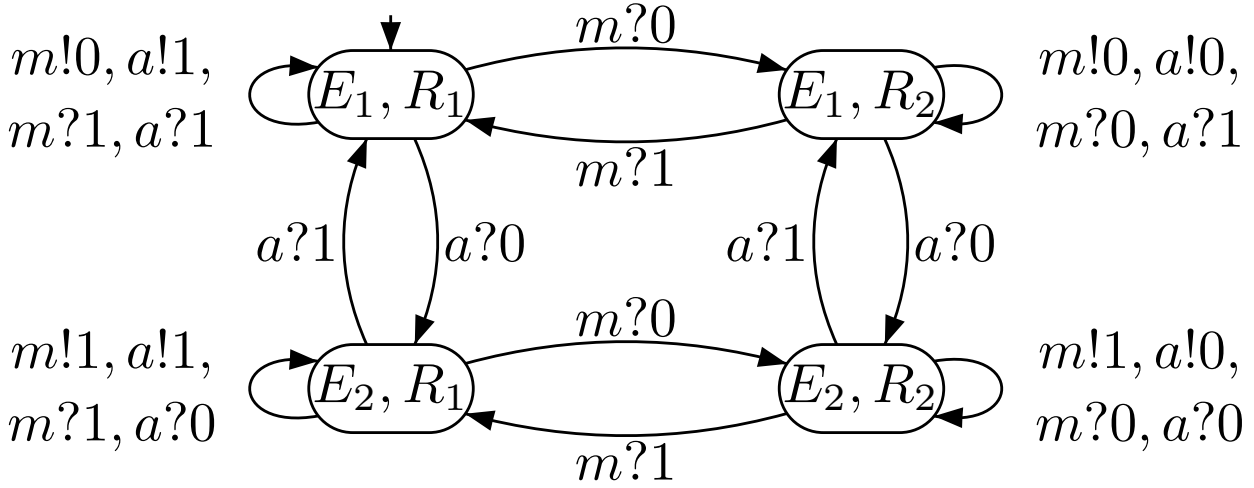
- model for asynchronous communications protocols
- finite-state control + infinite-range variables

Lossy Channel Systems



Lossy Channel Systems





Some results on Lossy Channel Systems

Decidability results

Termination	Decidable	Finkel
Reachability	Decidable	Pachl, Abdulla/Jonsson, ../Bouajjani/Annichini
Safety properties	Decidable	Abdulla/Jonsson
Eventuality	Decidable	Abdulla/Jonsson

Some results on Lossy Channel Systems

Decidability results

Termination	Decidable	Finkel
Reachability	Decidable	Pachl, Abdulla/Jonsson, ../Bouajjani/Annichini
Safety properties	Decidable	Abdulla/Jonsson
Eventuality	Decidable	Abdulla/Jonsson

Undecidability results

Liveness LTL properties	Undecidable	Abdulla/Jonsson
Eventuality assuming fairness	Undecidable	Abdulla/Jonsson
Boundedness	Undecidable	Mayr
Equivalence between 2 systems	Undecidable	Schnoebelen

Some results on Lossy Channel Systems

Decidability results

Termination	Decidable	Finkel
Reachability	Decidable	Pachl, Abdulla/Jonsson, ../Bouajjani/Annichini
Safety properties	Decidable	Abdulla/Jonsson
Eventuality	Decidable	Abdulla/Jonsson

Undecidability results

Liveness LTL properties	Undecidable	Abdulla/Jonsson
Eventuality assuming fairness	Undecidable	Abdulla/Jonsson
Boundedness	Undecidable	Mayr
Equivalence between 2 systems	Undecidable	Schnoebelen

Conclusion: Safety decidable. Liveness undecidable.

Liveness properties

Aim Verify liveness and fairness properties, eventuality properties assuming fairness hypothesis

On the example of Alternated Bit Protocol, verify progress properties of the form:

- $\phi = \Box\Diamond E_1 \wedge \Box\Diamond E_2 \wedge \Box\Diamond R_1 \wedge \Box\Diamond R_2$
  undecidable (general case) and false
- $\psi = fair \rightarrow \phi$
  where $fair$ is a formula describing fairness
  (even more) undecidable!

Une approche probabiliste

On considère que les pertes de message ne sont pas des événements non-déterministes, mais des fautes apparaissant de façon probabiliste. P.ex. chaque perte est indépendante des autres et obéit à une loi constante.

