Diagnostic et contrôle de la dégradation des systèmes probabilistes

Nathalie Bertrand[1], Serge Haddad[2], Engel Lefaucheux[1,2]

1 Inria, Rennes
2 LSV, ENS Paris-Saclay & CNRS & Inria, Saclay

MSR, 16 Novembre 2017

Motivation

Dans les systèmes embarqués, les fautes sont inévitables.

Comment y faire face en temps réel ?

Motivation

Dans les systèmes embarqués, les fautes sont inévitables.

Comment y faire face en temps réel ?

- 1ère approche : *Diagnostic*
  Intéret : préalable à la réparation

Motivation

Dans les systèmes embarqués, les fautes sont inévitables.

Comment y faire face en temps réel ?

- 1ère approche : *Diagnostic*
  Intéret : préalable à la réparation
- 2ème approche : *Contrôle de la dégradation*
  Intéret : retardement des fautes.

Motivation

Dans les systèmes embarqués, les fautes sont inévitables.

Comment y faire face en temps réel ?

- 1ère approche : *Diagnostic*
  Intéret : préalable à la réparation
- 2ème approche : *Contrôle de la dégradation*
  Intéret : retardement des fautes.

Comment combiner les deux approches ?

Plan

Formalisation

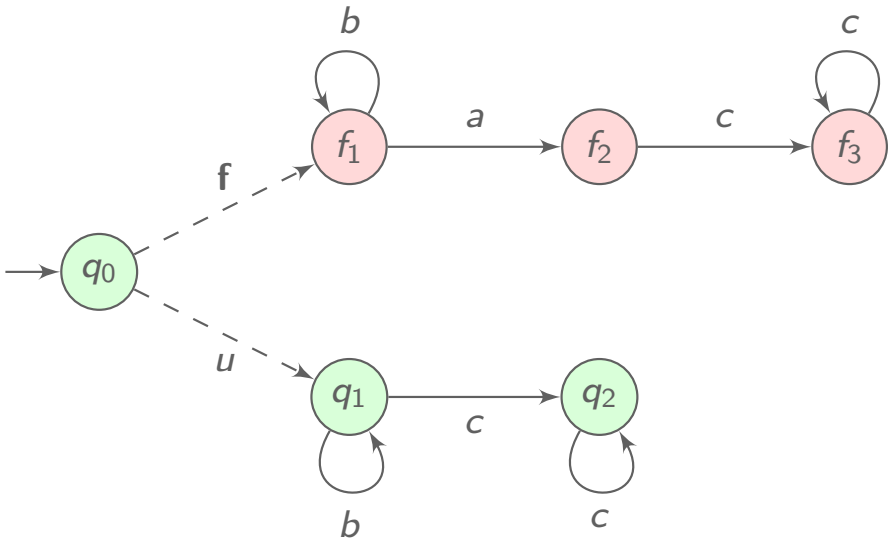
Analyse sémantique

Analyse algorithmique

Outline

Cadre du diagnostic [SSLST95]

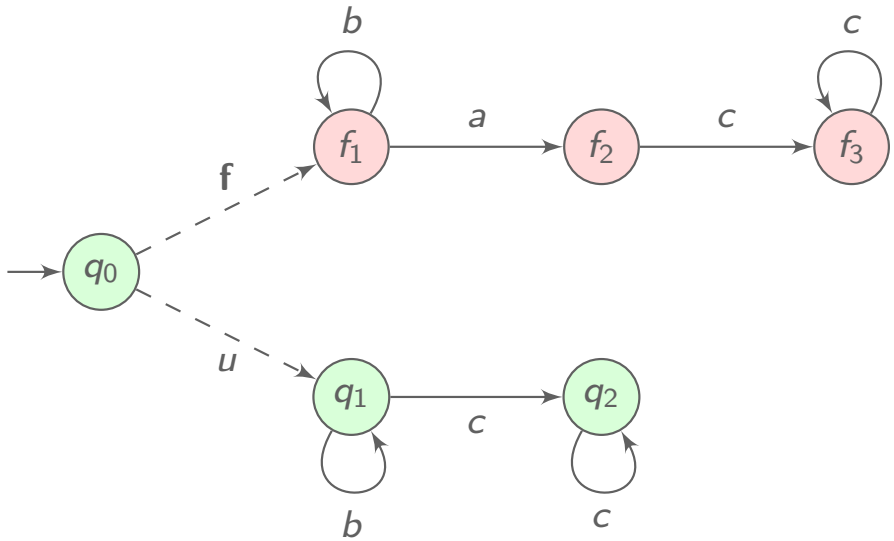
Système de Transition Étiqueté convergent.



Objectif : utiliser les observations pour indiquer si une faute **f** a eu lieu.

Cadre du diagnostic [SSLST95]

Système de Transition Étiqueté convergent.



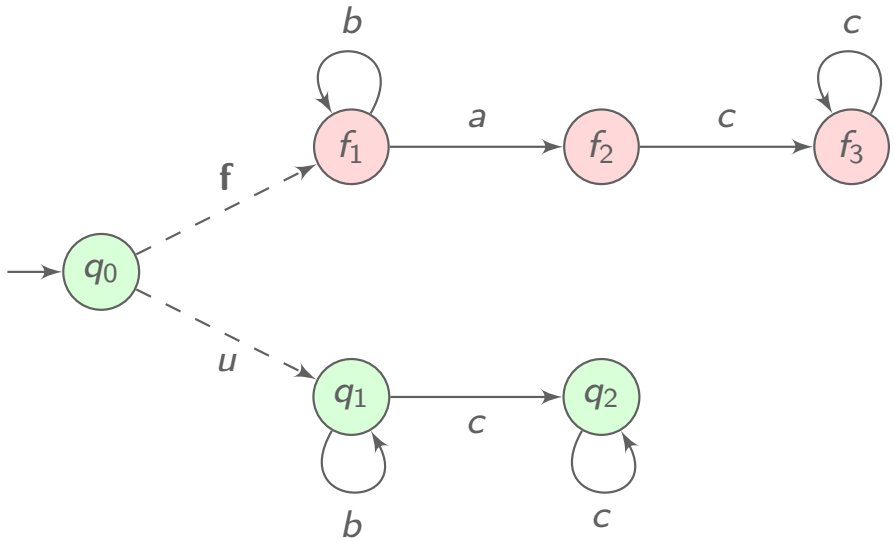
Objectif : utiliser les observations pour indiquer si une faute **f** a eu lieu.

L'*exécution* $\rho = q_0 \xrightarrow{u} q_1 \xrightarrow{c} q_2$ a pour *séquence d'observation* $\mathcal{P}(\rho) = c$.

Cadre du diagnostic

[SSLST95]

Système de Transition Étiqueté convergent.



Objectif : utiliser les observations pour indiquer si une faute **f** a eu lieu.

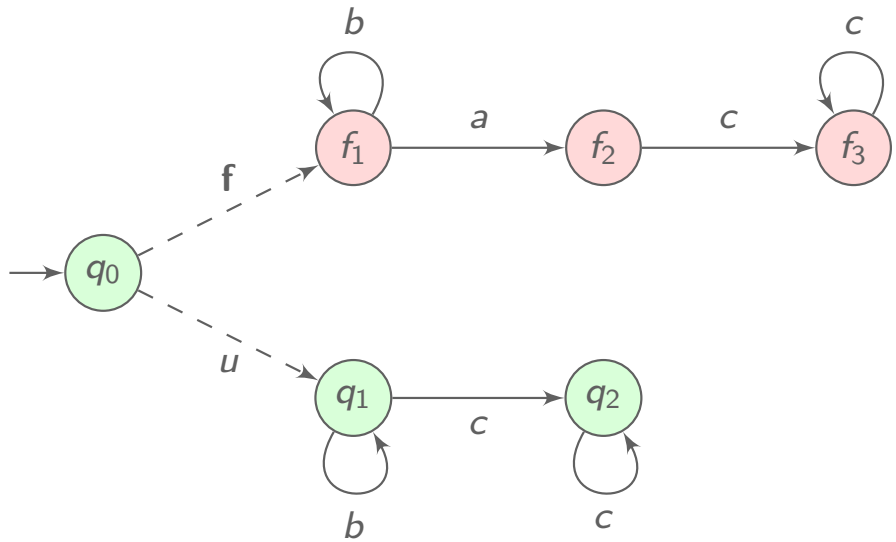
L'*exécution* $\rho = q_0 \xrightarrow{u} q_1 \xrightarrow{c} q_2$ a pour *séquence d'observation* $\mathcal{P}(\rho) = c$.

✗ ac est *surement fautive* car $\mathcal{P}^{-1}(ac) = \{q_0 \xrightarrow{\mathbf{f}} f_1 \xrightarrow{a} f_2 \xrightarrow{c} f_3\}$.

Cadre du diagnostic

[SSLST95]

Système de Transition Étiqueté convergent.



Objectif : utiliser les observations pour indiquer si une faute **f** a eu lieu.

L'*exécution* $\rho = q_0 \xrightarrow{u} q_1 \xrightarrow{c} q_2$ a pour *séquence d'observation* $\mathcal{P}(\rho) = c$.

✗ ac est *surement fautive* car $\mathcal{P}^{-1}(ac) = \{q_0 \xrightarrow{\mathbf{f}} f_1 \xrightarrow{a} f_2 \xrightarrow{c} f_3\}$.

? b est *ambiguë* car $\mathcal{P}^{-1}(b) = \{q_0 \xrightarrow{\mathbf{f}} f_1 \xrightarrow{b} f_1, q_0 \xrightarrow{u} q_1 \xrightarrow{b} q_1\}$.

[SSLST95] Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis. *Diagnosability of discrete-event systems*. TAC, 1995.

Diagnostiquabilité et synthèse de diagnostiqueur

Diagnostiquabilité

Toute exécution fautive infinie a une séquence d'observation surement fautive.

Diagnostiquabilité et synthèse de diagnostiqueur

Diagnostiquabilité

Toute exécution fautive infinie a une séquence d'observation surement fautive.

La diagnostiquabilité est NLOGSPACE-complète.

Diagnostiqueur

Assigne un verdict aux séquences d'observation $D : \Sigma_o^* \to \{✗, ?\}$

Propriétés du diagnostiqueur

- **Exactitude** : si une faute est déclarée, ✗, une faute a eu lieu.
- **Réactivité** : toute faute est détectée.

Diagnostiquabilité et synthèse de diagnostiqueur

Diagnostiquabilité

Toute exécution fautive infinie a une séquence d'observation surement fautive.

La diagnostiquabilité est NLOGSPACE-complète.

Diagnostiqueur

Assigne un verdict aux séquences d'observation $D : \Sigma_o^* \to \{✗, ?\}$

Propriétés du diagnostiqueur

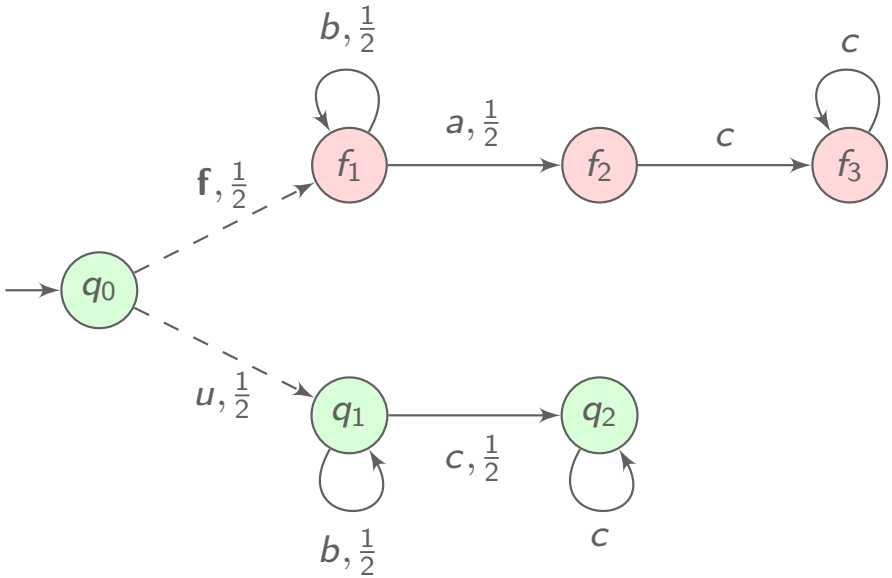
- **Exactitude** : si une faute est déclarée, ✗, une faute a eu lieu.
- **Réactivité** : toute faute est détectée.

