Cadre Formel pour le Test de Robustesse des Protocoles de Communication

Farès SAAD KHORCHEF

LaBRI - Université BORDEAUX 1

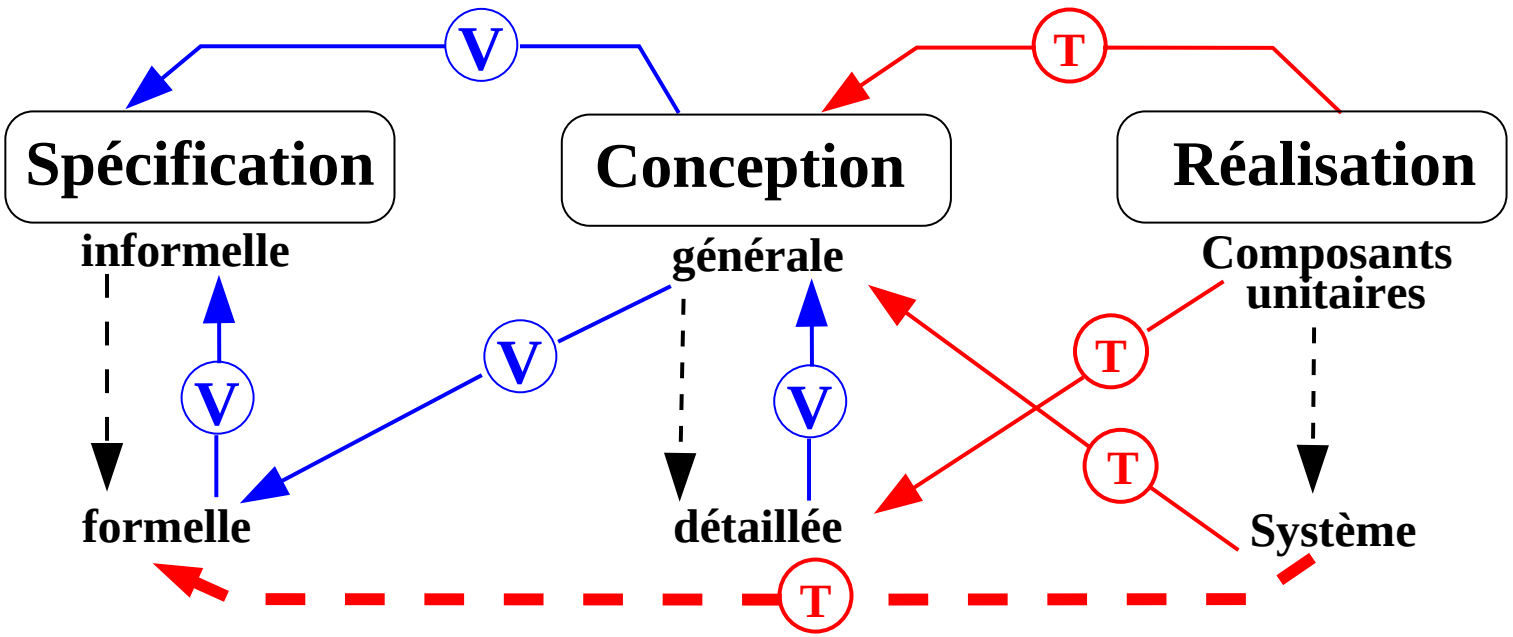
13 décembre 2006

Plan

Plan

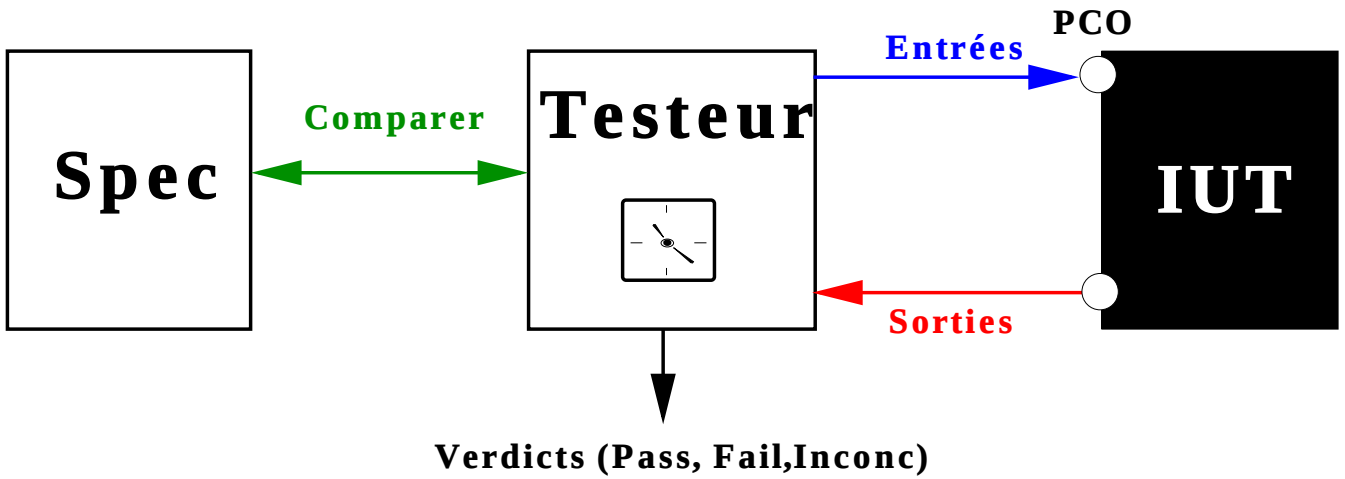
Test et cycle de vie d'un système

(T) : Tests **(V)** : Vérifications



- Le **test** ≡ exécution + observation d'une implémentation
- Le test peut être : **Boîte blanche** (structurel), **Boîte noire** (fonctionnel) ou **Boîte grise**

Test en boîte noire



- Le code de l'IUT (Implementation Under Test) est inconnu
- Vérification du comportement de l'IUT vis-à-vis de la **spécification** (formelle)
- Les verdicts : **Pass**, **Fail** ou **Inconclusive**
- Différents types de test en boîte noire : Conformité[1], **Robustesse**...

[1] ISO 9646. Conformance testing methodology and framework. Part 1-7 : 1994-95

Problématique de Robustesse

Robustesse selon AS23 [2]

La capacité d'un système à fonctionner de façon **acceptable** en présence d'**aléas**

[2] R. Castanet and H. Waeselynk. Techniques avancées de test des systèmes complexes : test de robustesse. *Action spécifique N°23 du CNRS* , IRISA, LAAS, LaBRI, LRI, Verimag.

Problématique de Robustesse

Robustesse selon AS23 [2]

La capacité d'un système à fonctionner de façon **acceptable** en présence d'**aléas**

- **Aléas** : fautes et conditions environnementales stressantes.
- Le comportement **acceptable** peut être différent du comportement **correct**

[2] R. Castanet and H. Waeselynk. Techniques avancées de test des systèmes complexes : test de robustesse. *Action spécifique N°23 du CNRS* , IRISA, LAAS, LaBRI, LRI, Verimag.

Problématique de Robustesse

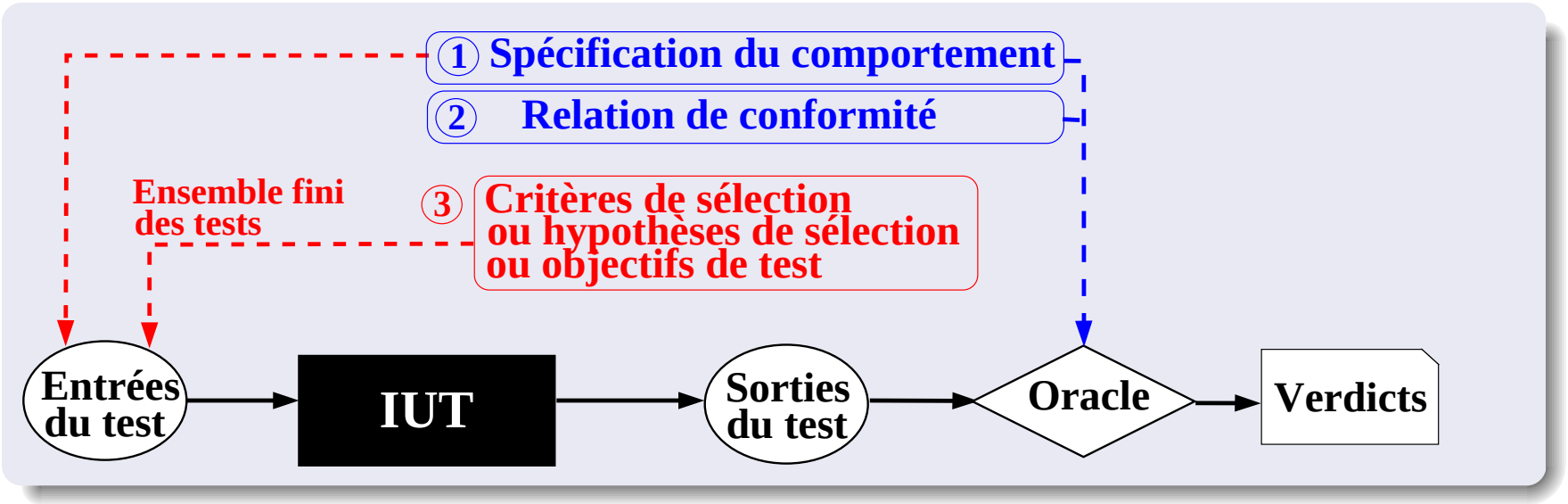
Robustesse selon AS23 [2]

La capacité d'un système à fonctionner de façon **acceptable** en présence d'**aléas**

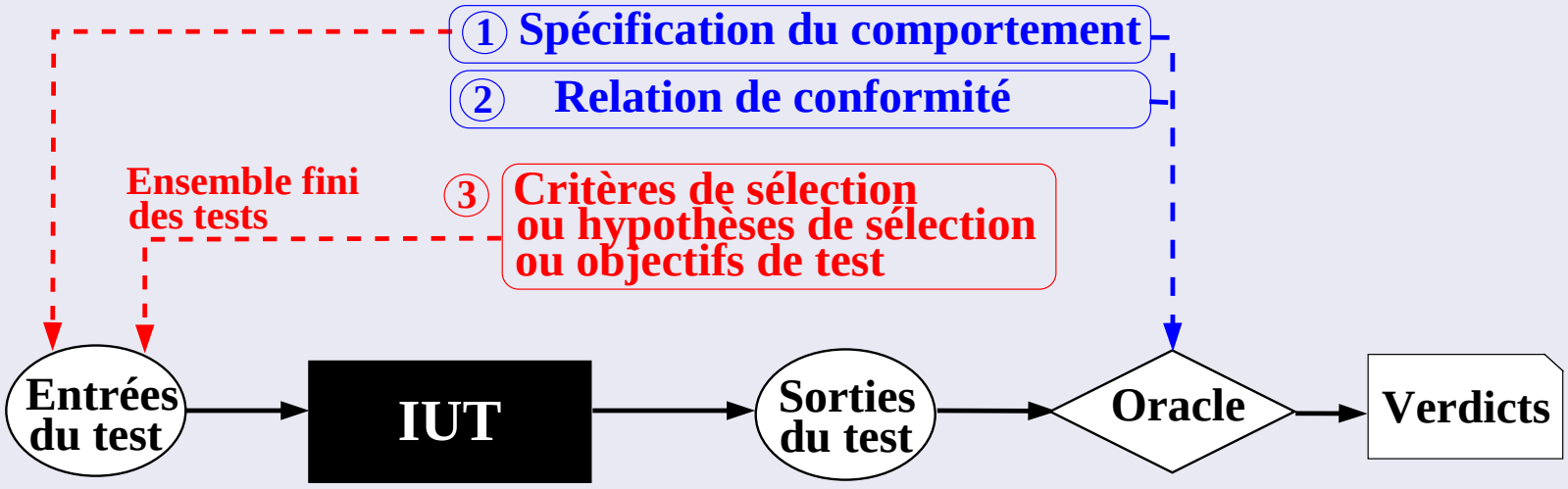
- **Aléas** : fautes et conditions environnementales stressantes.
- Le comportement **acceptable** peut être différent du comportement **correct**
- Aléas **imprévisibles** ⇒ comportement acceptable non spécifié
- Robustesse en présence d'aléas non prévus ?