Une approche probabiliste

On considère que les pertes de message ne sont pas des événements non-déterministes, mais des fautes apparaissant de façon probabiliste. P.ex. chaque perte est indépendante des autres et obéit à une loi constante.

Conséquences :

1. On introduit une hypothèse d'équité réaliste sur les pertes de message.

2. On donne une mesure aux ensembles de comportements (un comportement qui a une probabilité 0 n'est pas nécessairement logiquement interdit).

Une approche probabiliste

On considère que les pertes de message ne sont pas des événements non-déterministes, mais des fautes apparaissant de façon probabiliste. P.ex. chaque perte est indépendante des autres et obéit à une loi constante.

Conséquences :

1. On introduit une hypothèse d'équité réaliste sur les pertes de message.

2. On donne une mesure aux ensembles de comportements (un comportement qui a une probabilité 0 n'est pas nécessairement logiquement interdit).

Autre conséquence utile :

Une modélisation probabiliste naturelle des pertes de message permet de garantir l'existence d'un attracteur fini (un ensemble fini de configurations qui sera visité infiniment souvent avec probabilité 1).

Une approche probabiliste

On considère que les pertes de message ne sont pas des événements non-déterministes, mais des fautes apparaissant de façon probabiliste. P.ex. chaque perte est indépendante des autres et obéit à une loi constante.

Conséquences :

1. On introduit une hypothèse d'équité réaliste sur les pertes de message.

2. On donne une mesure aux ensembles de comportements (un comportement qui a une probabilité 0 n'est pas nécessairement logiquement interdit).

Autre conséquence utile :

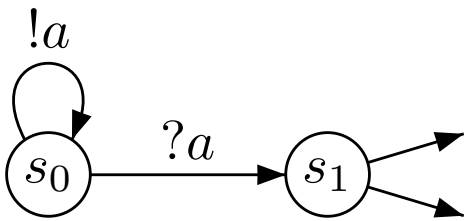
Une modélisation probabiliste naturelle des pertes de message permet de garantir l'existence d'un attracteur fini (un ensemble fini de configurations qui sera visité infiniment souvent avec probabilité 1).

Inconvénient :

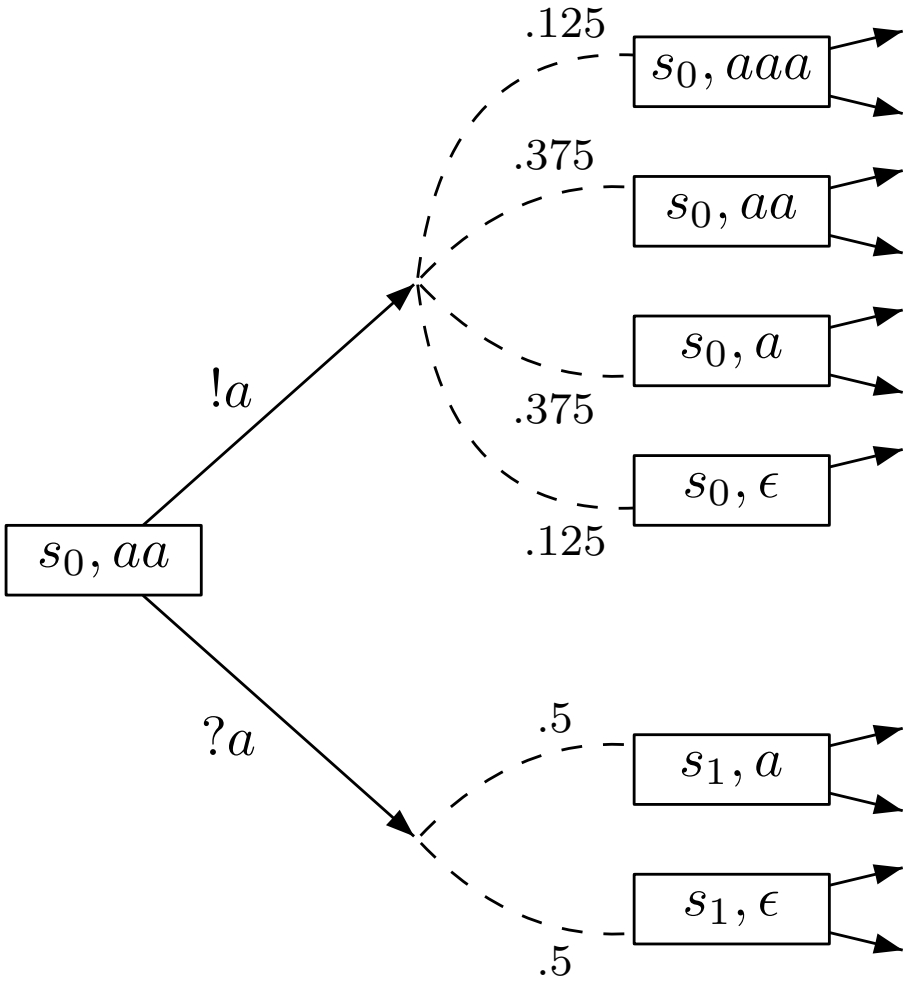
Les modèles deviennent des processus de décision markoviens.