La synthèse du diagnostiqueur est réalisable en EXPTIME.

Probabilités et diagnostic

[TT05]

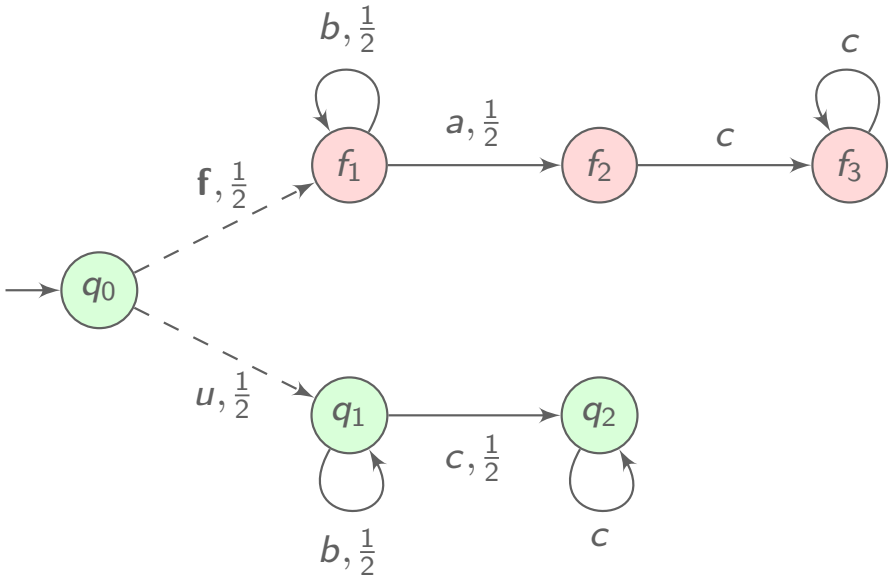
Imprédictabilité de l'environnement, d'où choix probabiliste.
Système Probabiliste de Transition Étiqueté (SPTE).



Probabilités et diagnostic

[TT05]

Imprédictabilité de l'environnement, d'où choix probabiliste.
Système Probabiliste de Transition Étiqueté (SPTE).

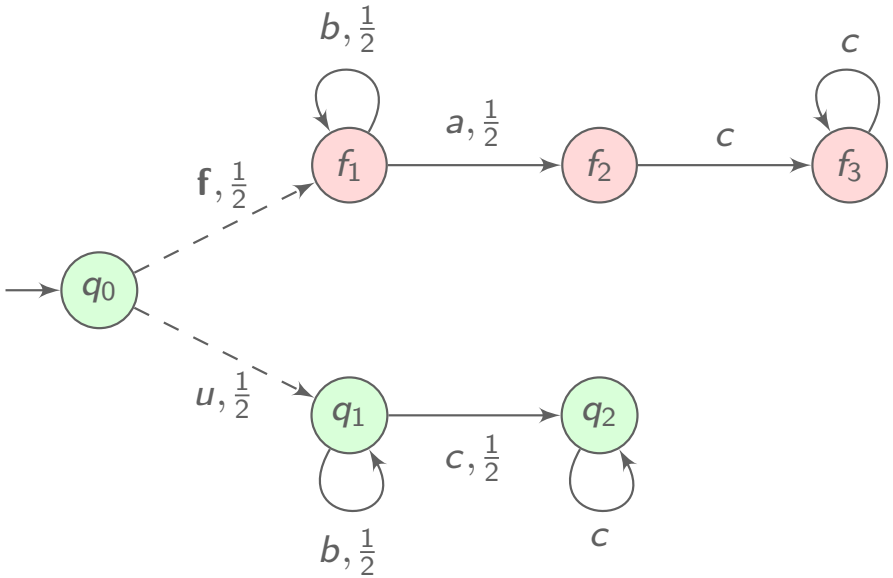


b^n ambiguë mais...

Probabilités et diagnostic

[TT05]

Imprédictabilité de l'environnement, d'où choix probabiliste.
Système Probabiliste de Transition Étiqueté (SPTE).



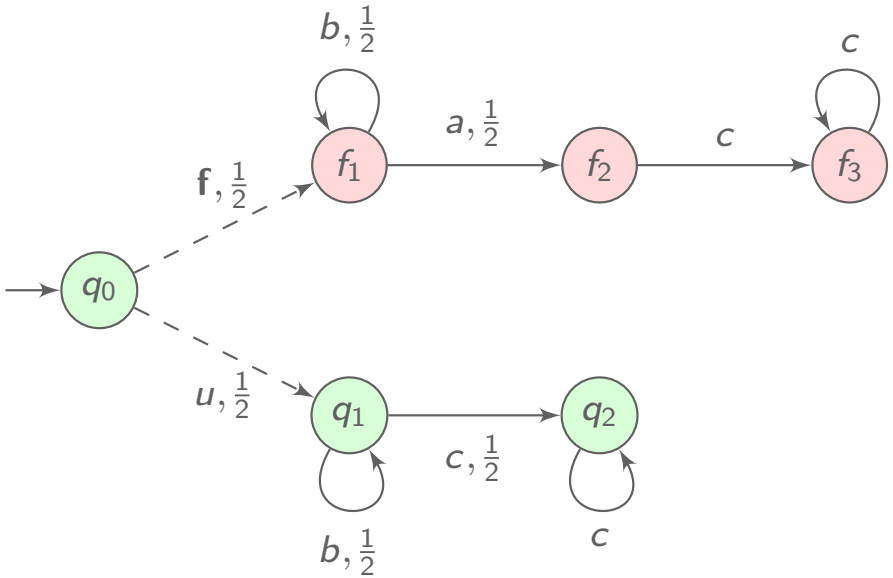
b^n ambiguë mais...

$$\lim_{n \to \infty} \mathbb{P}(\mathbf{f} b^n) = 0$$

Probabilités et diagnostic

[TT05]

Imprédictabilité de l'environnement, d'où choix probabiliste.
Système Probabiliste de Transition Étiqueté (SPTE).



b^n ambiguë mais...

$$\lim_{n\to\infty} \mathbb{P}(\mathbf{f}b^n) = 0$$

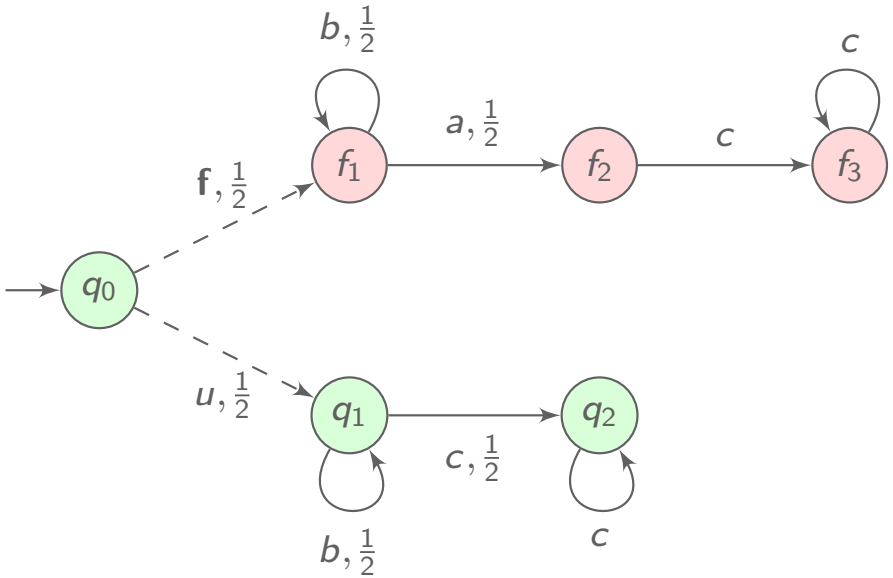
Diagnostiquabilité

La probabilité des exécutions ayant une observation infinie ambiguë est nulle.

Probabilités et diagnostic

[TT05]

Imprédictabilité de l'environnement, d'où choix probabiliste.
Système Probabiliste de Transition Étiqueté (SPTE).



b^n ambiguë mais...

$$\lim_{n\to\infty} \mathbb{P}(\mathbf{f}b^n) = 0$$

Diagnostiquabilité

La probabilité des exécutions ayant une observation infinie ambiguë est nulle.

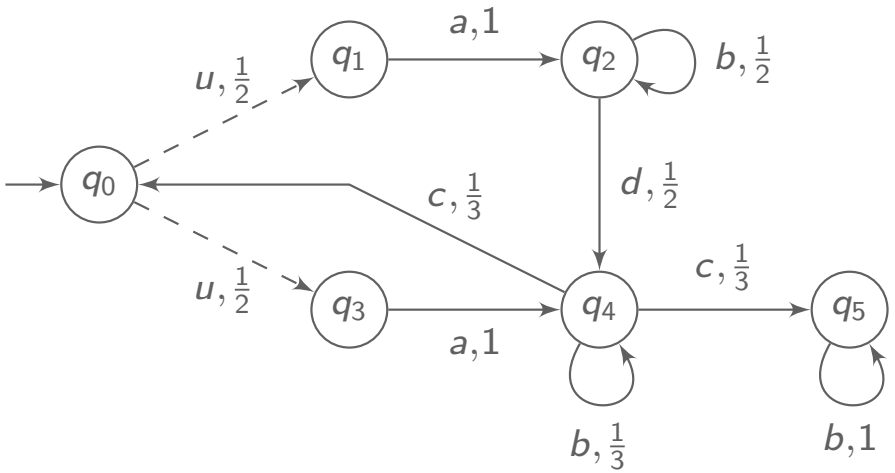
La diagnostiquabilité est PSPACE-complète pour les SPTE. [BHL14]

[TT05] Thorsley and Teneketzis, *Diagnosability of stochastic discrete-event systems*, TAC, 2005.
[BHL14] Bertrand, Haddad and Lefaucheux, *Foundation of diagnosis and predictability in probabilistic systems*, FSTTCS'14.

Contrôle des SPTE

Contrôleur

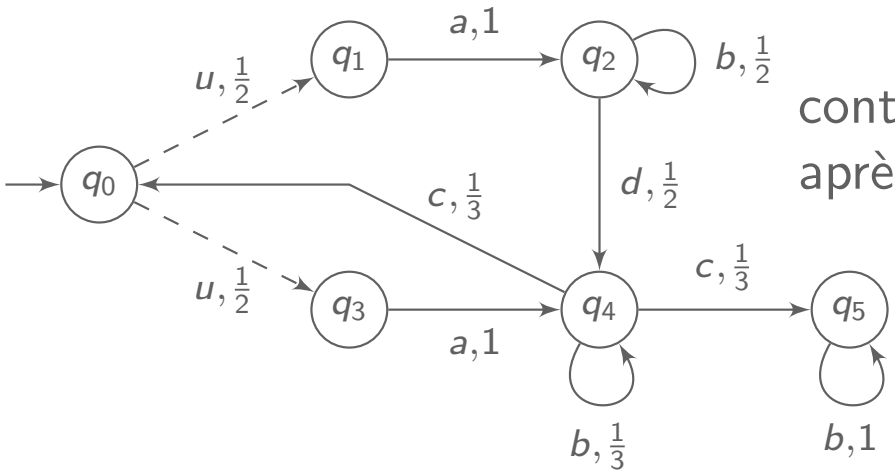
Utilise les observations pour choisir les actions autorisées.



Contrôle des SPTE

Contrôleur

Utilise les observations pour choisir les actions autorisées.

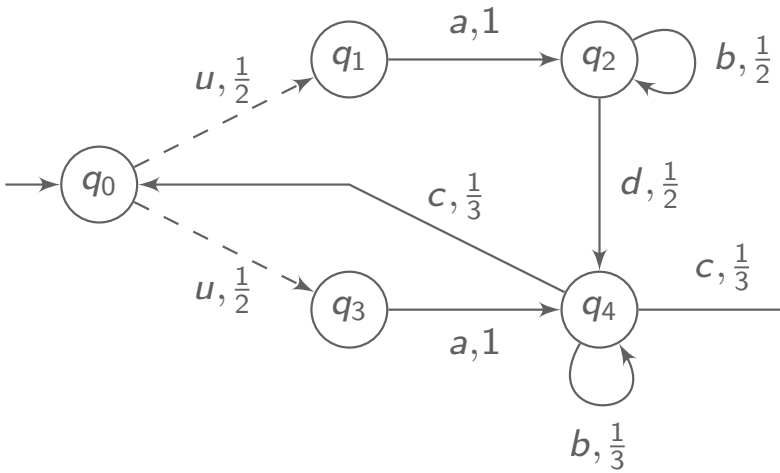


contrôleur : interdit deux b consécutifs après un a.