[2] R. Castanet and H. Waeselynk. Techniques avancées de test des systèmes complexes : test de robustesse. *Action spécifique N°23 du CNRS* , IRISA, LAAS, LaBRI, LRI, Verimag.

Méthodologie et Objectifs



Méthodologie et Objectifs



Objectifs

1. Construction d'un modèle référence pour le test de robustesse
2. Proposition d'une relation formelle pour la robustesse
3. Proposition d'une méthode pour la génération des cas de test de robustesse

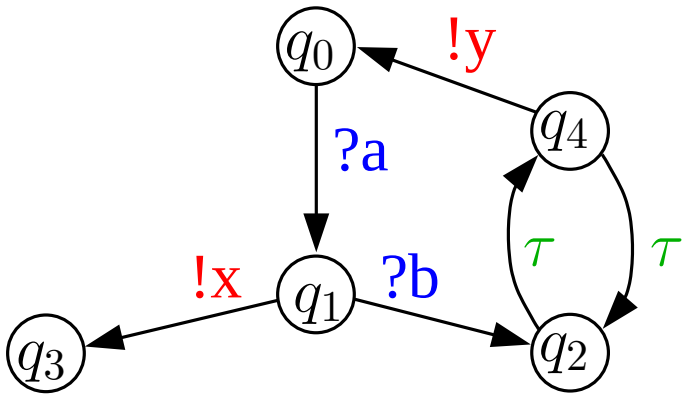
Plan

Système de Transitions Étiquetées à Entrée/Sortie [3]

Definition ($IOLTS$)

Un $IOLTS$ $S = (Q, A, \rightarrow, q_0)$:

- Q : ensemble fini d'états, q_0 : état initial.
- A : alphabet d'actions observables.
  - Sortie : $!x$
  - Entrée : $?a$
- $\rightarrow : Q \times A \cup \{\tau\} \times Q$ relation de transition (τ : action interne).



Un IOLTS S

- $A = \{?a, ?b, !x, !y\}$
- $Traces(S) = \{?a, ?a.!x, ?a.?b, ?a.?b.!y, ...\}$
- $q_0\ after\ ?a = q_1$
- $Out(q_0) = \emptyset$ et $Out(q_1) = \{!x\}$

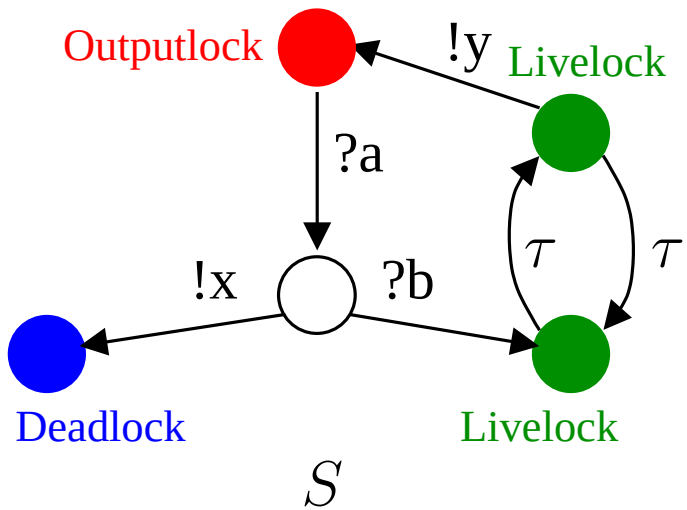
[3] Jan Tretmans. Conformance Testing with Labelled Transition Systems. Implementation Relations and Test Generation. Computer Networks and ISDN Systems 29(1). 49-79 (1996)

Silence dans les IOLTSs [4]

- Le testeur observe les sorties (**outputs**) et le silence (**quiescence**) de l'IUT

Silences des IOLTS

- **Outputlock**
- **Deadlock**
- **Livelock**



[4] J. Tretmans. Test Generation with Inputs, Outputs and Repetitive Quiescence. *Software - Concepts and Tools. Vol.17(3), pp.103-120, 1996.*

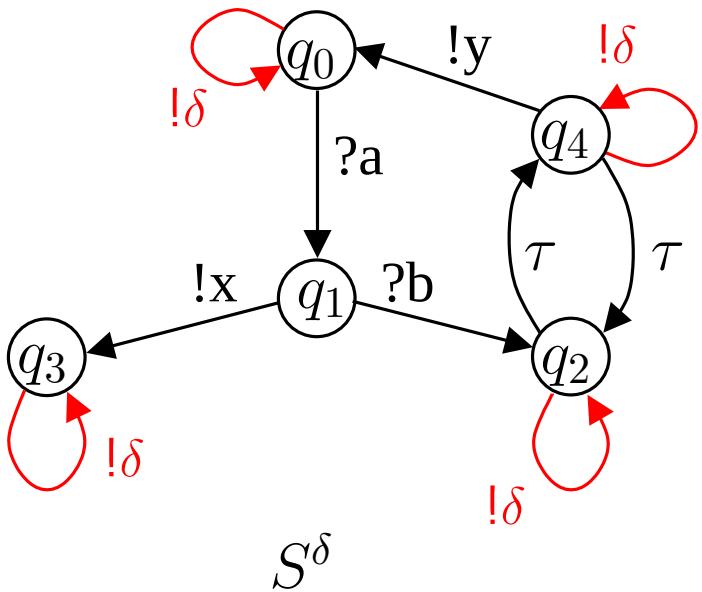
Silence dans les IOLTSs [4]

- Il est nécessaire de modéliser les silences (quiescence) dans la spécification

Automate Suspendu S^{δ}

Addition à S des boucles $q \xrightarrow{!\delta} q$ pour tout état de silence.

$!\delta$: une sortie



S^{δ}

[4] J. Tretmans. Test Generation with Inputs, Outputs and Repetitive Quiescence. *Software - Concepts and Tools. Vol.17(3), pp.103-120, 1996.*

Aléas

Aléa : tout événement omis dans la spécification nominale

- fautes et conditions de stress
- actions correctes, mais imprévues dans l'état courant

Aléas

Aléa : tout événement omis dans la spécification nominale

- fautes et conditions de stress
- actions correctes, mais imprévues dans l'état courant

Classification d'aléas

1. La **situation vis-à-vis des frontières** du système [AS23]
2. La **représentabilité** dans un modèle formel
3. La **contrôlabilité** par le testeur

Aléas

Aléa : tout événement omis dans la spécification nominale

- fautes et conditions de stress
- actions correctes, mais imprévues dans l'état courant

Classification d'aléas

1. La **situation vis-à-vis des frontières** du système [AS23]
2. La **représentabilité** dans un modèle formel
3. La **contrôlabilité** par le testeur

Classification proposée[5]

1. **Aléas contrôlables et représentables**
2. **Aléas contrôlables et non représentables**

[5] F. SAAD KHORCHEF. Robustness Testing for Reactive Systems, EDCC 2006, IEEE, Coimbra

Aléas contrôlables et représentables

- Dans le domaine des protocoles, on peut identifier :

Entrées invalides

- entrées spécifiées, mais erronées
- entrées non spécifiées

Aléas contrôlables et représentables

- Dans le domaine des protocoles, on peut identifier :

Entrées invalides

- entrées spécifiées, mais erronées
- entrées non spécifiées

Entrées inopportunes

- entrées spécifiées dont la réception est inattendue dans l'état courant du système

Aléas contrôlables et représentables

- Dans le domaine des protocoles, on peut identifier :

Entrées invalides

- entrées spécifiées, mais erronées
- entrées non spécifiées

Entrées inopportunes

- entrées spécifiées dont la réception est inattendue dans l'état courant du système

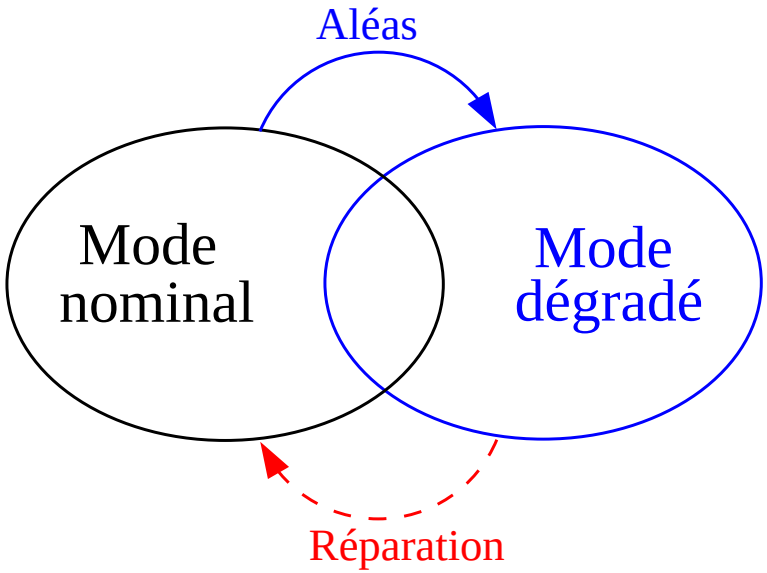
Sorties inattendues

- sorties spécifiées dont l'émission est inattendue dans l'état courant du système
- sorties non spécifiées

