# Utilisation de TReX pour la vérification de «Lossy Channels» à pertes probabilistes

Nathalie Bertrand, Christophe Darlot & Philippe Schnoebelen

# Cadre général

Systèmes à canaux à pertes probabilistes

- Modélisation par des processus de décision markoviens
  - Choix non-déterministe pour les actions (lectures, écritures)
  - Distribution de probabilité pour les pertes de messages
- Un adversaire $u$ effectue les choix non-déterministes
- Étude qualitative : les questions sont de la forme $\forall u, \mathbb{P}_u(\phi) = 1$ où $\phi$ est une formule de $\mathtt{LTL} \setminus \mathtt{X}$.
- Existence d'un attracteur fini (ensemble fini de configurations visitées infiniment souvent avec probabilité $1$) : configurations avec canaux vides
- La vérification probabiliste se réduit à des questions d'accessibilité dans le graphe des configurations
- But : utiliser TReX pour résoudre des problèmes grâce à la réduction.

# Deux hypothèses pour commencer

- «idling» : Pour faciliter certaines preuves, nous faisons l'hypothèse que l'adversaire peut choisir de ne rien faire. Note : On peut coder dans la formule le fait de ne pas stationner dans un état (en utilisant l'opérateur `X`).
- propositions atomiques : Dans un premier temps les ensembles de configurations que nous manipulons sont des ensembles d'états de contrôle. En particulier, on ne peut rien dire sur le contenu des canaux. On peut tout de même coder beaucoup de choses dans les états, par exemple le passé, ceci étant coûteux (duplication des états).

Ces hypothèses permettent aussi d'utiliser TReX plus facilement.

# Un exemple

Soit $A$ un ensemble d'états de contrôle.
Question : $\forall u\ \mathbb{P}_u(\Box A) > 0$ ?
Si $B = \bar{A}$, ce problème s'exprime également ainsi : $\neg\exists u\ \mathbb{P}_u(\Diamond B) = 1$ ?

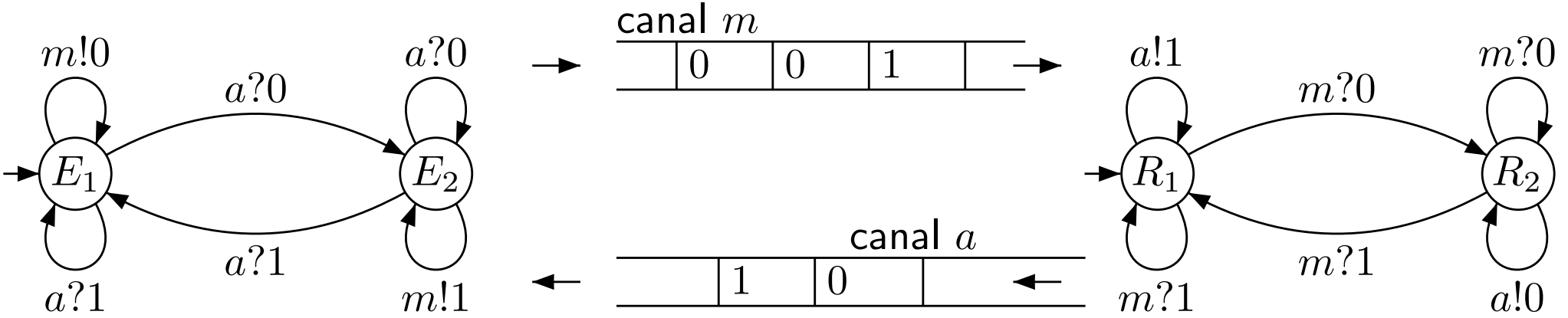
Ce problème est décidable.

$$\exists u\ \mathbb{P}_u(\Diamond B) = 1$$
ssi
$$\exists S \subset Q,\ s_0 \in Q \wedge \forall s \in S,\ \langle s, \epsilon\rangle \rightarrow_S^* B$$

- $S$ peut donc être calculé comme un plus grand point fixe, en retirant au fur et à mesure les états $s$ tels que $B$ n'est pas accessible depuis $\langle s, \epsilon\rangle$.
- Si un tel $S$ existe, comment construire $u$?

Cet exemple met en évidence qu'il est pratique de faire l'hypothèse que l'adversaire peut «ne rien faire».

# Le bit alterné




Objectif : Vérifier des propriétés de progrès pour ce modèle, à partir des nos algorithmes et avec l'aide de TReX.

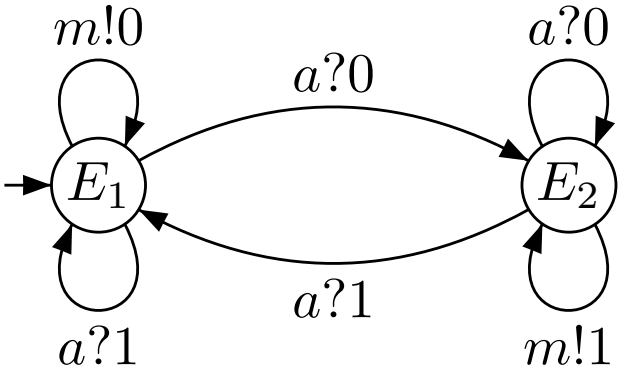
# Propriété de progrès dans le B.A.