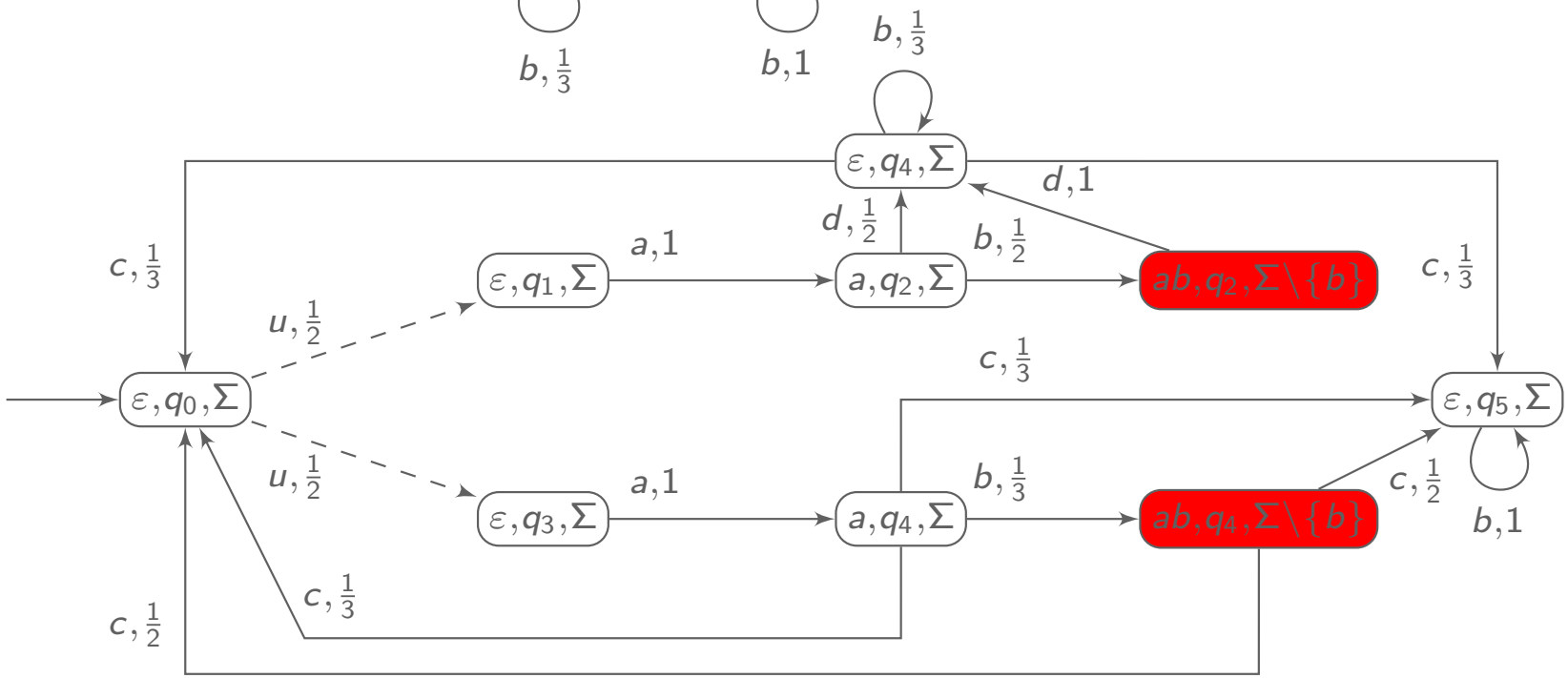
Contrôle des SPTE

Contrôleur

Utilise les observations pour choisir les actions autorisées.

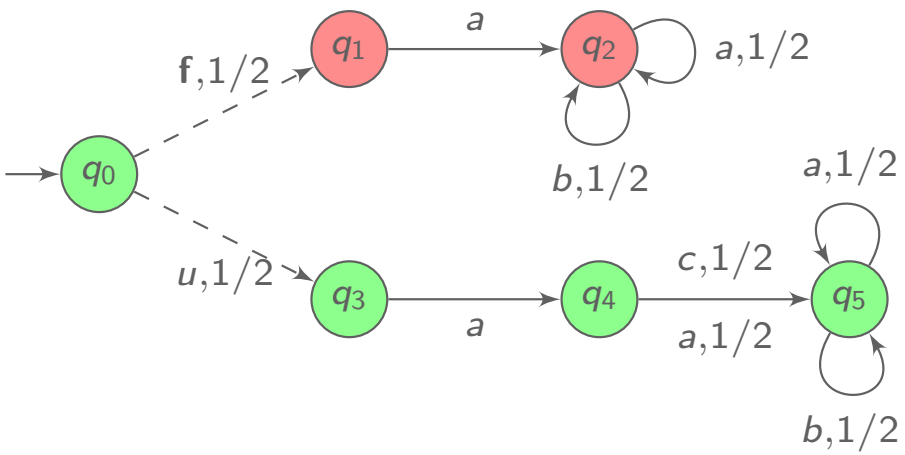


contrôleur : interdit deux b consécutifs après un a.



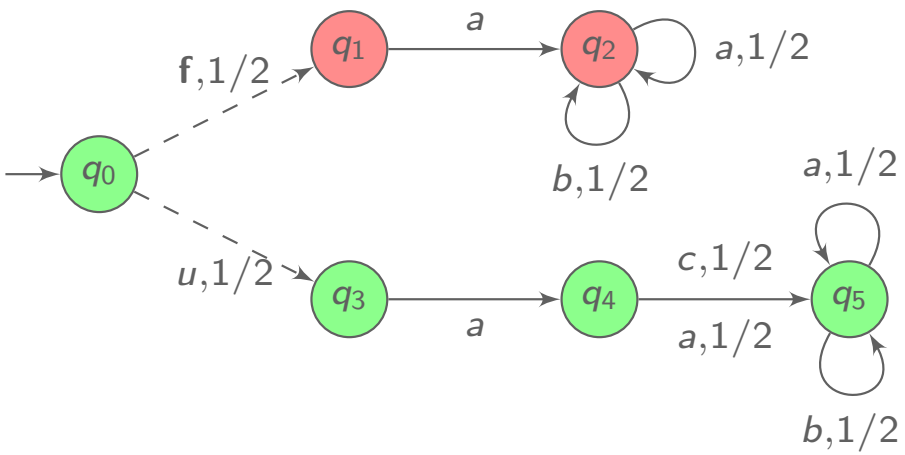
Diagnostic actif des systèmes probabilistes

Objectif : contrôler le système pour le rendre diagnostiquable.



Diagnostic actif des systèmes probabilistes

Objectif : contrôler le système pour le rendre diagnostiquable.

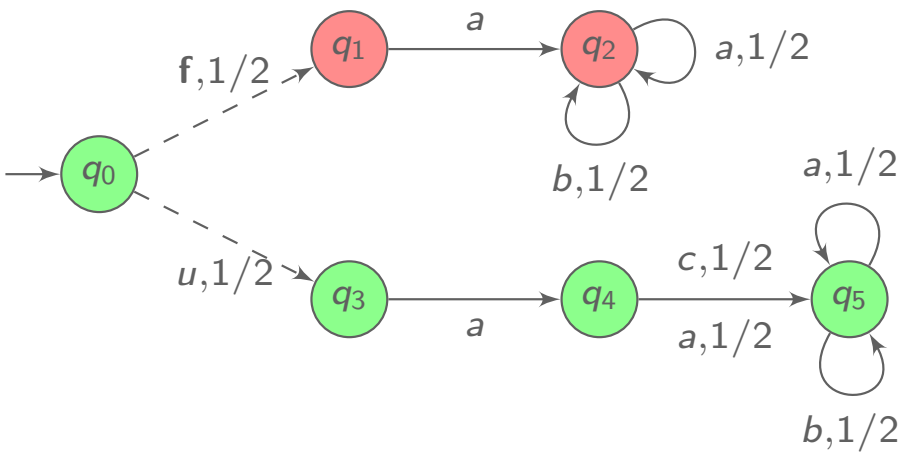


Toute séquence d'observation débutant par aa est ambigüe

$\mathbb{P}(\mathbf{f}aa(a+b)^{\omega}) > 0$

Diagnostic actif des systèmes probabilistes

Objectif : contrôler le système pour le rendre diagnostiquable.



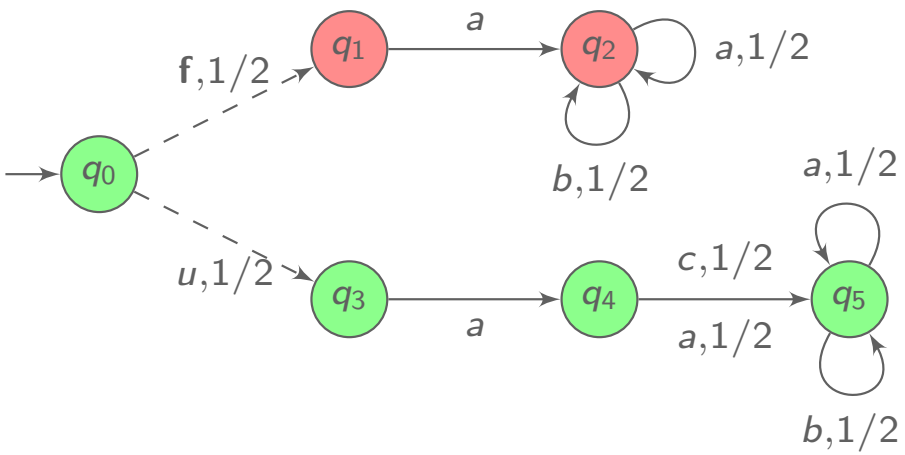
Toute séquence d'observation débutant par aa est ambigüe

$\mathbb{P}(\mathbf{f}aa(a+b)^{\omega}) > 0$

$\{a, b, c\}$ contrôlable

Diagnostic actif des systèmes probabilistes

Objectif : contrôler le système pour le rendre diagnostiquable.



Toute séquence d'observation débutant par aa est ambigüe

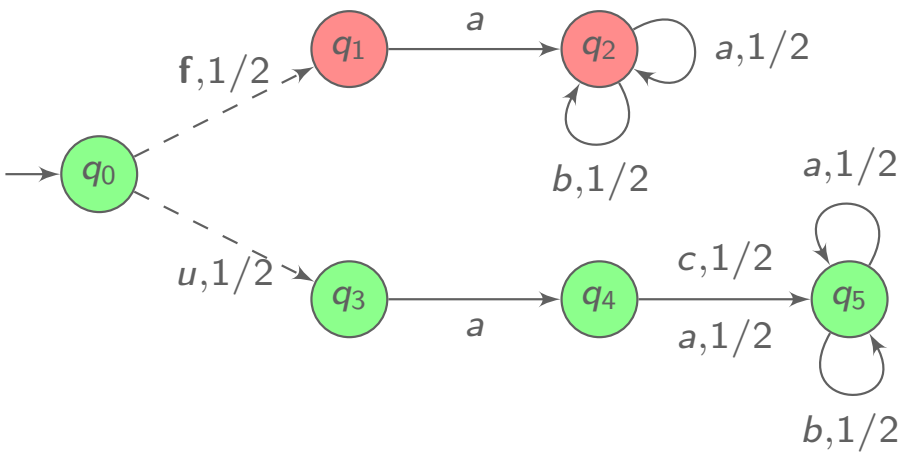
$\mathbb{P}(\mathbf{f}aa(a+b)^{\omega}) > 0$

$\{a, b, c\}$ contrôlable

Un contrôle adéquat : bloquer le second a

Diagnostic actif des systèmes probabilistes

Objectif : contrôler le système pour le rendre diagnostiquable.