★ certaines sorties inattendues peuvent être **acceptables**

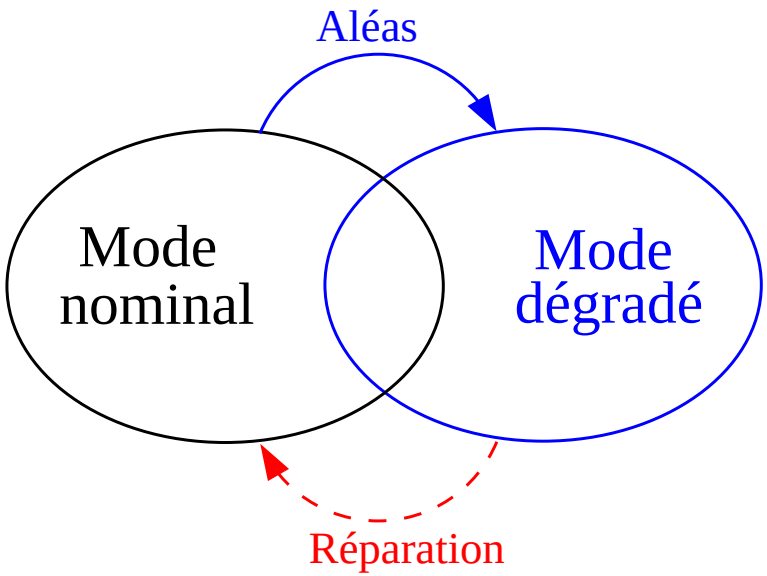
Plan

Modélisation du comportement en présence d'aléas



- **Mode nominal** ≡ IOLTS (états + transitions nominales)
- **Mode dégradé** ≡ IOLTS (états + transitions dégradées)
- Seul le **mode nominal** est disponible (spécification nominale)
- Le **mode dégradé** est obtenu à la demande du testeur de robustesse et défini vis-à-vis un ensemble d'aléas

Modélisation du comportement en présence d'aléas



Meta-graphe

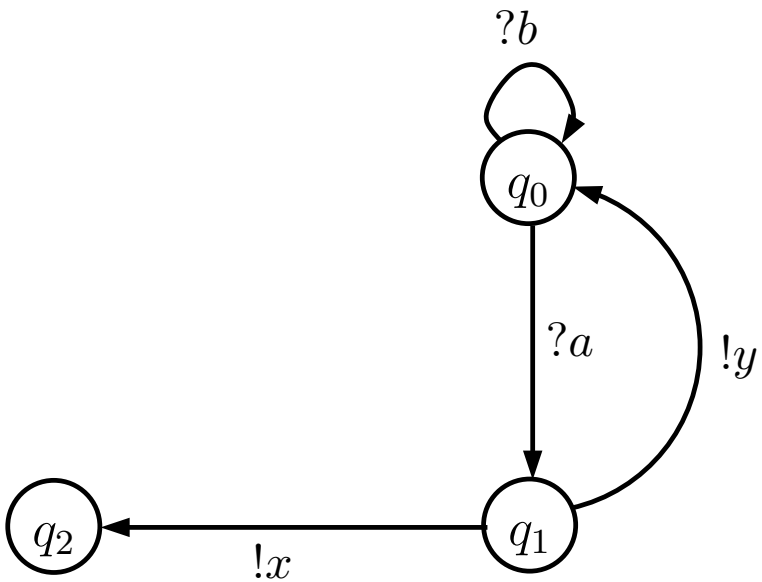
Un meta-graphe $G = (V, E, L)$ associé a un IOLTS S :

- V : meta-état(s) + états nominaux + états dégradés
- E : ensemble de transitions
- L : alphabet d'action

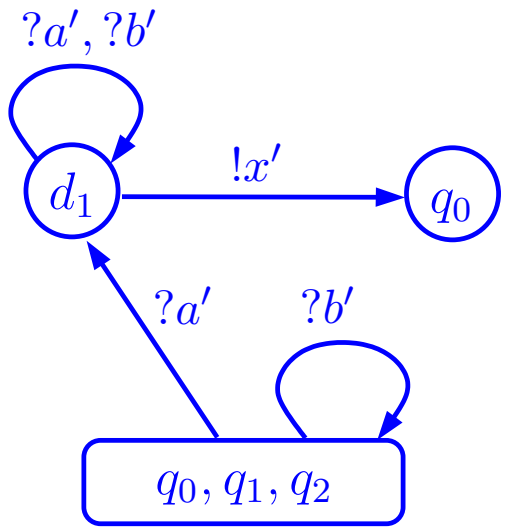
Modélisation du comportement en présence d'aléas

Meta-graphe d'aléas

Ce meta-graphe est fourni par les concepteurs pour spécifier le comportment en présence d'entrées invalides



Spécification nominale S

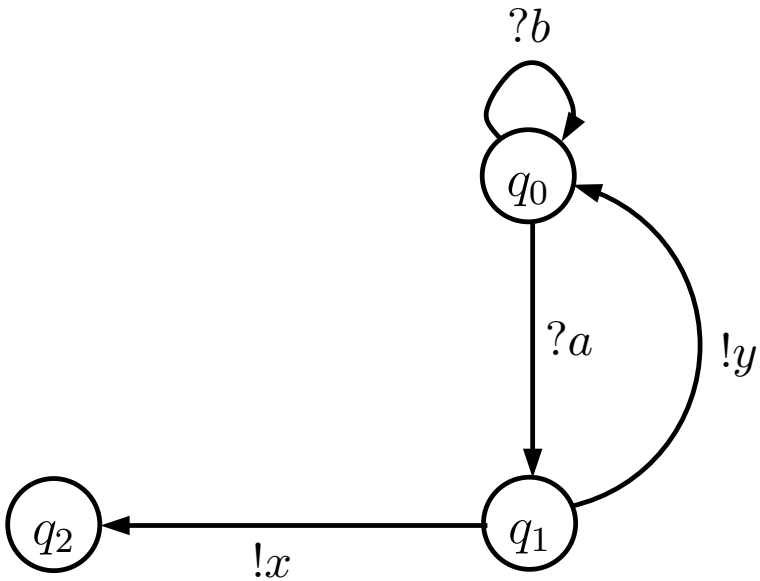


Meta-graphe d'aléas (entrées invalides)

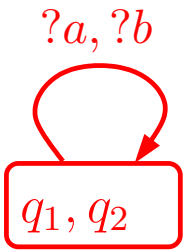
Modélisation du comportement en présence d'aléas

Meta-graphe d'entrées inopportunes

Ce meta-graphe est fourni par les concepteurs pour spécifier le comportment en présence d'entrées inopportunes



Spécification nominale S



Meta-graphe d'entrées inopportunes

Approche proposée

Définition de la robustesse

Un système est considéré comme robuste s'il est d'abord conforme à sa spécification nominale et montre un comportement acceptable en présence d'aléas

Approche proposée

Définition de la robustesse

Un système est considéré comme robuste s'il est d'abord conforme à sa spécification nominale et montre un comportement acceptable en présence d'aléas

Il existe D'autres visions de la robustesse

Attribut spécial de sûreté de fonctionnement [6]

[6] A.AVIZIENIS, J.C.LAPRIE, B.RANDELL, C.LANDWEHR. Basic concepts and taxonomy of dependable and secure computing, *IEEE Trans on Dependable and Secure Computing*, Vol.1, N°1, pp.11-33, 2004

Approche proposée

Définition de la robustesse

Un système est considéré comme robuste s'il est d'abord conforme à sa spécification nominale et montre un comportement acceptable en présence d'aléas

Approche proposée

1. **Méthode TRACOR** ≡ *Test de Robustesse en présence d'Aléas COntrôlables et Représentables*
2. **Méthode TRACON** ≡ *Test de Robustesse en présence d'Aléas COntrôlables et Non représentables*

Méthode TRACOR [6] [7]

Objectifs

Génération des cas de test de robustesse en présence d'aléas contrôlables et représentables

[6] F. SAAD KHORCHEF, A. ROLLET and R. CASTANET. A Framework and a Tool for Robustness Testing of communicating Software, ACM SAC 2007 (accepted paper)

[7] F. SAAD KHORCHEF, I. BERRADA, A. ROLLET and R. CASTANET. Automated Robustness Testing for Reactive Systems : Application to Communicating Protocols, I2CS 2006, LNCS, Neuchâtel.

Méthode TRACOR [6] [7]

Objectifs

Génération des cas de test de robustesse en présence d'aléas contrôlables et représentables

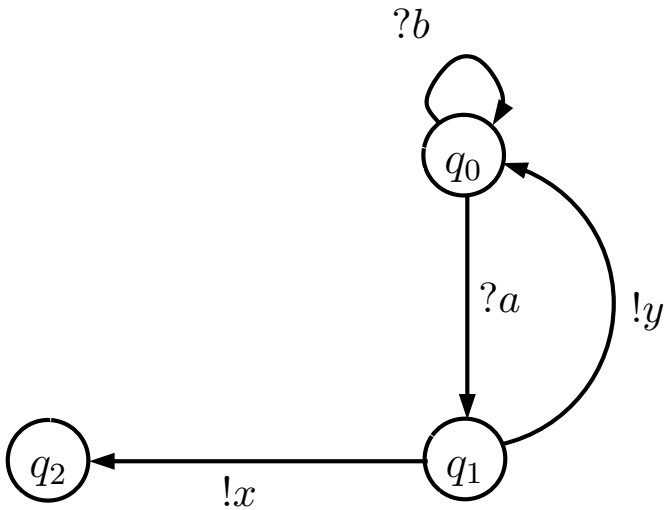
- **Phase 1** : Augmentation de la spécification :
  1. Ajout de silence
  2. Intégration d'entrées invalides
  3. Intégration d'entrées inopportunes
  4. Mise à jour de silence et déterminisation
- **Phase 2** : Génération des cas de test de robustesse

[6] F. SAAD KHORCHEF, A. ROLLET and R. CASTANET. A Framework and a Tool for Robustness Testing of communicating Software, ACM SAC 2007 (accepted paper)

[7] F. SAAD KHORCHEF, I. BERRADA, A. ROLLET and R. CASTANET. Automated Robustness Testing for Reactive Systems : Application to Communicating Protocols, I2CS 2006, LNCS, Neuchâtel.