Le modèle

Actions : non-déterministes
Pertes : probabilistes



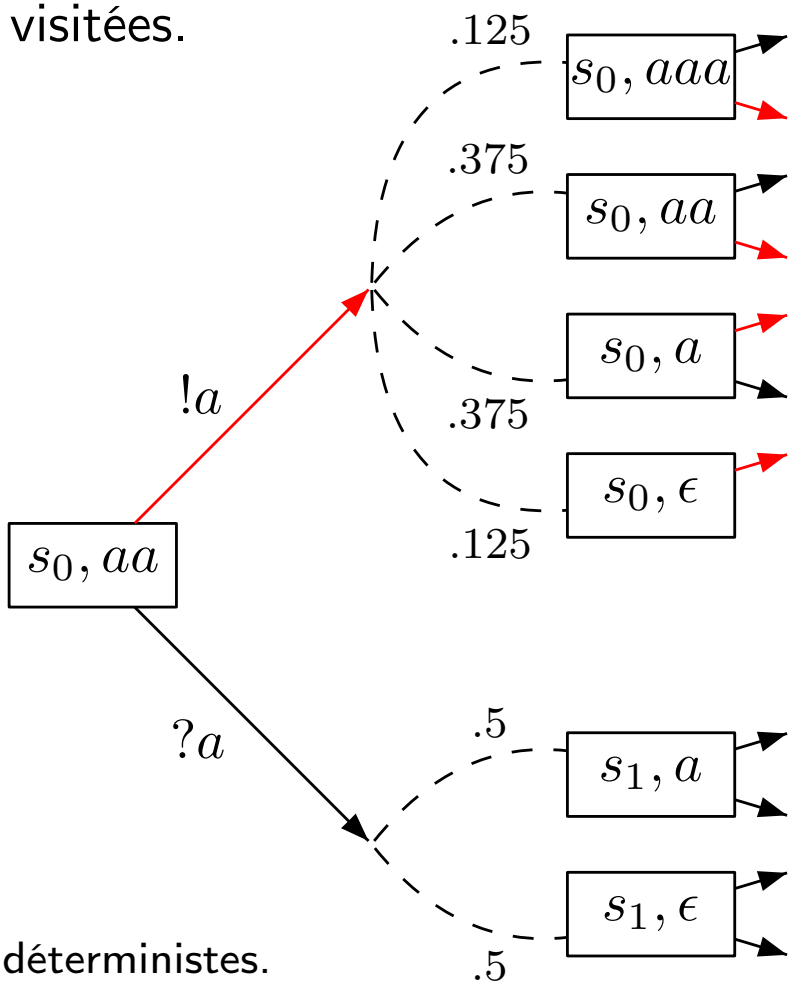
avec $p_{loss} = \frac{1}{2}$



On obtient un processus de décision markovien.