Toute séquence d'observation débutant par aa est ambigüe

$\mathbb{P}(\mathbf{f}aa(a+b)^\omega) > 0$

$\{a, b, c\}$ contrôlable

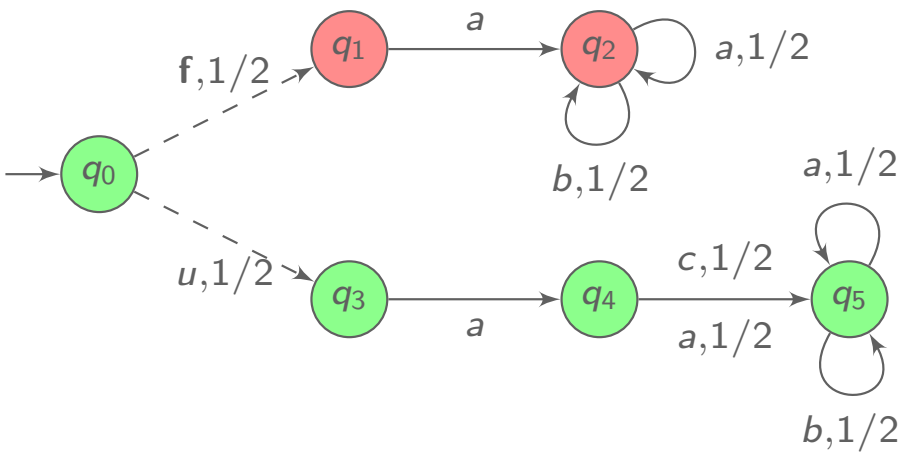
Un contrôle adéquat : bloquer le second a

Problème du diagnostic actif probabiliste [BFHHH14]

Existe-t-il un contrôleur tel que le système devienne diagnostiquable ?

Diagnostic actif des systèmes probabilistes

Objectif : contrôler le système pour le rendre diagnostiquable.



Toute séquence d'observation débutant par aa est ambigüe

$\mathbb{P}(\mathbf{f}aa(a+b)^\omega) > 0$

$\{a, b, c\}$ contrôlable

Un contrôle adéquat : bloquer le second a

Problème du diagnostic actif probabiliste [BFHHH14]

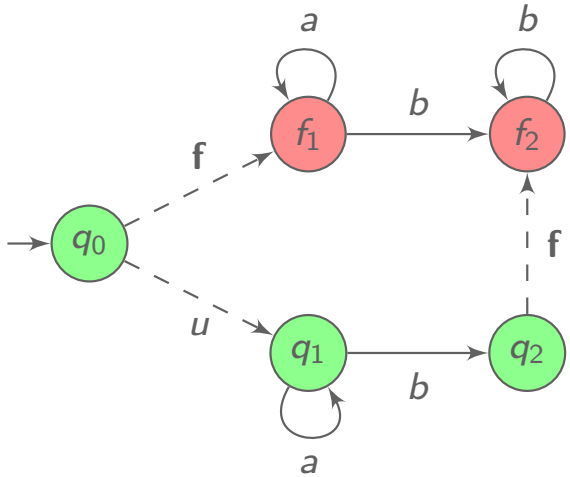
Existe-t-il un contrôleur tel que le système devienne diagnostiquable ?

Le problème du diagnostic actif probabiliste est EXPTIME-complet.

[BFHHH14] Bertrand, Fabre, Haar, Haddad and Hélouët, *Active diagnosis for probabilistic systems*, FoSSaCS'14.

Contrôle de la vitesse de dégradation du système

Objectif: empêcher une décroissance trop rapide de la probabilité des exécutions correctes $\mathbb{P}(C_n)$.



interdire b : non diagnostiquable

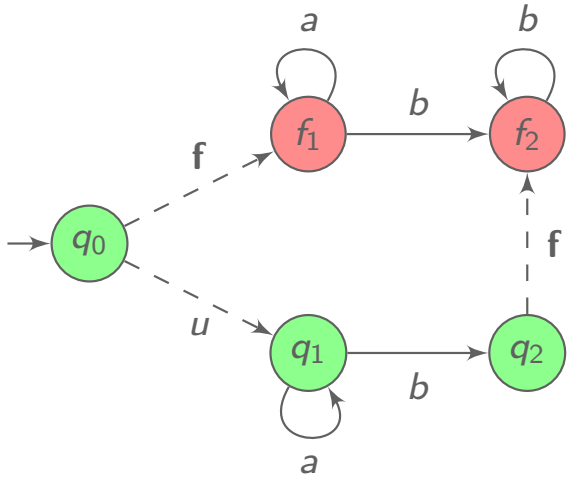
interdire a : diagnostiquable mais $\mathbb{P}(C_2) = 0$

autoriser $\{a\}$ avec probabilité p
et $\{b\}$ avec probabilité $1 - p$:
diagnostiquable, et $\mathbb{P}(C_n) = \frac{p^n}{2}$

Contrôle de la vitesse de dégradation du système

Objectif: empêcher une décroissance trop rapide de la probabilité des exécutions correctes $\mathbb{P}(C_n)$.

diagnostic ε-sûr : l'ensemble des exécutions infinies correctes a une probabilité supérieure à ε : $\lim_{n\to\infty} \mathbb{P}(C_n) > \varepsilon$.



interdire b : non diagnostiquable

interdire a : diagnostiquable mais $\mathbb{P}(C_2) = 0$

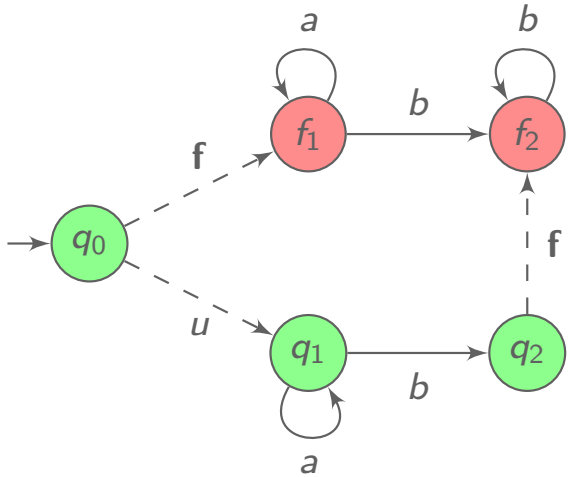
autoriser $\{a\}$ avec probabilité p
et $\{b\}$ avec probabilité $1-p$:
diagnostiquable, et $\mathbb{P}(C_n) = \frac{p^n}{2}$

Contrôle de la vitesse de dégradation du système

Objectif: empêcher une décroissance trop rapide de la probabilité des exécutions correctes $\mathbb{P}(C_n)$.

diagnostic ε-sûr : l'ensemble des exécutions infinies correctes a une probabilité supérieure à ε : $\lim_{n\to\infty} \mathbb{P}(C_n) > \varepsilon$.

α-résistance : l'ensemble des exécutions finies correctes décroit plus lentement que α : $\lim_{n\to\infty} \frac{\alpha^n}{\mathbb{P}(C_n)} = 0$.



interdire b : non diagnostiquable
interdire a : diagnostiquable mais $\mathbb{P}(C_2) = 0$

autoriser $\{a\}$ avec probabilité p
et $\{b\}$ avec probabilité $1-p$:
diagnostiquable, et $\mathbb{P}(C_n) = \frac{p^n}{2}$

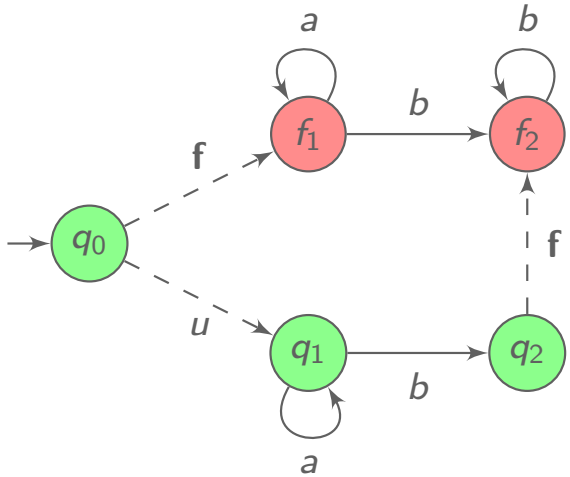
Contrôle de la vitesse de dégradation du système

Objectif: empêcher une décroissance trop rapide de la probabilité des exécutions correctes $\mathbb{P}(C_n)$.

diagnostic ε-sûr : l'ensemble des exécutions infinies correctes a une probabilité supérieure à ε : $\lim_{n\to\infty} \mathbb{P}(C_n) > \varepsilon$.

α-résistance : l'ensemble des exécutions finies correctes décroit plus lentement que α : $\lim_{n\to\infty} \frac{\alpha^n}{\mathbb{P}(C_n)} = 0$.

(γ, v)-correction : l'espérance avec décote γ de la longueur des exécutions correctes est supérieure à v : $\sum_{n\geq 1} \mathbb{P}(C_n)\gamma^n \geq v$.



interdire b : non diagnostiquable

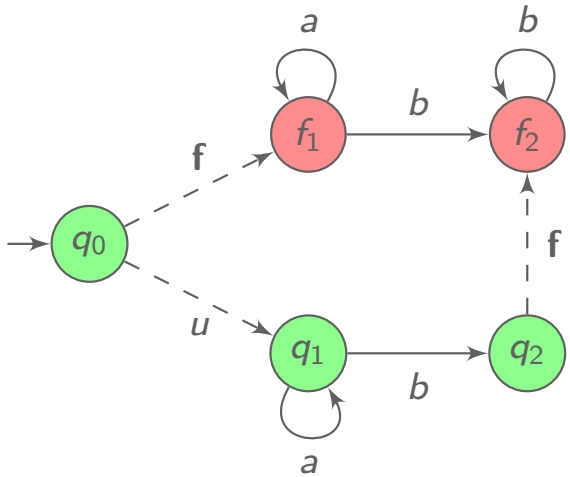
interdire a : diagnostiquable mais $\mathbb{P}(C_2) = 0$

autoriser $\{a\}$ avec probabilité p et $\{b\}$ avec probabilité $1-p$: diagnostiquable, et $\mathbb{P}(C_n) = \frac{p^n}{2}$

Versions qualitatives du contrôle de la dégradation

diagnostic sûr

Un SPTE est surement diagnostiquable ssi il est 0-sûr.



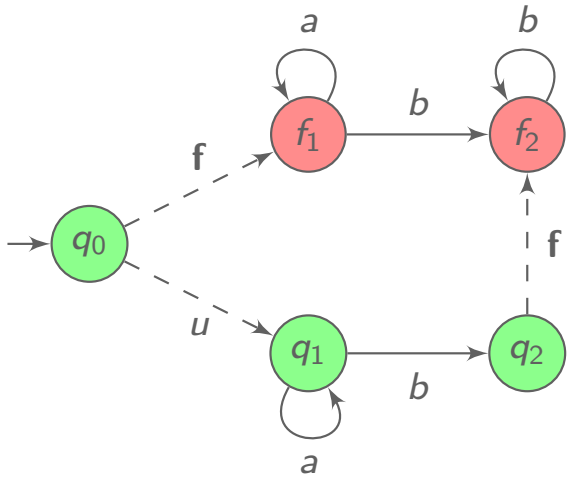
Versions qualitatives du contrôle de la dégradation

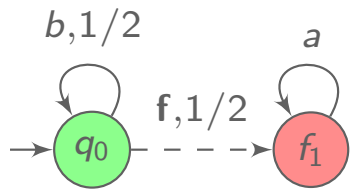
diagnostic sûr

Un SPTE est surement diagnostiquable ssi il est 0-sûr.

Faible-résistance

Un SPTE est faiblement résistant ssi $\exists \alpha > 0$ tel qu'il est α-résistant.





$$\mathbb{P}(C_n) = \frac{1}{2^n}$$

Versions qualitatives du contrôle de la dégradation

diagnostic sûr

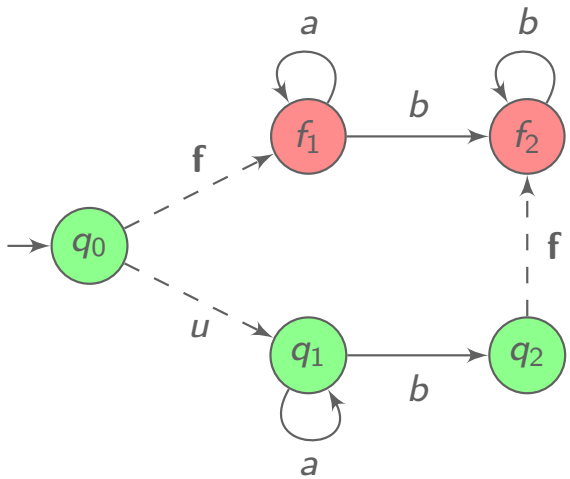
Un SPTE est surement diagnostiquable ssi il est 0-sûr.

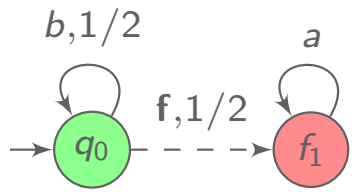
Faible-résistance

Un SPTE est faiblement résistant ssi $\exists \alpha > 0$ tel qu'il est α-résistant.