TRACOR : augmentation de la spécification

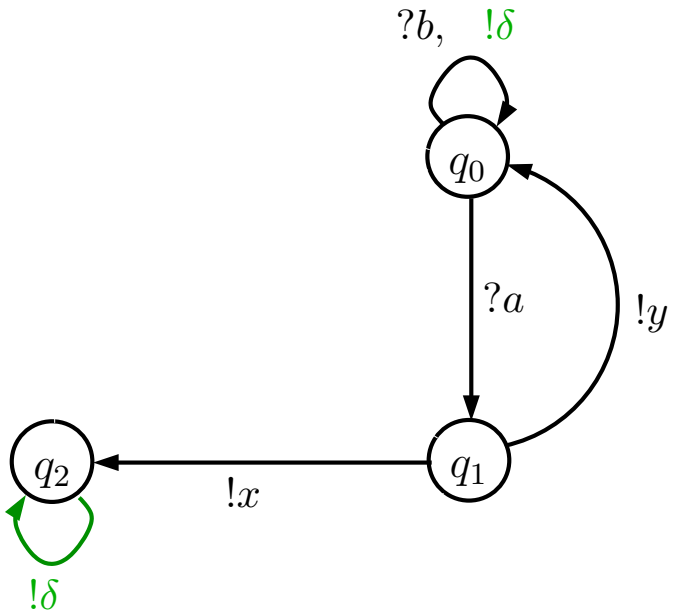
- Ajout de silence : boucles étiquetées par $!\delta$ dans chaque état de silence



Spécification nominale S

TRACOR : augmentation de la spécification

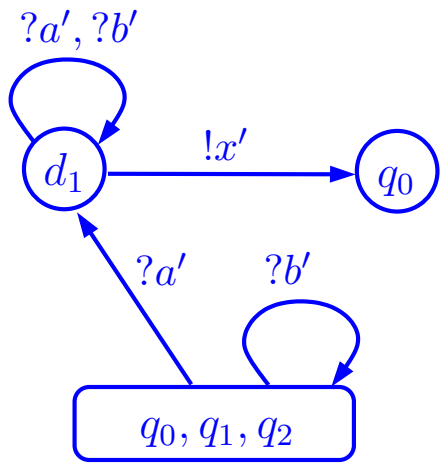
- Ajout de silence : boucles étiquetées par $!\delta$ dans chaque état de silence



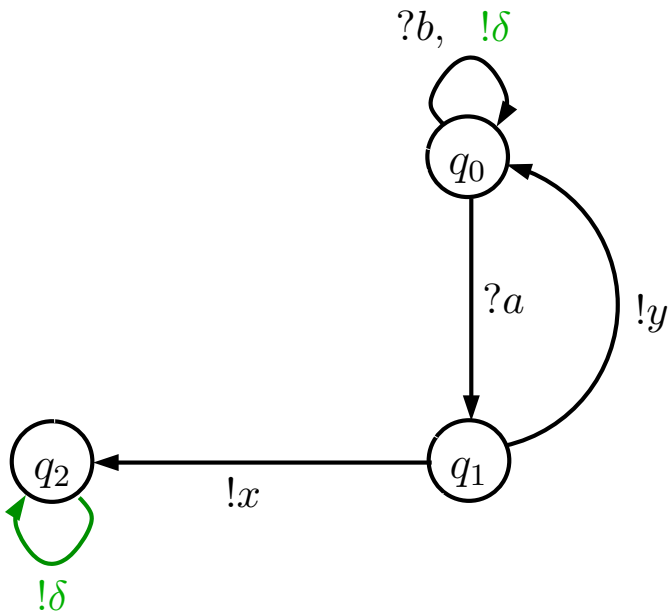
Automate suspendu S^{δ}

TRACOR : augmentation de la spécification

- Intégration d'états dégradés et transitions du meta-graphe d'aléas (entrées invalides)



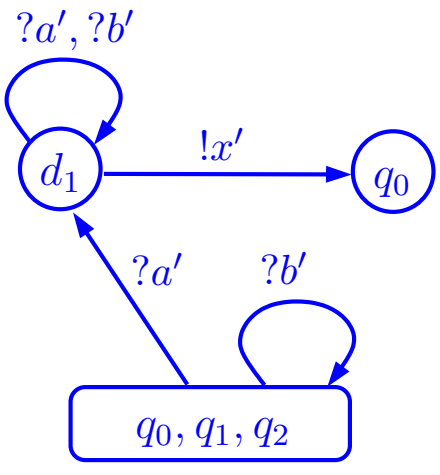
Meta-graphe d'aléas



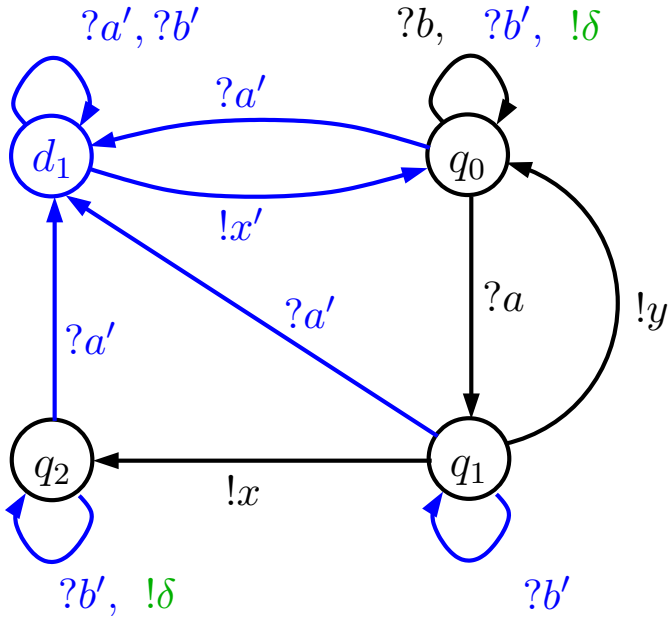
Automate suspendu

TRACOR : augmentation de la spécification

- Intégration d'états dégradés et transitions du meta-graphe d'aléas (entrées invalides)



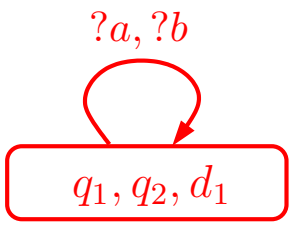
Meta-graphe d'aléas



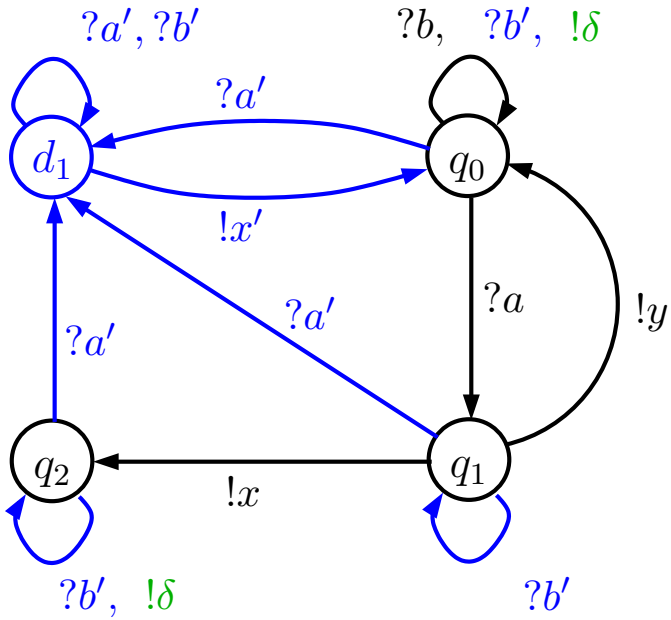
$S' = S^{\delta}$ avec entrées invalides

TRACOR : augmentation de la spécification

- Intégration d'états dégradés et transitions du meta-graphe d'entrées inopportunes



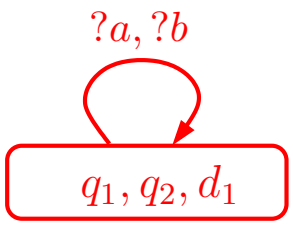
Meta-graphe d'entrées inopportunes



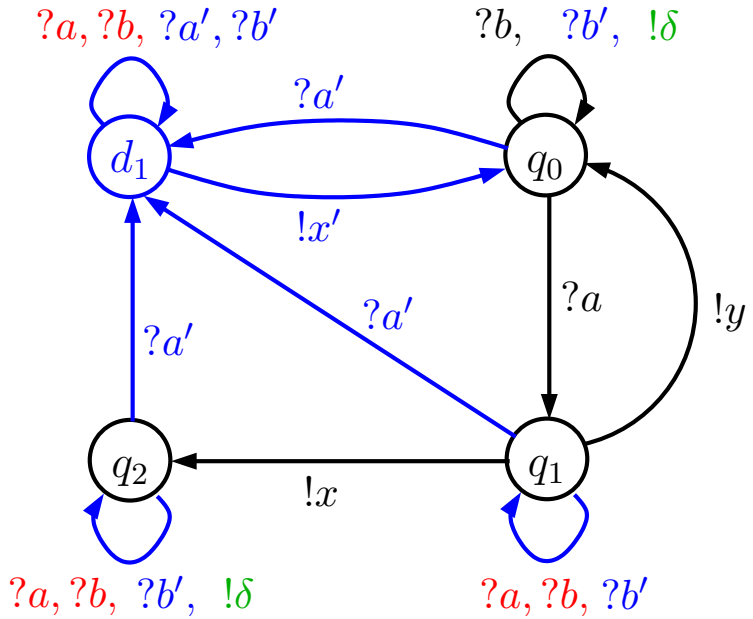
$S' = S^{\delta}$ avec entrées invalides

TRACOR : augmentation de la spécification

- Intégration d'états dégradés et transitions du meta-graphe d'entrées inopportunes



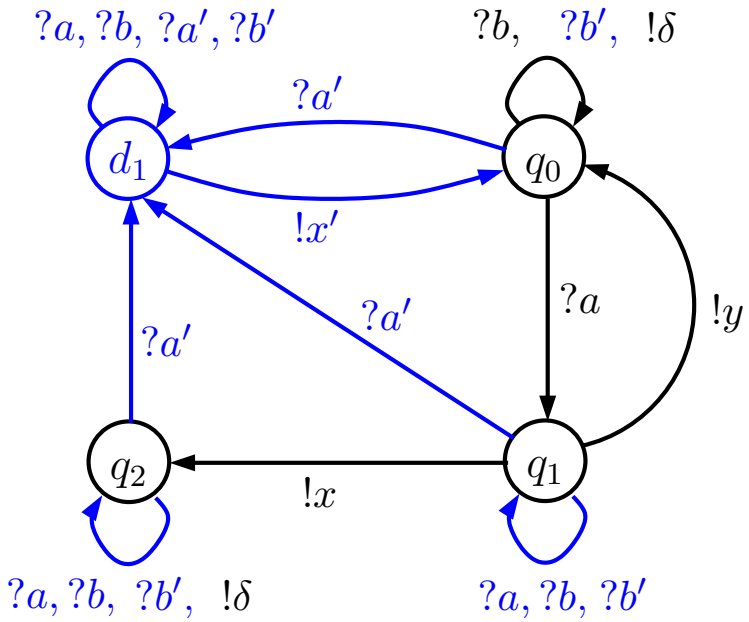
Meta-graphe d'entrées inopportunes



$S'' = S'$ avec entrées inopportunes

TRACOR : augmentation de la spécification

- Mise à jour de silence et déterminisation



Spécification augmentée S_A

- **Spécification augmentée** (S_A) décrit le comportement du système en présence d'aléas contrôlables et représentables
- S_A est coloriée avec **deux couleurs**

Relation de robustesse [8]