Comportement

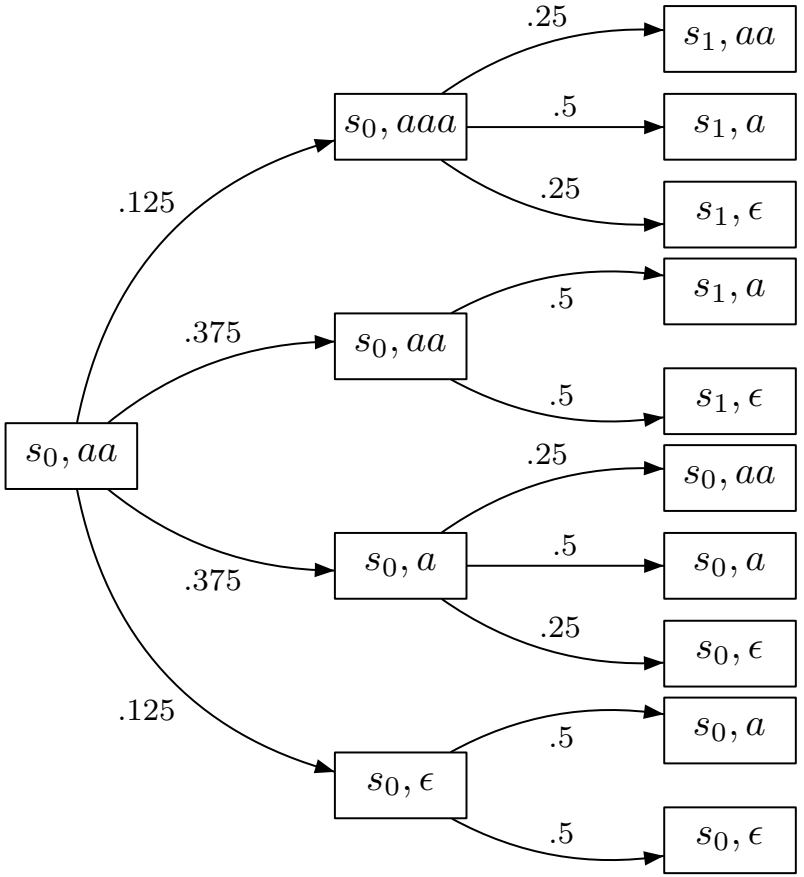
Adversaire : il fait les choix non-déterministes, en se basant sur l'historique des configurations précédemment visitées.



NB : On considère des adversaires déterministes.

Comportement

Pour un adversaire u donné, le MDP donne lieu à une chaîne de Markov.



On peut alors définir la probabilité qu'une propriété ϕ soit vérifiée par le système « sous u », notée $\mathbb{P}(u \models \phi)$.

Objectifs de vérification

Chaînes de Markov

$\mathbb{P}(\phi) = 1$?

Systèmes non-déterministes

$\forall u,\ u \models \phi$?

Objectifs de vérification

Chaînes de Markov

$\mathbb{P}(\phi) = 1$?

Systèmes non-déterministes

$\forall u,\ u \models \phi$?

Processus de décision markoviens

$\forall u,\ \mathbb{P}(u \models \phi) = 1$?

Questions

Model Checking Markov Decision Processes

$$\forall u,\ \mathbb{P}(u \models \phi) = 1\ ?$$

We consider LTL formulae of the form $\Diamond A$ (guarantee), $\bigwedge_i \Box\Diamond A_i$ (response), $\bigwedge_i(\Box\Diamond A_i \vee \Diamond\Box B_i)$ (reactivity), or their negations.

Duality and/or negation, give rise to the following problems:

- $\forall u,\ \mathbb{P}(u \models \phi) = 0$
- $\forall u,\ \mathbb{P}(u \models \phi) > 0$
- $\forall u,\ \mathbb{P}(u \models \phi) < 1$

Answers

Model Checking Markov Decision Processes

$$\forall u,\ \mathbb{P}(u \models \phi) = 1\ ?$$

- Unfortunately, the problem is undecidable in the general case.
- Many cases are decidable.

All problems become decidable under the assumption that the schedulers are memory-bounded.

The decision methods are reductions to reachability questions in the underlying nondeterministic lossy channel system.

Questions soulevées

- Le modèle est-il pertinent ?
- Quelques ultimes réglages techniques sont encore nécessaires.
- Les algorithmes de décision sont-ils suffisamment efficaces ?

Questions soulevées

- Le modèle est-il pertinent ?
- Quelques ultimes réglages techniques sont encore nécessaires.
- Les algorithmes de décision sont-ils suffisamment efficaces ?

Plus généralement

- Cette approche s'étend-elle à des systèmes plus riches (p.ex. *lossy channel systems* temporisés) ?
- Suggère-t-elle des pistes pour la vérification de propriétés de vivacité dans d'autres modèles ?