Forte-résistance

Un SPTE est fortement résistant ssi $\forall \alpha > 0$ il est α-résistant.





$$\mathbb{P}(C_n) = \frac{1}{2^n}$$

Versions qualitatives du contrôle de la dégradation

diagnostic sûr

Un SPTE est surement diagnostiquable ssi il est 0-sûr.

Faible-résistance

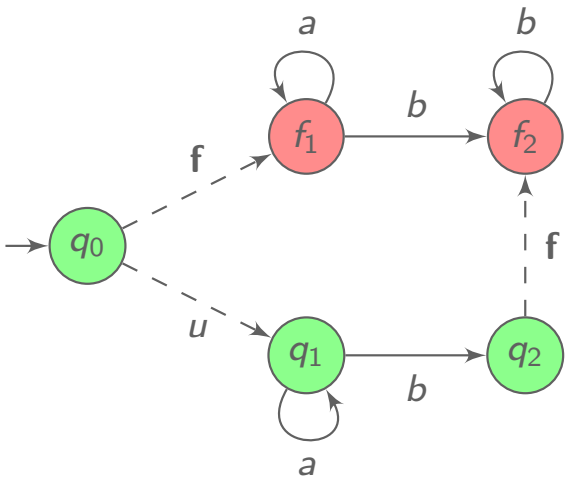
Un SPTE est faiblement résistant ssi $\exists \alpha > 0$ tel qu'il est α-résistant.

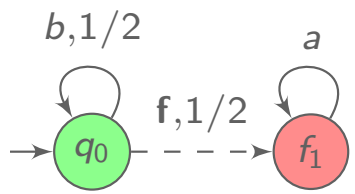
Forte-résistance

Un SPTE est fortement résistant ssi $\forall \alpha > 0$ il est α-résistant.

Longue-correction

Un SPTE est longtemps correct ssi il est $(1, \infty)$-correct.

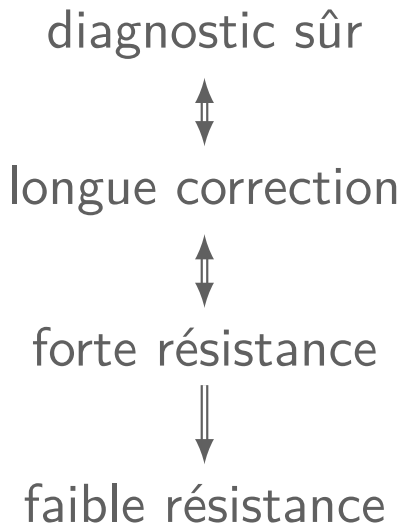




$$\mathbb{P}(C_n) = \frac{1}{2^n}$$

Outline

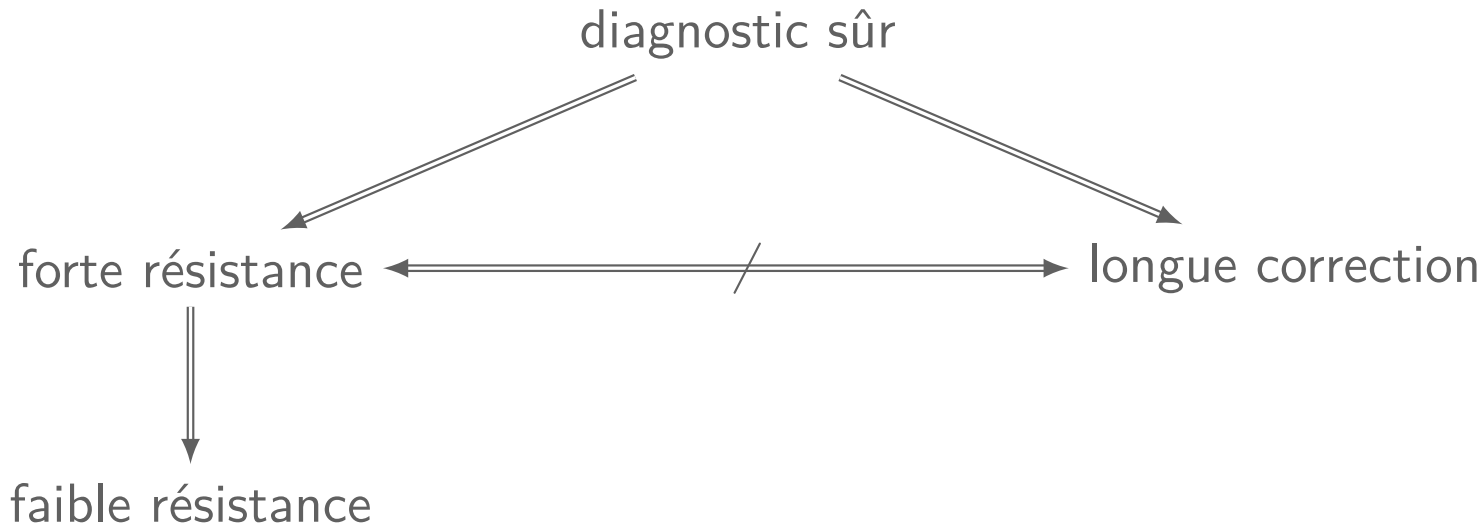
Liens entre les notions pour un SPTE fini



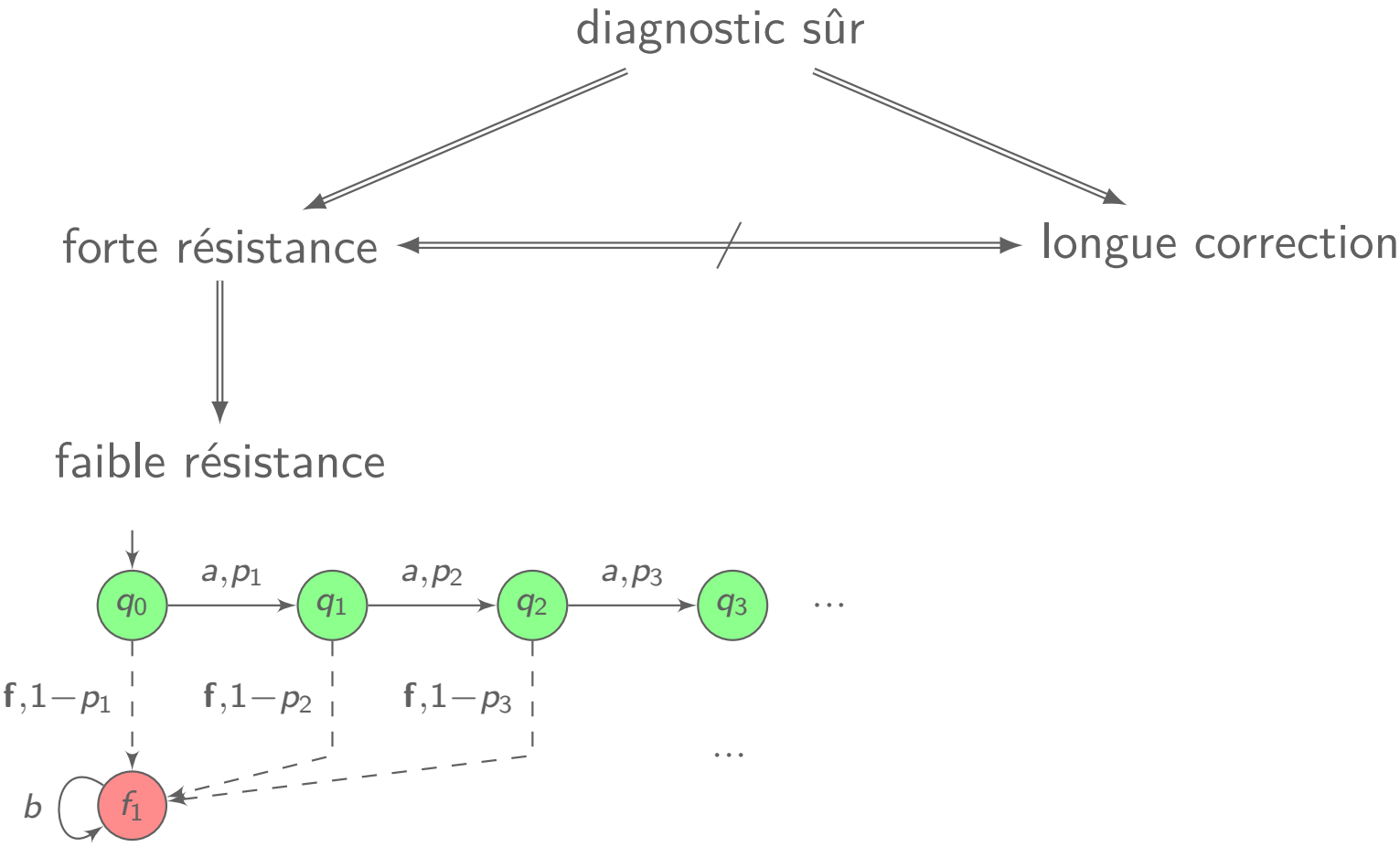
Un SPTE fini est surement diagnostiquable ssi

- il est diagnostiquable
- il possède une composante fortement connexe finale correcte.

Liens entre les notions pour un SPTE infini sans contrôle

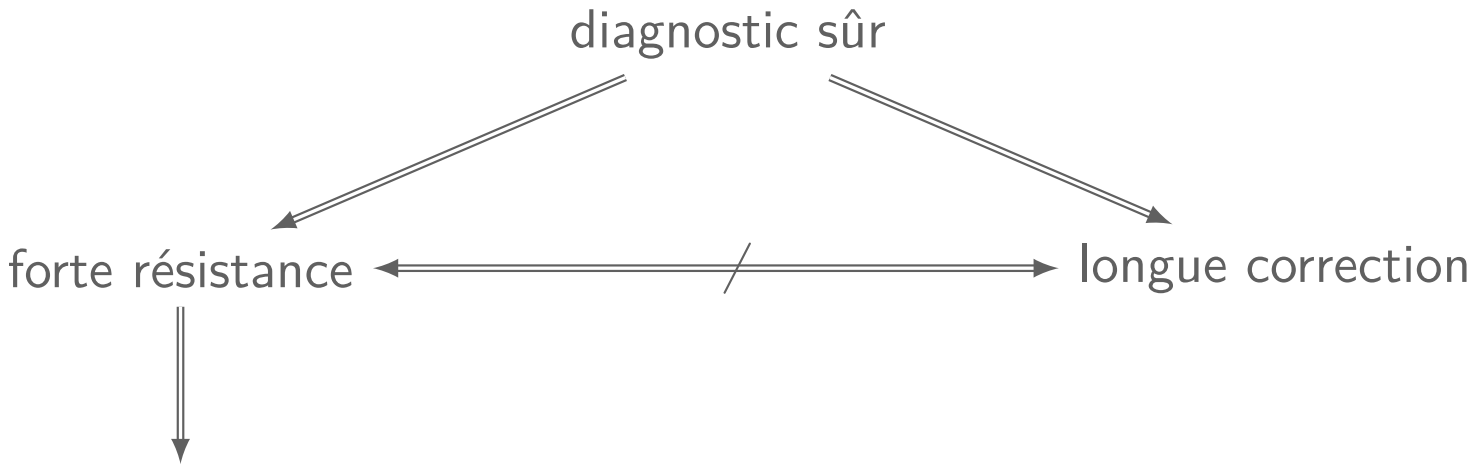


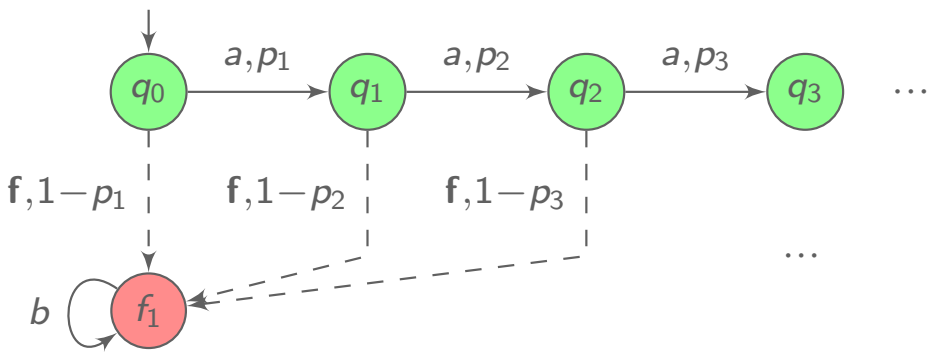
Liens entre les notions pour un SPTE infini sans contrôle