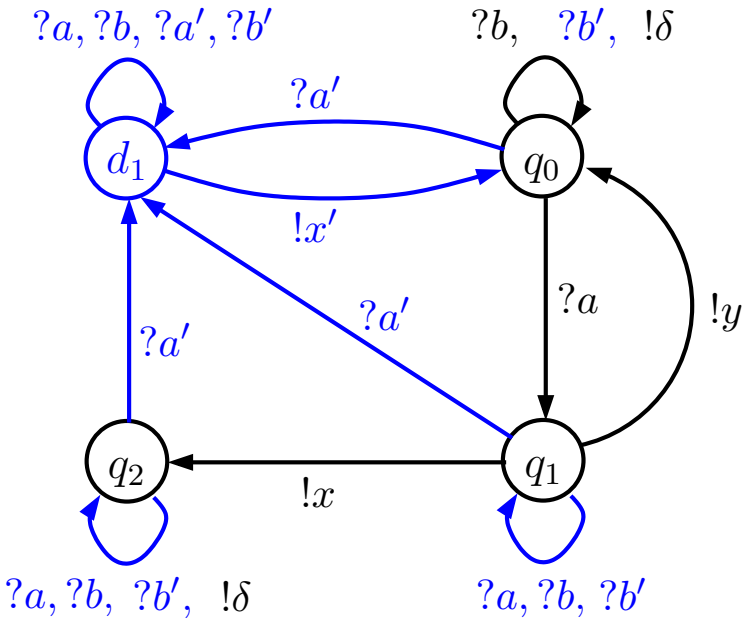
- Hypothèse du test : IUT est modélisable par un IOLTS

$$IUT \ \textbf{Robust} \ S_A \equiv_{def} \forall \sigma \in Traces(S_A) \backslash Traces(S^{\delta}) \Rightarrow Out(IUT^{\delta} \ after \ \sigma) \subseteq Out(S_A \ after \ \sigma)$$

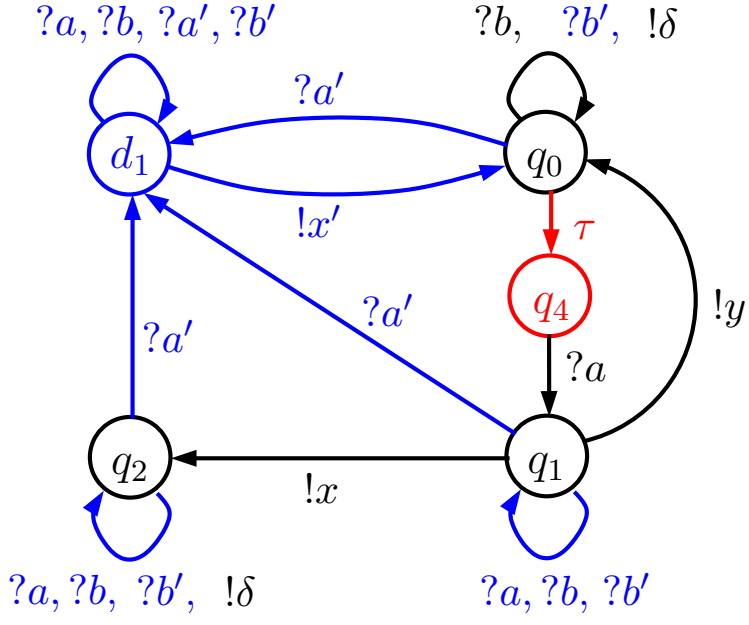
- **Robust** est fondée sur :
  - Observation de sorties et de silences (quiescence) de l'IUT
  - Exclusion des traces uniquement nominales

[8] F. SAAD KHORCHEF,I. BERRADA, A. ROLLET et R. CASTANET. Cadre formel pour le test de robustesse : Application au protocole SSL. CFIP 2006, Tozeur.

Exemple (Robust)



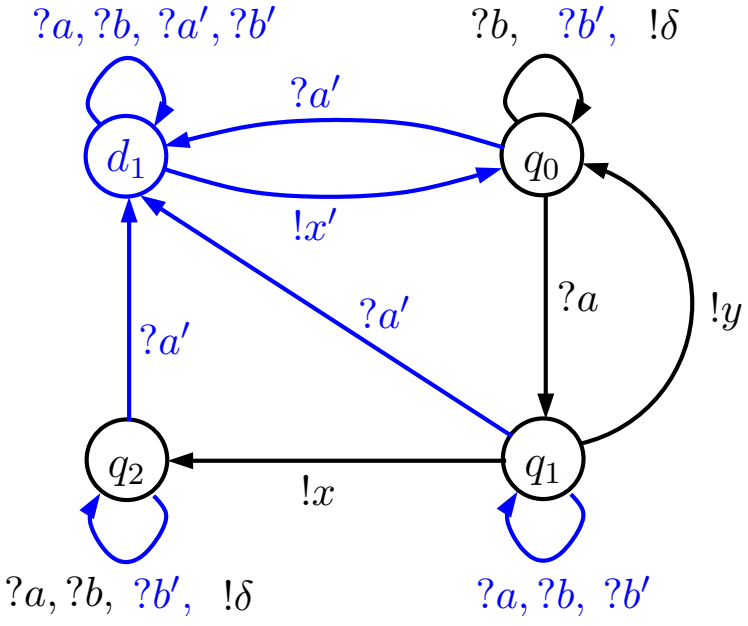
S_A



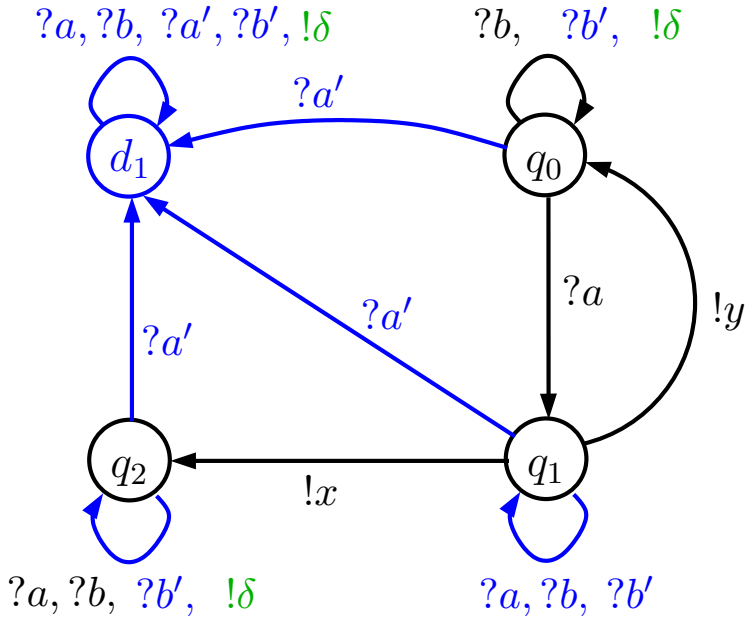
$IUT_1{}^{\delta}$

- $IUT1$ **Robust** S_A
  $Traces(IUT_1) = Traces(S_A)$

Exemple (Robust)



S_A



$IUT_2{}^{\delta}$

- $(IUT2$ **Not Robust** $S_A)$
  $Out(S_A\ after\ ?a') = \{!x'\} \subsetneq Out(IUT_2\ after\ ?a') = \{!\delta\}$

TRACOR : Génération des tests [9]

Principe

- **Référence** : spécification augmentée (S_A) + ***Robust***
- S_A est de taille importante $\Longrightarrow$ objectifs de test de robustesse
- Cas de test incluant les aléas

[9] F. SAAD KHORCHEF, R. CASTANET. Génération des tests de robustesse, NOTERE 2006, Hermès, Toulouse

TRACOR : Génération des tests [9]

Principe

- **Référence** : spécification augmentée (S_A) + ***Robust***
- S_A est de taille importante $\Longrightarrow$ objectifs de test de robustesse
- Cas de test incluant les aléas

Méthode proposée

1. Choix d'un objectif de test de robustesse RTP
2. Synchronisation de RTP avec la spécification augmentée S_A
3. Construction du graphe du test de robustesse (RTG)
4. Construction du graphe réduit de test de robustesse RRTG
5. Sélection d'un cas de test de robustesse RTC

[9] F. SAAD KHORCHEF, R. CASTANET. Génération des tests de robustesse, NOTERE 2006, Hermès, Toulouse

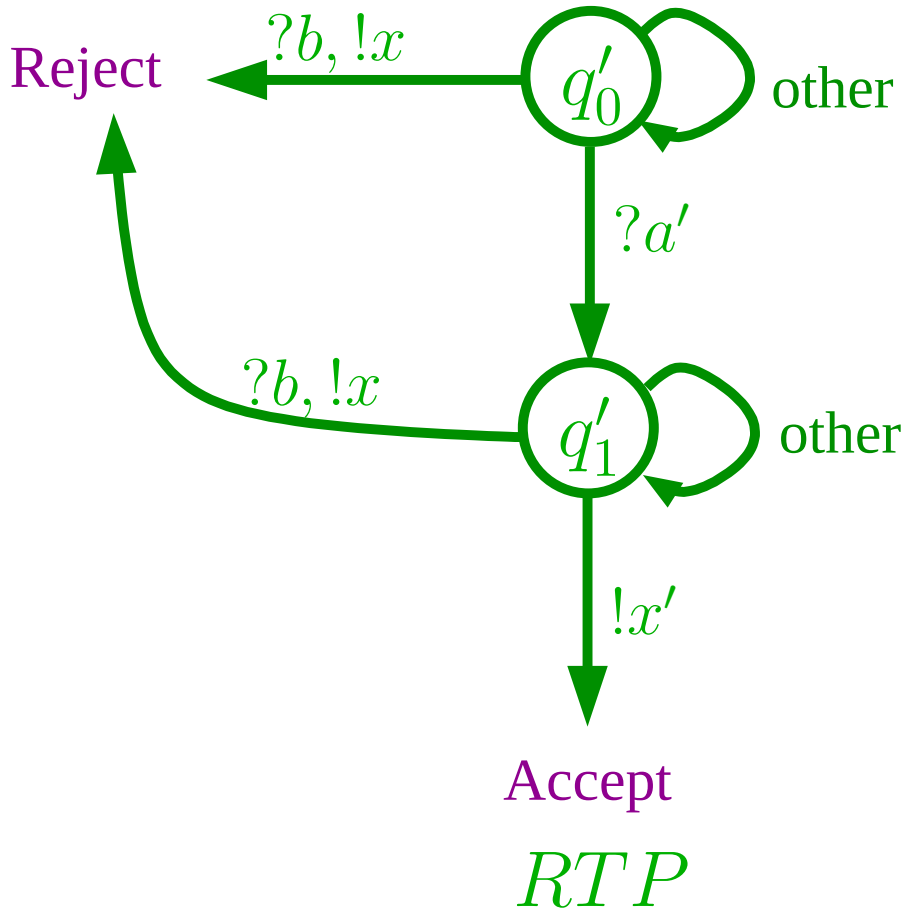
TRACOR : Objectifs de test de robustesse