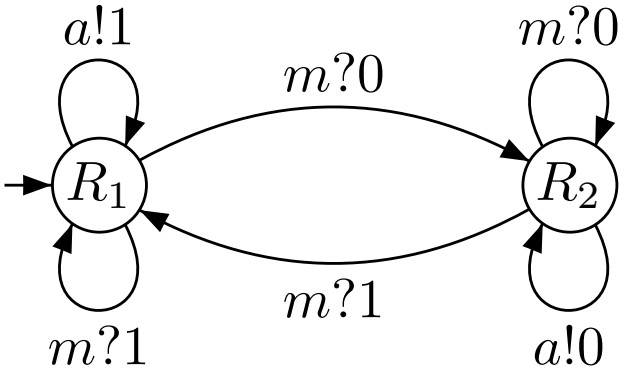
- On cherche à vérifier la propriété de progrès $\phi$ :
  $\Box\Diamond E_1 \wedge \Box\Diamond E_2 \wedge \Box\Diamond R_1 \wedge \Box\Diamond R_2$, qui traduit que la transmission a bien lieu.

# Propriété de progrès dans le B.A.

- On cherche à vérifier la propriété de progrès $\phi$ :
  $\Box\Diamond E_1 \wedge \Box\Diamond E_2 \wedge \Box\Diamond R_1 \wedge \Box\Diamond R_2$, qui traduit que la transmission a bien lieu.

Pb: Le progrès n'est pas garanti (si l'adversaire fait les «mauvais» choix).



# Propriété de progrès dans le B.A.

- On cherche à vérifier la propriété de progrès $\phi$ :
  $\Box\Diamond E_1 \wedge \Box\Diamond E_2 \wedge \Box\Diamond R_1 \wedge \Box\Diamond R_2$, qui traduit que la transmission a bien lieu.

Pb: Le progrès n'est pas garanti (si l'adversaire fait les «mauvais» choix).

- Il faut rajouter des hypothèses d'équité :
  - Équité sur les lectures
  - Équité entre les deux entités
  - Équité des pertes

Ces hypothèses sont rajoutées dans la formule à vérifier.

# Hypothèses d'équité

- Priorité des lectures sur les écritures : exemple pour l'état $E_1$
  **équité forte** $\Diamond\Box E_1 \Rightarrow \Diamond\Box\langle E_1, a = \epsilon\rangle$
  **équité faible** $\Diamond\Box E_1 \Rightarrow \Box\Diamond\langle E_1, a = \epsilon\rangle$
- Équité entre les deux entités : exemple pour l'émetteur dans l'état $E_1$
  **équité forte ou faible** $\Diamond\Box E_1 \Rightarrow \Box\Diamond\langle E_1, m \neq \epsilon\rangle \vee \Box\Diamond E_2$
- Équité des pertes : elle est garantie par les pertes probabilistes.

Les hypothèses d'équité semblent garantir un comportement correct du système (avec probabilité $1$)...
...mais elles ne sont pas exprimables uniquement avec des états de contrôle.

# Utilisation de TReX

- Comment vérifier $\exists u\ \mathbb{P}_u(\phi) = 1$ ?
  - La question est équivalente à l'existence d'un plus grand ensemble d'états de contrôle $S$ contenant l'état initial et tel que à partir de chaque état de $S$ et des canaux vides, on peut atteindre $E_1$, $E_2$, $R_1$ et $R_2$, en restant dans $S$.
- Comment utiliser TReX pour répondre à cette question?
  - Initialiser $S$ à l'ensemble de tous les états de contrôle du produit des deux composantes.
  - Calculer avec TReX le $\texttt{Post}^*$ des $\langle s, \epsilon, \epsilon \rangle$, pour tous les états de $S$ (donné par SRE).
  - Retirer les états de $S$ s'ils ne peuvent atteindre l'un de $E_1$, $E_2$, $R_1$ ou $R_2$, et considérer comme nouveau système, celui restreint aux états de $S$.
  - Revenir à l'étape de calcul de $\texttt{Post}^*$ et ce jusqu'à stabilisation de $S$.
  - L'état initial appartient-t-il au point fixe?

# Des améliorations possibles

- Pour nos algorihmes, un calcul de $\texttt{Pre}^*$ serait plus approprié que du $\texttt{Post}^*$. En effet l'intersection des $\texttt{Pre}^*(E_i)$ et de $\texttt{Pre}^*(R_i)$ donnerait directement les états capables d'atteindre les $E_i$ et les $R_i$, plutôt que de calculer le $\texttt{Post}^*$ pour tous les états du système.
- Dans le cas de systèmes à plusieurs composants, il serait utile d'avoir accès au produit dans l'étape où l'on retire des états. Pour l'instant, le produit est réalisé à la main, ce qui n'est pas envisageable pour des modèles plus gros.
- Pour exprimer les hypothèses d'équité, on est amené à faire des copies de chacune des composantes. Par exemple pour connaître le premier message d'un canal. Ces méthodes font croître le nombre d'états, en particulier le nombre d'états du produit. À tel point que TReX ne termine plus. Pourtant les calculs de $\texttt{Post}^*$ sont très ressemblant entre les différentes copies.

# De nouveaux algorithmes...

- Constats sur les hypothèses
  - Constat 1 : Les états de contrôle ne suffisent pas pour exprimer des propriétés intéressantes
  - Constat 2 : Le fait d'autoriser les adversaires à «ne rien faire» simplifie *grandement* les algorithmes.

- Les problèmes restent-ils décidables lorsqu'on s'intéresse à des ensembles de configurations plus généraux? Par exemple pour des ensembles de la forme $\bigvee_{i=1}^{n} \alpha^i \uparrow \sigma_0^i - \beta_1^i \sigma_1^i - \cdots - \beta_{k_i}^i \sigma_{k_i}^i$

- Autoriser les adversaires à «ne rien faire» n'est-il qu'une hypothèse simplificatrice?