un SPTE paramétré établissant les non-équivalences

Liens entre les notions pour un SPTE infini sans contrôle

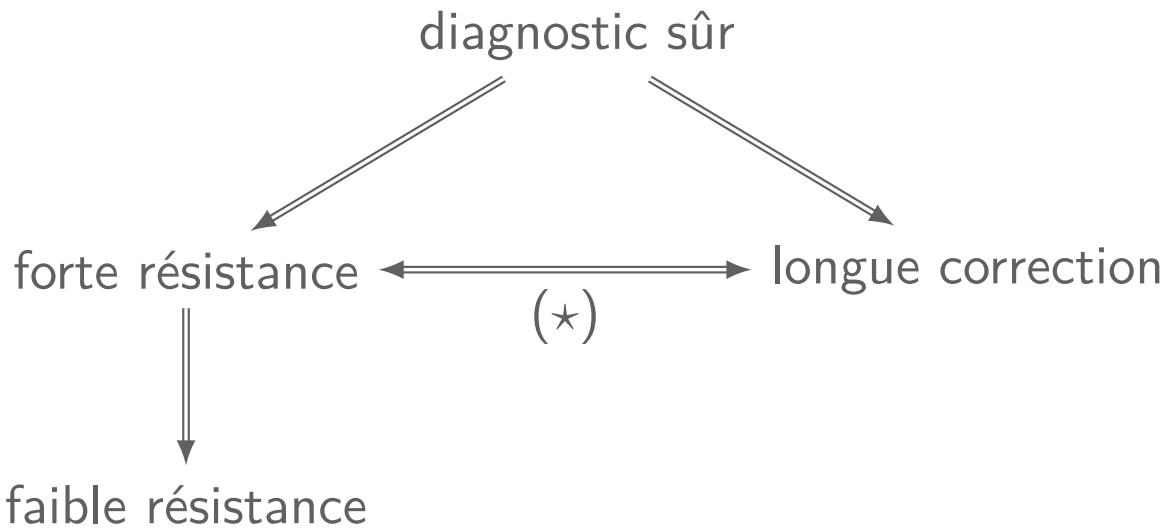




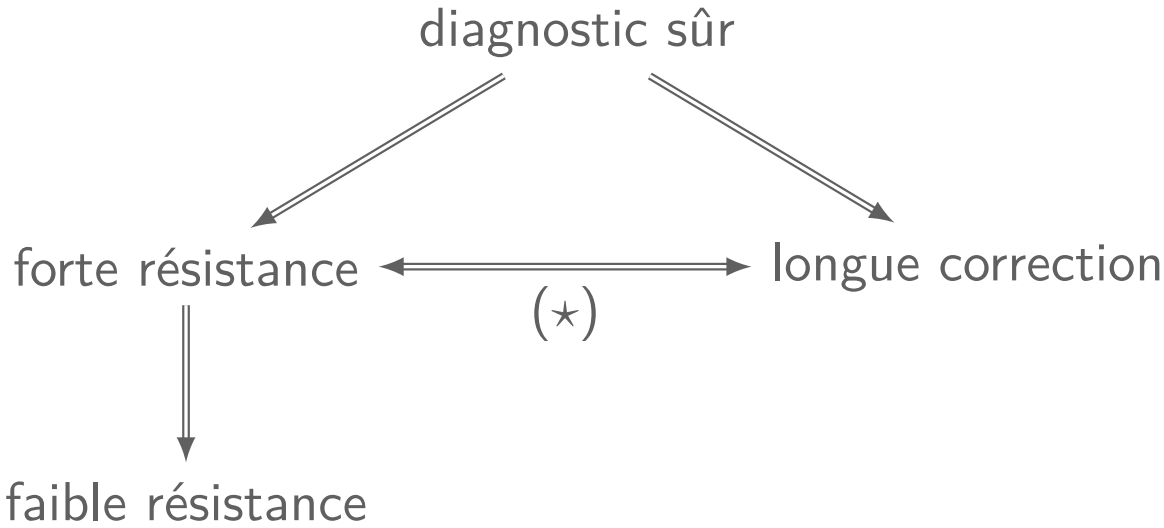
Diagnostic sûr ssi $\prod_{n \in \mathbb{N}} p_i > 0$

un SPTE paramétré établissant les non-équivalences

Liens entre les notions pour un SPTE fini avec contrôle



Liens entre les notions pour un SPTE fini avec contrôle



Observations :

- Aucun des schémas n'est identique,
- l'équivalence $(\star)$ s'établit grâce à l'analyse algorithmique.

Outline

Indécidabilité des objectifs quantitatifs

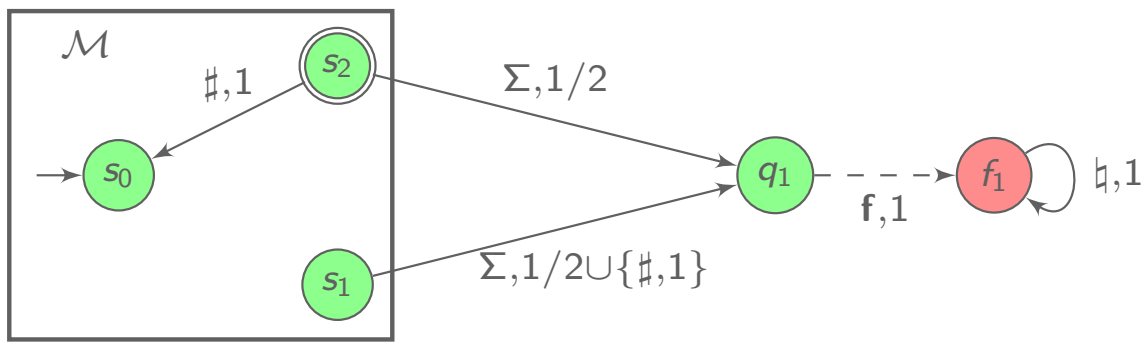
Pour $0 < \varepsilon < 1$, le problème du diagnostic ε-sûr est indécidable.

Indécidabilité des objectifs quantitatifs

Pour $0 < \varepsilon < 1$, le problème du diagnostic ε-sûr est indécidable.

Pour $0 < \alpha < 1$, le problème de l'α-résistance est indécidable.

Réduction du problème du vide des automates probabilistes.

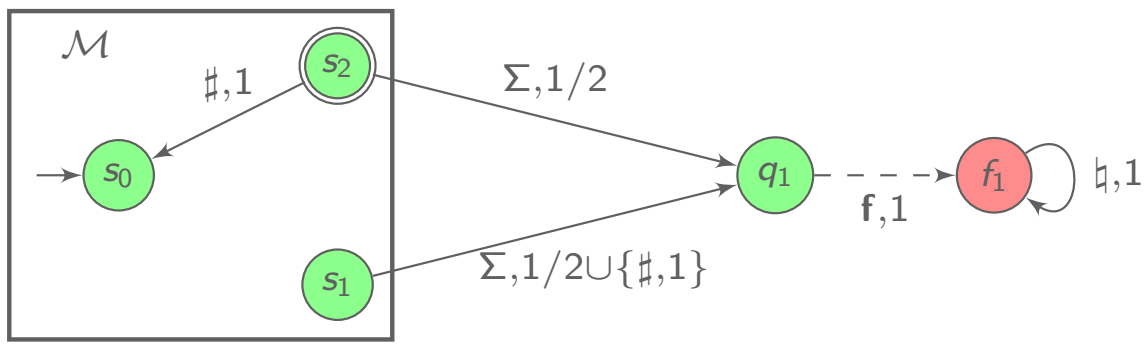


Indécidabilité des objectifs quantitatifs

Pour $0 < \varepsilon < 1$, le problème du diagnostic ε-sûr est indécidable.

Pour $0 < \alpha < 1$, le problème de l'α-résistance est indécidable.

Réduction du problème du vide des automates probabilistes.



Pour $0 < \gamma \leq 1$, $v \in]0, \infty[$,
le problème de la (γ, v)-correction est indécidable.

Et pour les objectifs qualitatifs ?

Le problème du diagnostic sûr est indécidable. [BFHHH14]

[BFHHH14] Bertrand, Fabre, Haar, Haddad and Hélouët, *Active diagnosis for probabilistic systems*, FoSSaCS'14.

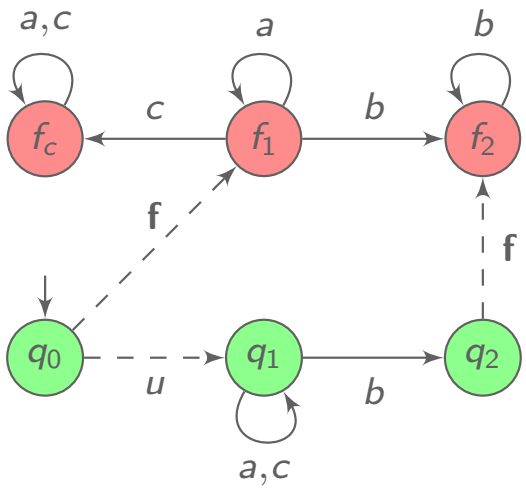
Et pour les objectifs qualitatifs ?

Le problème du diagnostic sûr est indécidable. [BFHHH14]

Les problèmes de la faible résistance, de la forte résistance et de la longue correction sont EXPTIME-complets.

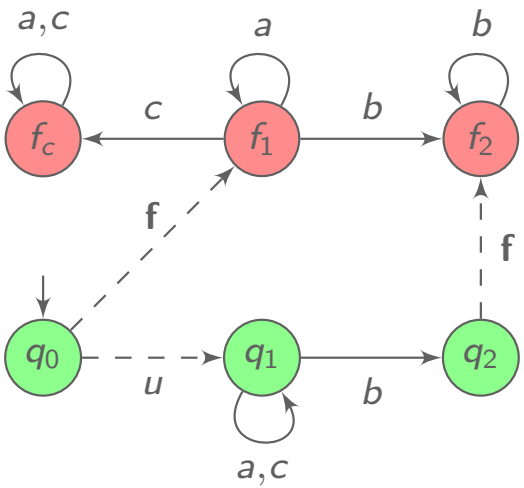
[BFHHH14] Bertrand, Fabre, Haar, Haddad and Hélouët, *Active diagnosis for probabilistic systems*, FoSSaCS'14.

Faible résistance : idée de la preuve (1)

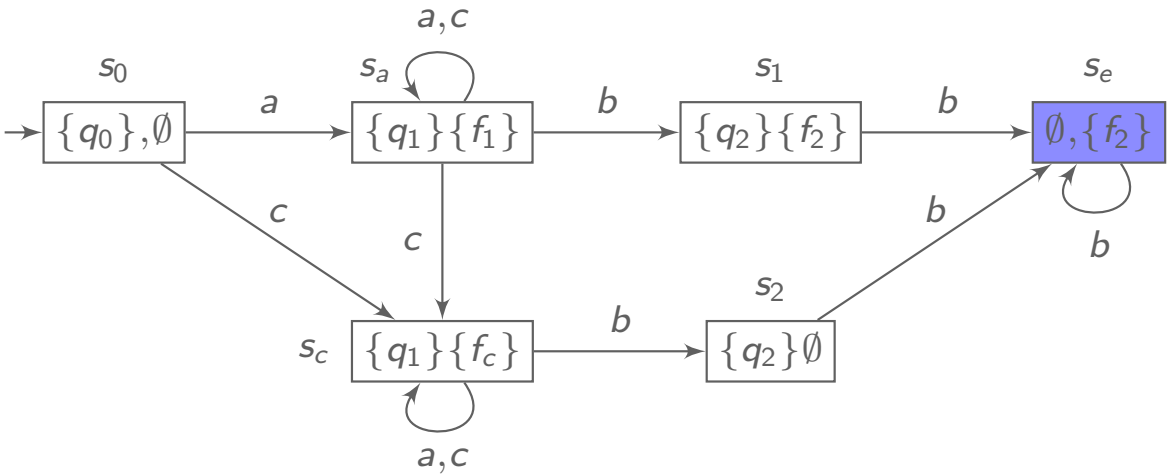


SPTE

Faible résistance : idée de la preuve (1)