RTP

Un objectif de test de robustesse RTP correspond à une suite d'entrées/sorties qui doivent figurer dans les séquences du test pour vérifier la propriété voulue :

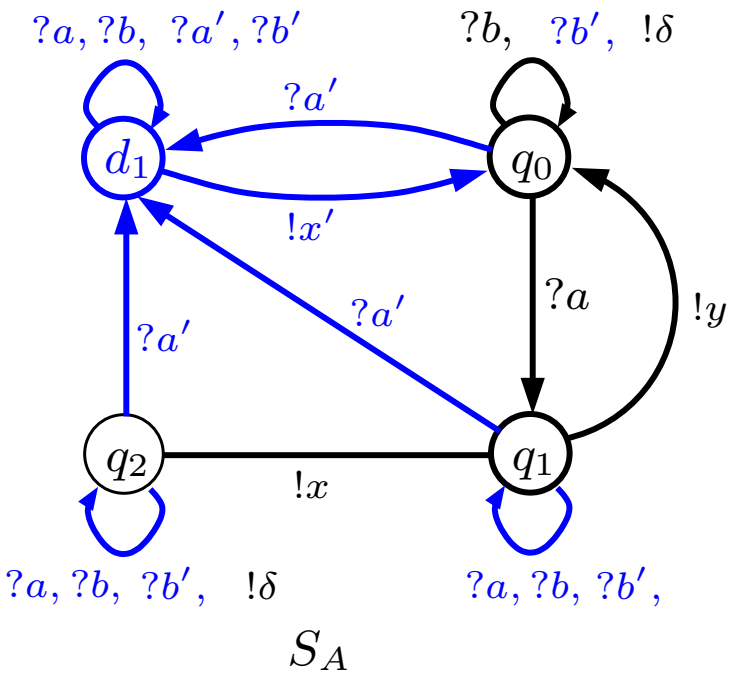
- **Accept** : traces acceptées
- **Reject** : traces rejetées

other : actions non spécifiées dans l'état courant



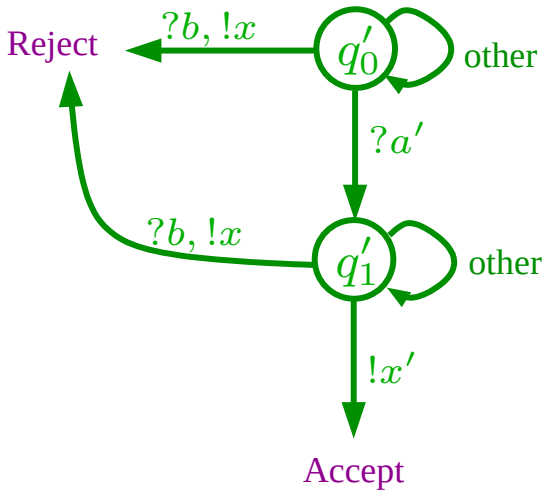
TRACOR : Produit synchrone

- Le produit synchrone PS permet de distinguer les traces de S_A acceptées par RTP de celles qui sont rejetées par RTP



S_A

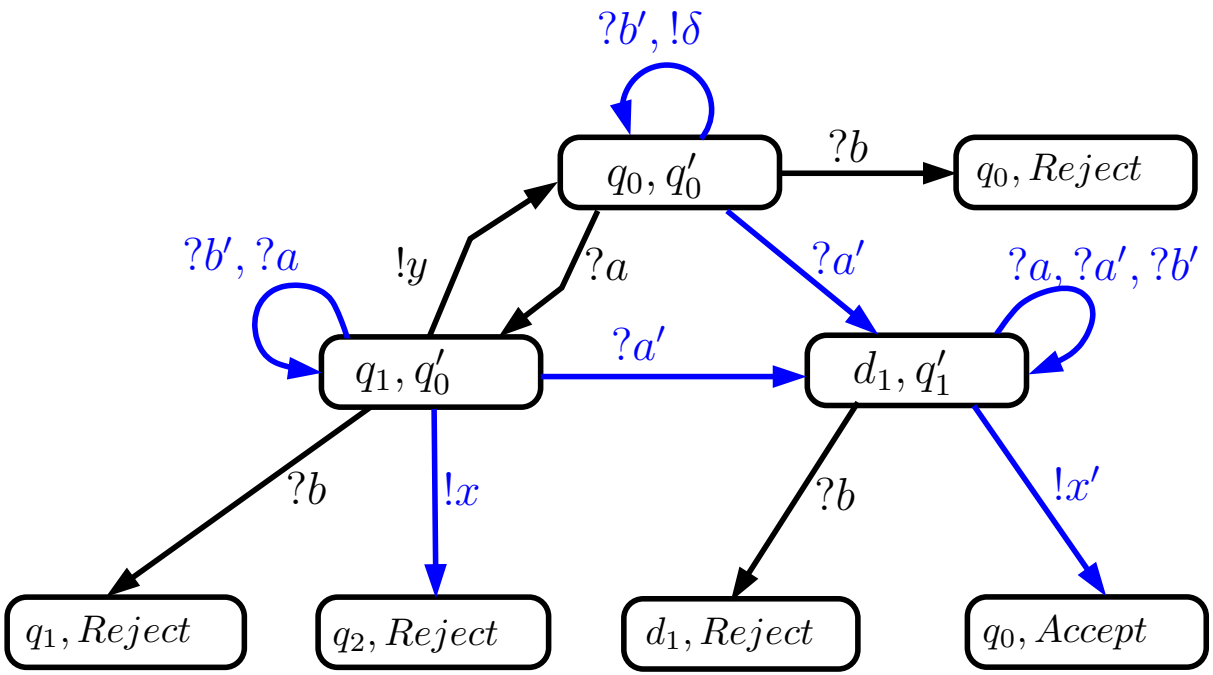
$\otimes$



RTP

TRACOR : Produit synchrone

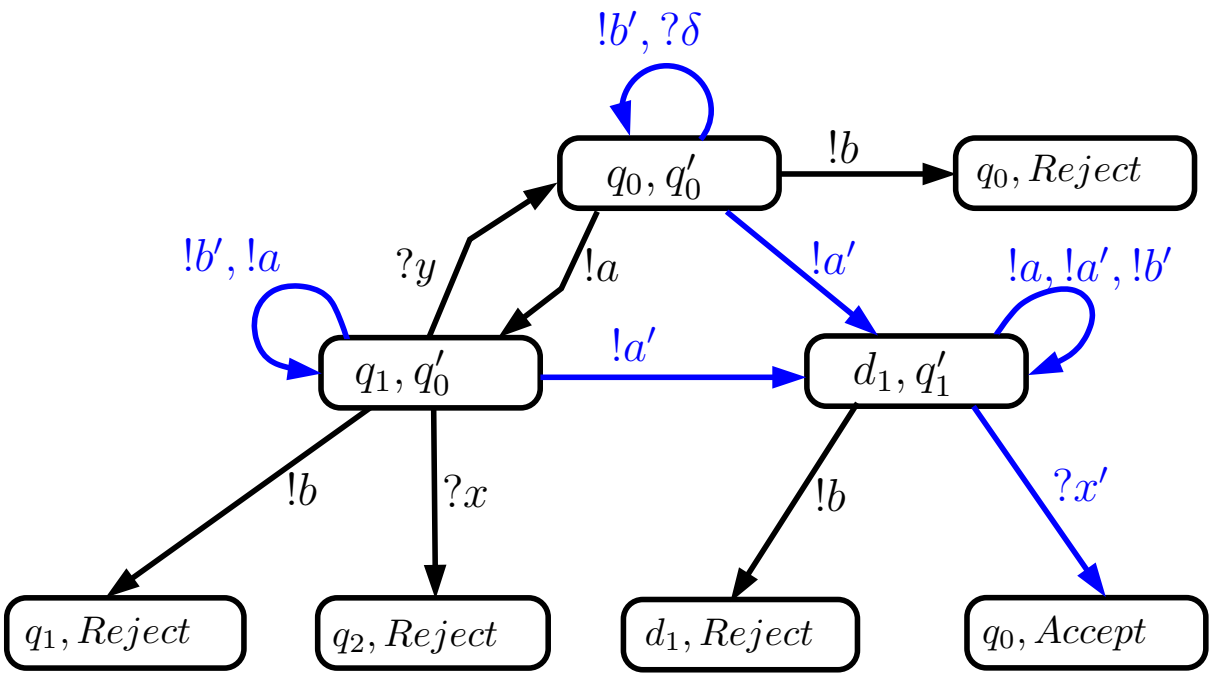
- Le produit synchrone PS permet de distinguer les traces de S_A acceptées par RTP de celles qui sont rejetées par RTP



Produit synchrone

TRACOR : Graphe du test de robustesse RTG

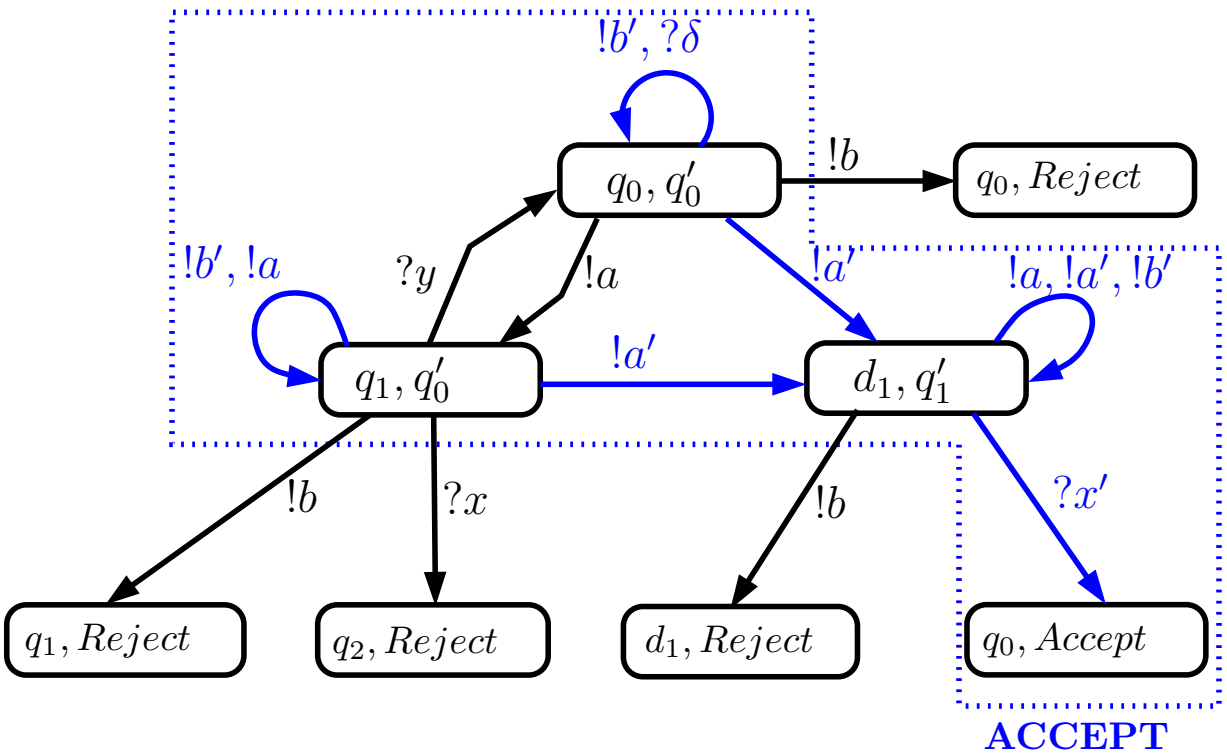
- Le graphe du test de robustesse RTG décrit tous les tests possibles correspondant à un objectif de test de robustesse RTP



Graphe du test de robustesse *RTG*

TRACOR : Graphe du test de robustesse RTG

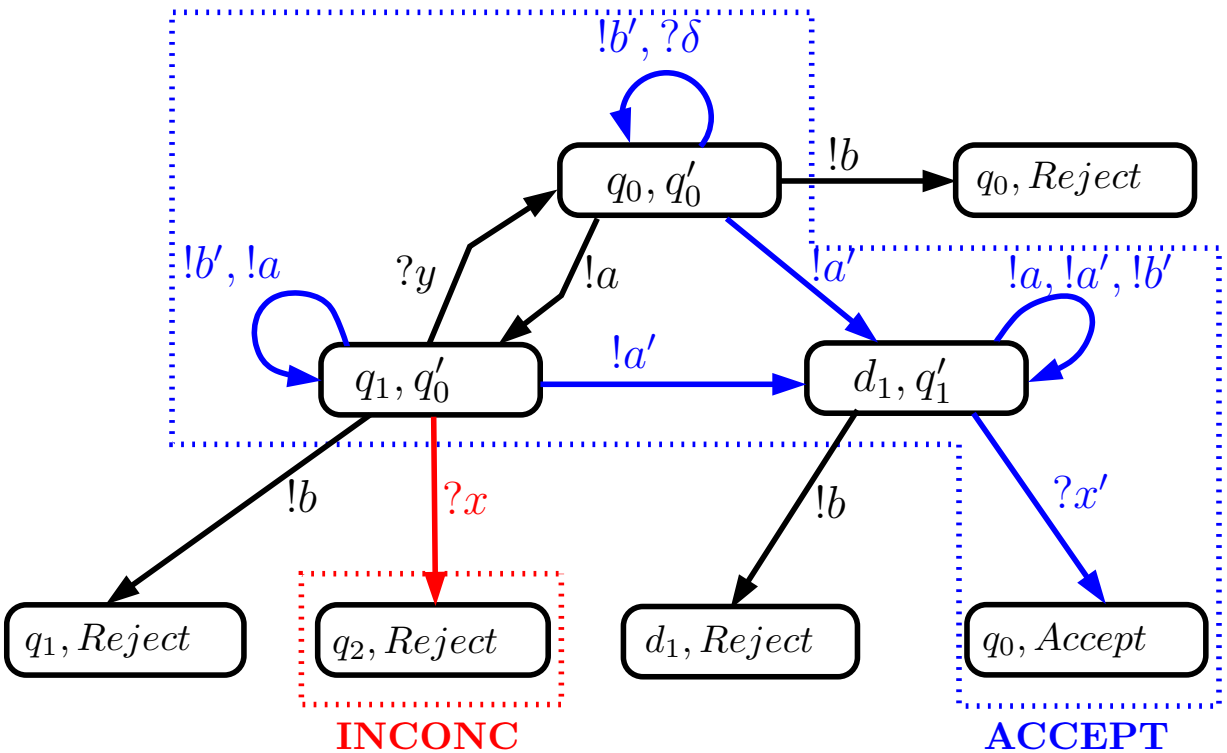
- Le graphe du test de robustesse RTG décrit tous les tests possibles correspondant à un objectif de test de robustesse RTP



Graphe du test de robustesse *RTG*

TRACOR : Graphe du test de robustesse RTG

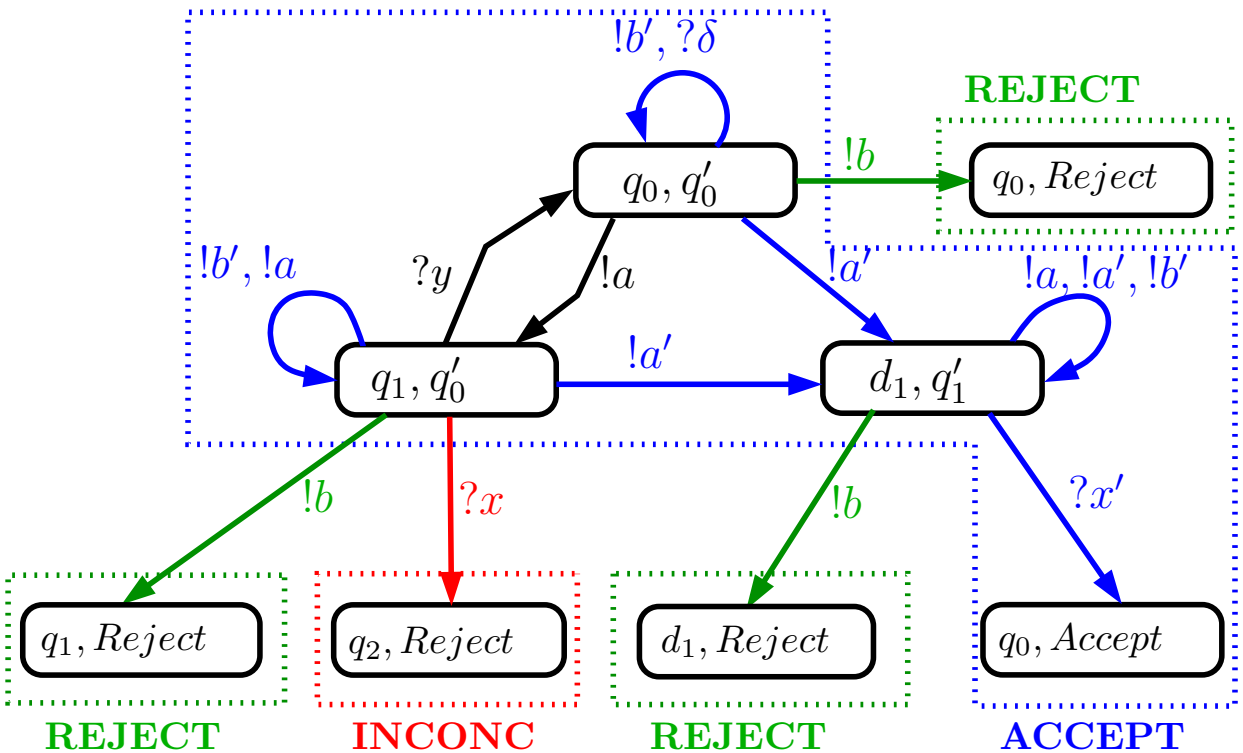
- Le graphe du test de robustesse RTG décrit tous les tests possibles correspondant à un objectif de test de robustesse RTP



Graphe du test de robustesse *RTG*

TRACOR : Graphe du test de robustesse RTG

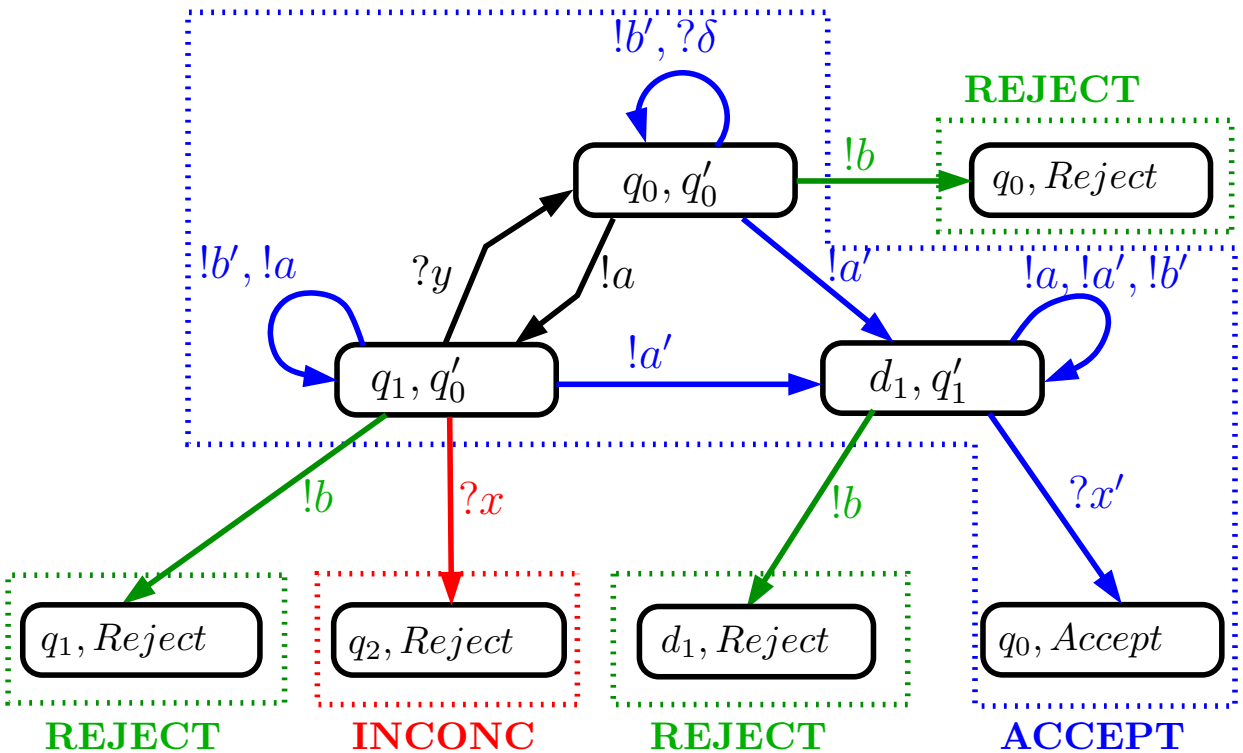
- Le graphe du test de robustesse RTG décrit tous les tests possibles correspondant à un objectif de test de robustesse RTP