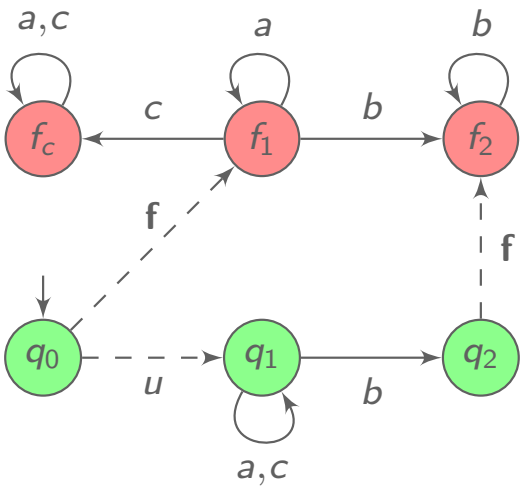


SPTE

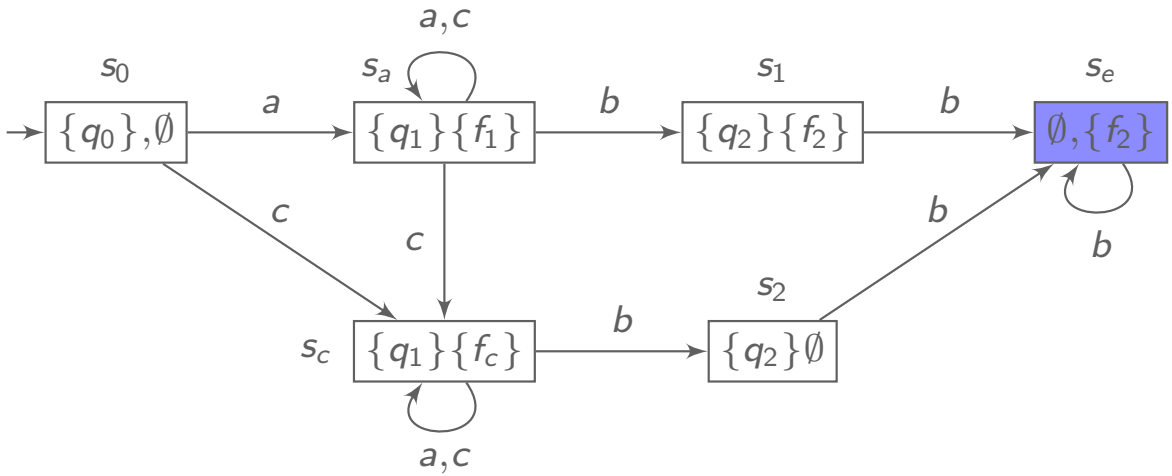


automate des croyances

Faible résistance : idée de la preuve (1)



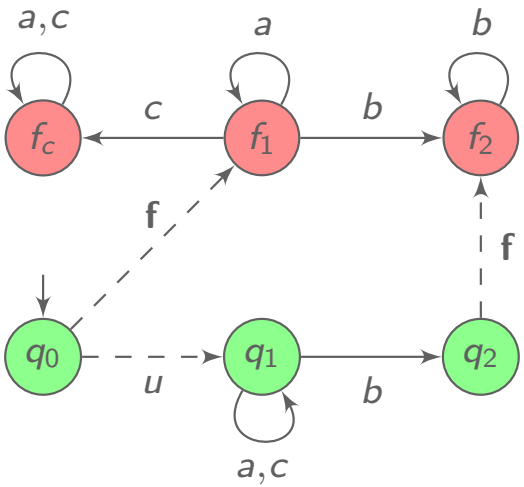
SPTE



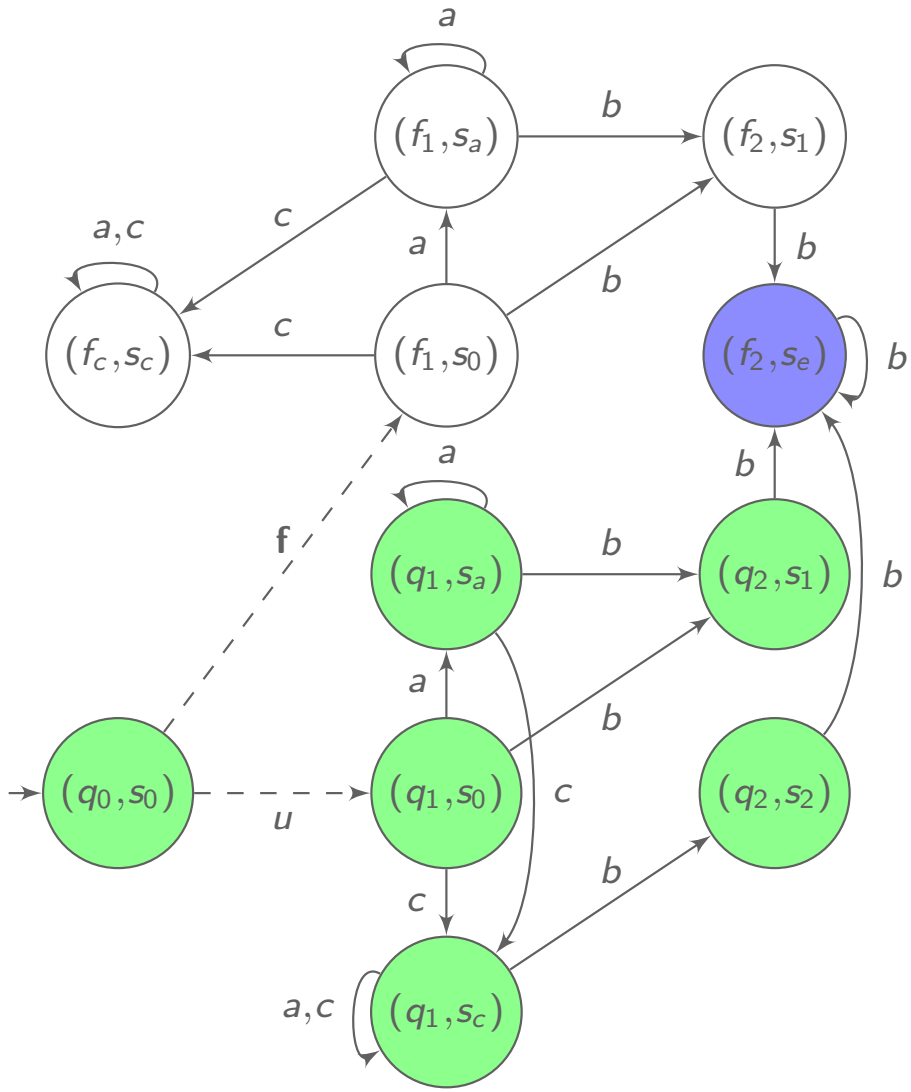
automate des croyances

s_e croyance surement fautive.

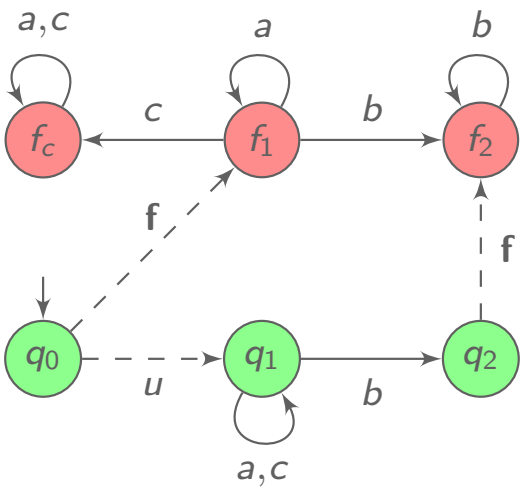
Faible résistance : idée de la preuve (2)



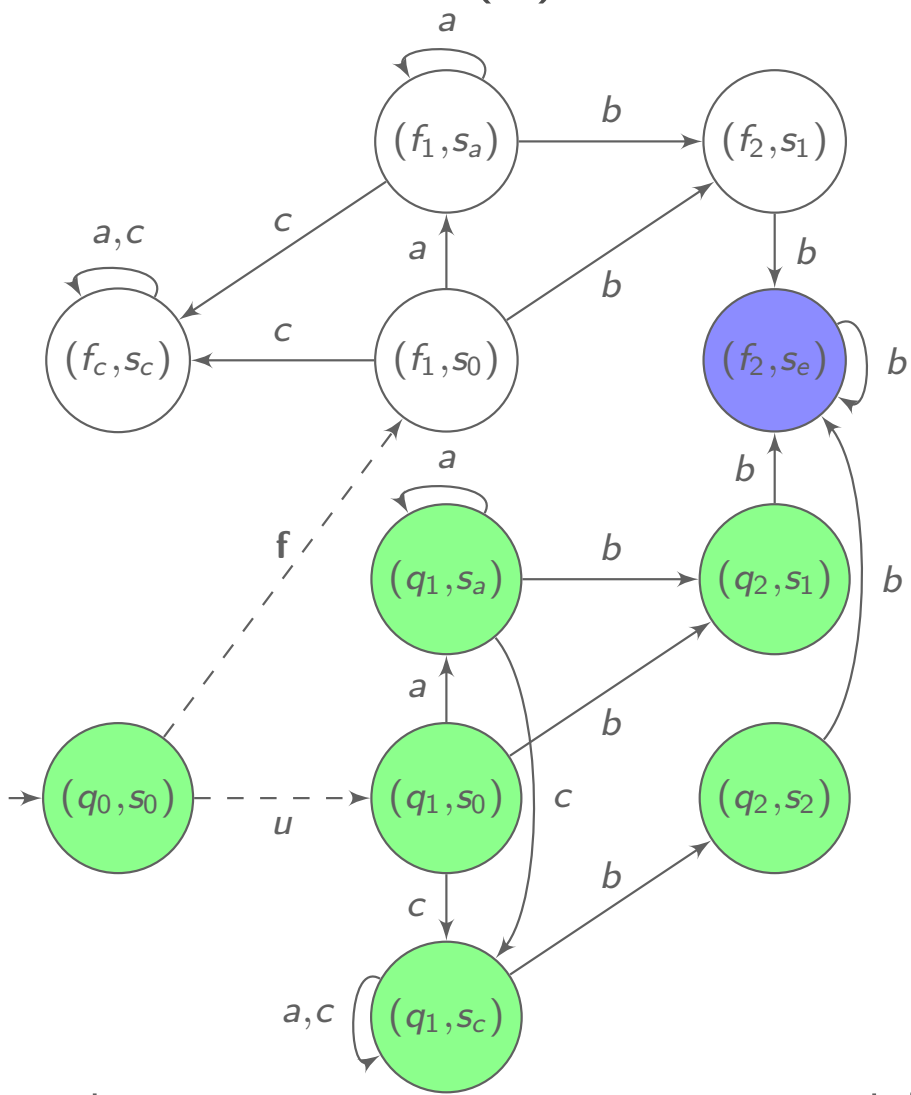
produit synchronisé



Faible résistance : idée de la preuve (2)

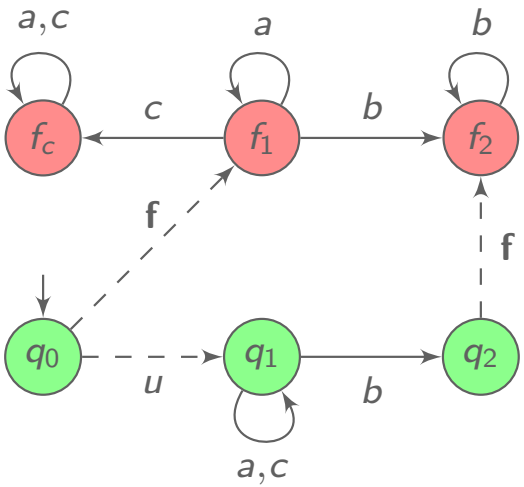


produit synchronisé

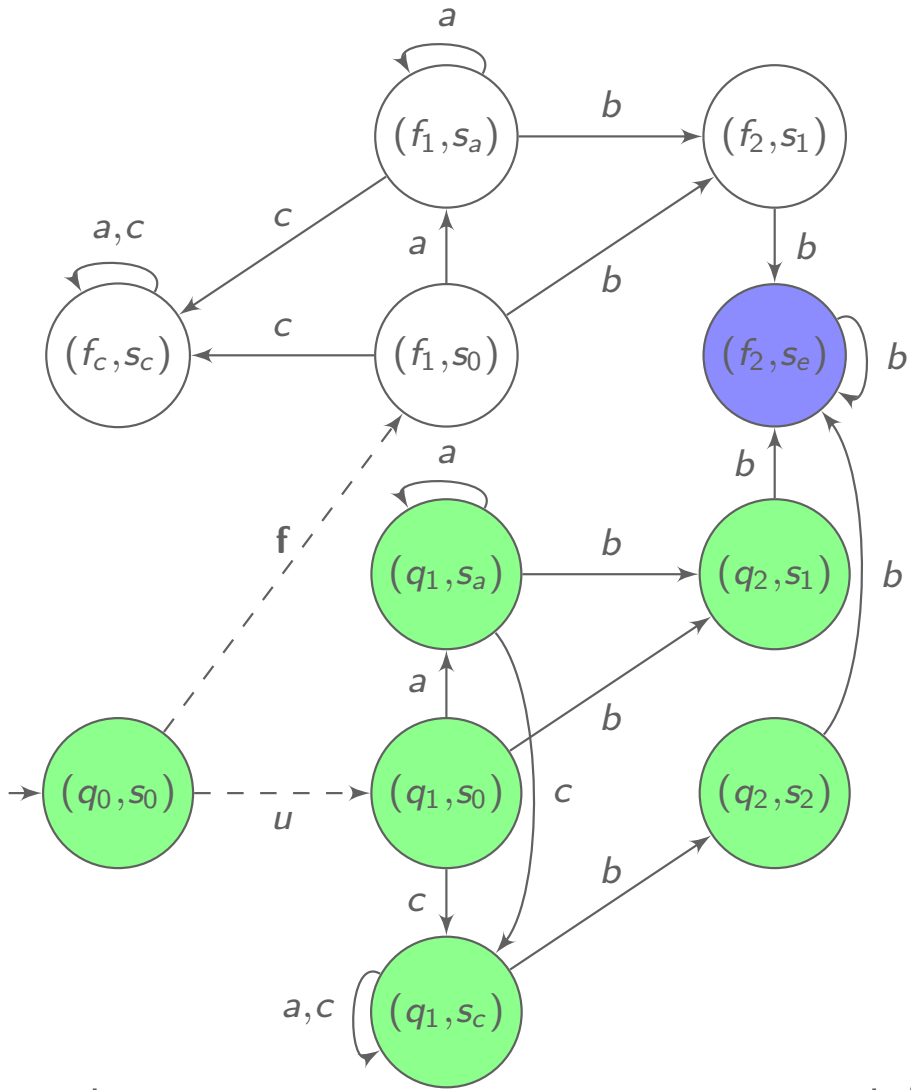


Target = configurations correctes ou avec une croyance surement fautive.

Faible résistance : idée de la preuve (2)

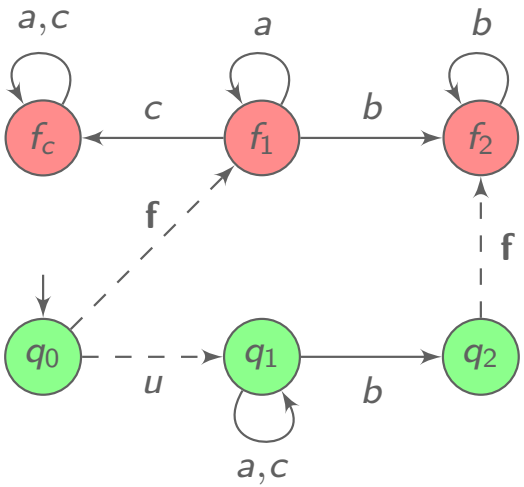


produit synchronisé

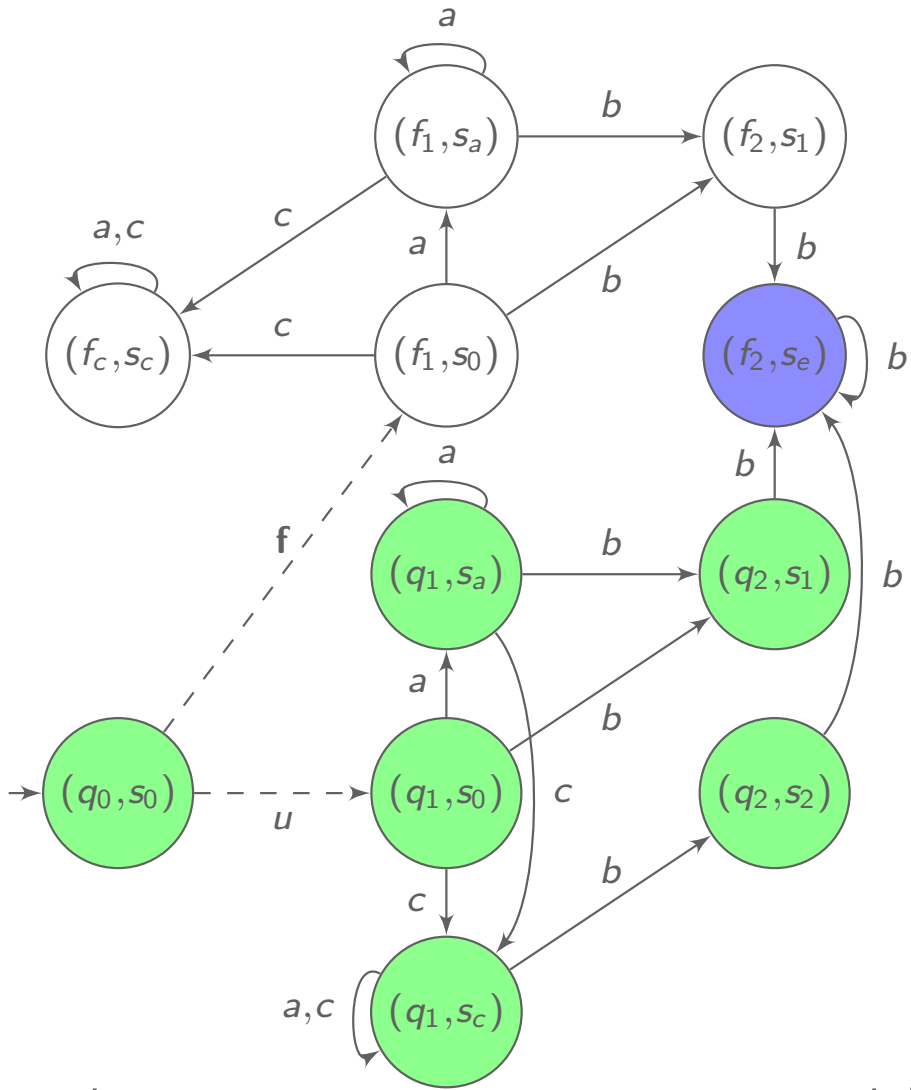


Target = configurations correctes ou avec une croyance surement fautive.
Win : plus grand point fixe tel que *Win* =
croyances dont les configurations atteignent *Target* sans quitter *Win*.

Faible résistance : idée de la preuve (2)

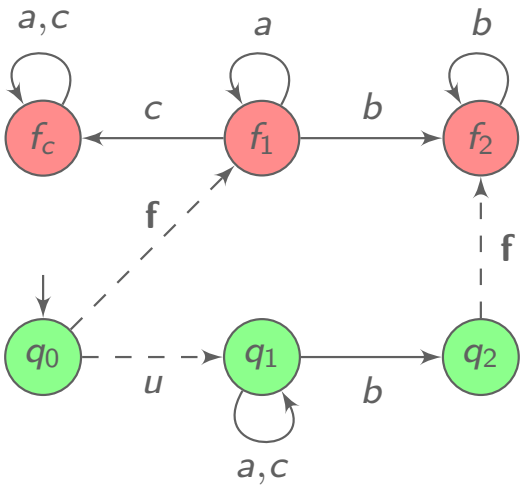


produit synchronisé

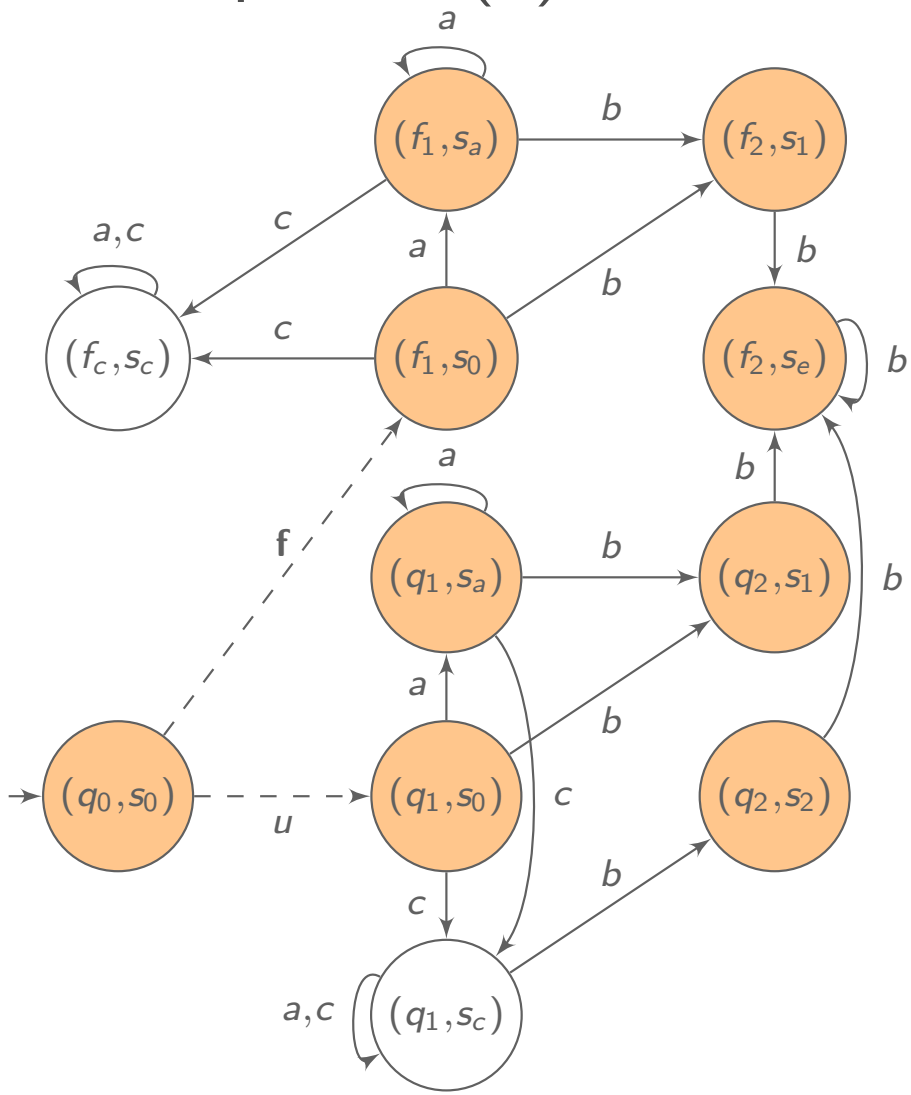


Target = configurations correctes ou avec une croyance surement fautive.
Win : plus grand point fixe tel que *Win* =
croyances dont les configurations atteignent *Target* sans quitter *Win*.

Faible résistance : idée de la preuve (2)



produit synchronisé



Target = configurations correctes ou avec une croyance surement fautive.
Win : plus grand point fixe tel que *Win* =
croyances dont les configurations atteignent *Target* sans quitter *Win*.

Faible résistance : idée de la preuve (3)

- SPTE diagnostiquable ssi $s_0 \in \mathit{Win}$.

Faible résistance : idée de la preuve (3)

- SPTE diagnostiquable ssi $s_0 \in \mathit{Win}$.

- SPTE faiblement résistant ssi diagnostiquable et il existe un circuit accessible de configurations correctes dont la croyance appartient à Win.
  - Absence de circuit $\Rightarrow \exists n \in \mathbb{N}, \mathbb{P}(C_n) = 0$,
  - Existence de circuit $\Rightarrow$ pour $\lambda <$ probabilité de réaliser le circuit,

$$\lim_{n \to \infty} \frac{\lambda^n}{\mathbb{P}(C_n)} = 0 \ .$$

Conclusion

Contributions

- Introduction de notions fines de dégradation d'un SPTE
- Liens sémantiques entre les notions
- Indécidabilité des nouvelles notions quantitatives
- EXPTIME-complétude des nouvelles notions qualitatives

Conclusion

Contributions

- Introduction de notions fines de dégradation d'un SPTE
- Liens sémantiques entre les notions
- Indécidabilité des nouvelles notions quantitatives
- EXPTIME-complétude des nouvelles notions qualitatives

Perspectives

- Étude d'autres formes de dégradation d'un système (compte de fautes, etc.)
- Implémentation des algorithmes dans COSMOS (model checker statistique pour automates hybrides)