Graphe du test de robustesse *RTG*

TRACOR : Graphe du réduit du test de robustesse RRTG

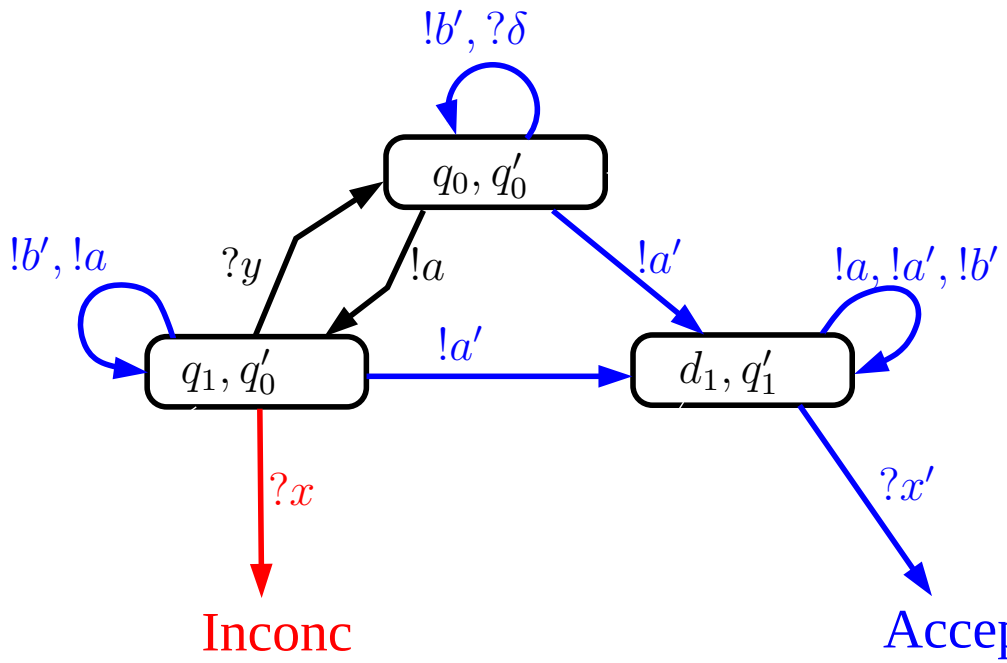
- Le graphe réduit du test de robustesse RRTG décrit seulement les tests acceptés par l'objectif de test de robustesse RTP



Graphe du test de robustesse *RTG*

TRACOR : Graphe du réduit du test de robustesse RRTG

- Le graphe réduit du test de robustesse RRTG décrit seulement les tests acceptés par l'objectif de test de robustesse RTP

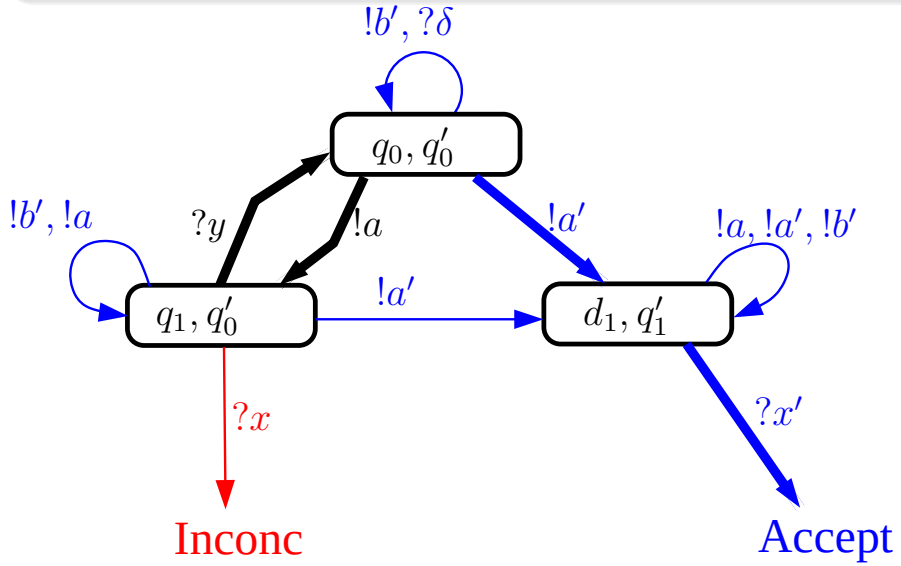


Graphe réduit du test de robustesse $RRTG$

TRACOR : Cas de test de Robustesse (RTC)

Règles de construction

- Trois verdicts (**Accept**, **Inconc**, **Fail**)
- Dans tout état : soit une sortie, soit toutes les entrées
- Un état de réception doit être complète en entrée
- La couleur de RTC doit être différente de celle de S (noire)

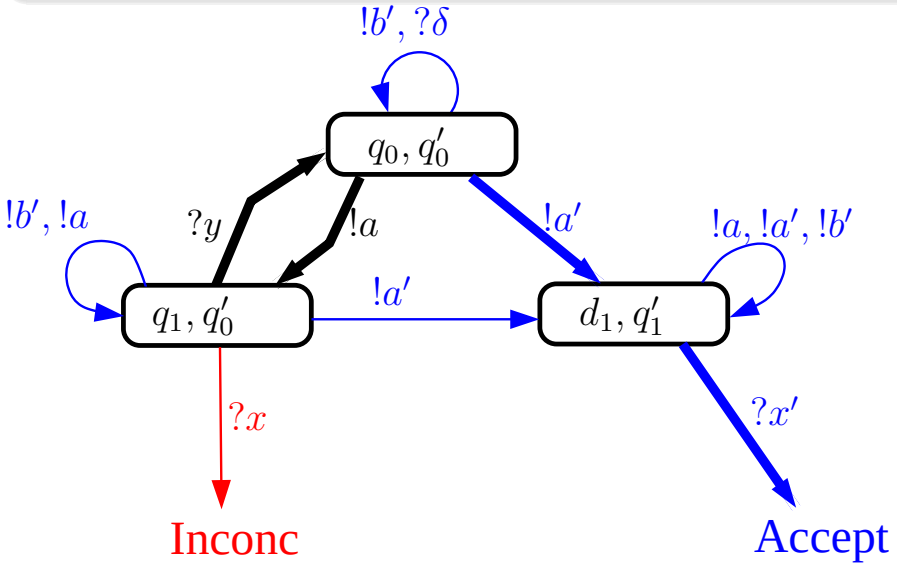


Graphe réduit du test de robustesse

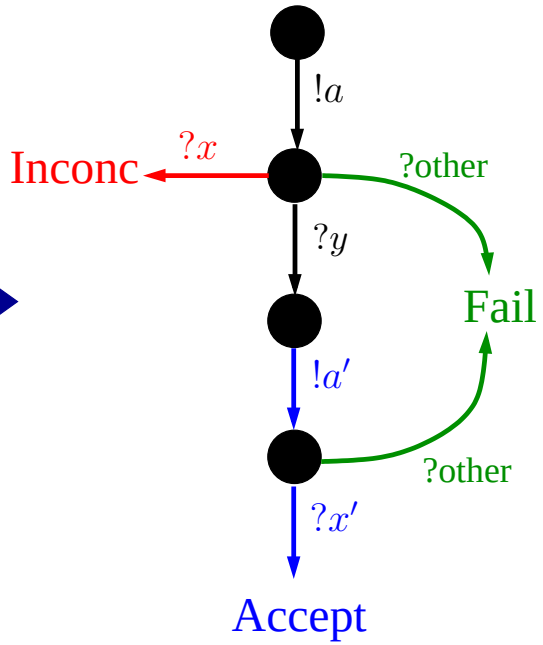
TRACOR : Cas de test de Robustesse (RTC)

Règles de construction

- Trois verdicts (**Accept**, **Inconc**, **Fail**)
- Dans tout état : soit une sortie, soit toutes les entrées
- Un état de réception doit être complète en entrée
- La couleur de RTC doit être différente de celle de S (noire)



Graphe réduit du test de robustesse



Cas de test de robustesse

Méthode TRACON [10]

Objectifs

- Aléas contrôlables non représentables
- Aléas **commandables** par **un contrôleur d'aléas**
- Intégration de sorties acceptables

[10] F. SAAD KHORCHEF, X. DELORD. Une méthode pour le test de robustese adaptée aux protocoles de communication, CFIP 2005, Hermès, Bordeaux.

Méthode TRACON [10]

Objectifs

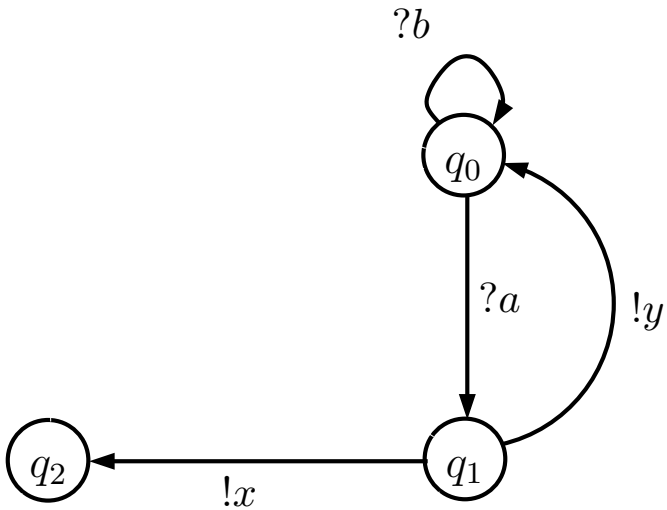
- Aléas contrôlables non représentables
- Aléas **commandables** par **un contrôleur d'aléas**
- Intégration de sorties acceptables

- **Phase 1** : Augmentation de la spécification :
  1. Ajout de silence
  2. Intégration de sorties acceptables
  3. Mise à jour de silence et déterminisation
- **Phase 2** : Génération des cas de test de robustesse

[10] F. SAAD KHORCHEF, X. DELORD. Une méthode pour le test de robustese adaptée aux protocoles de communication, CFIP 2005, Hermès, Bordeaux.

TRACON : augmentation de la spécification

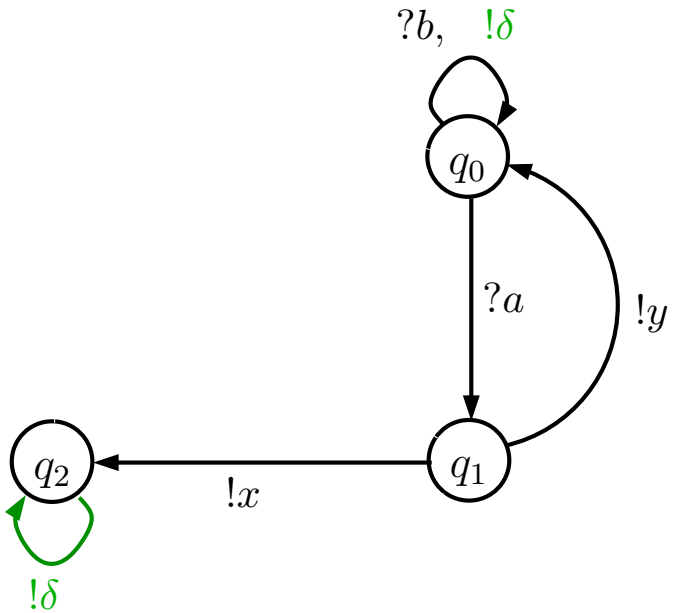
- Ajout de silence : boucles étiquetées par $!\delta$ dans chaque état de silence



Spécification nominale S

TRACON : augmentation de la spécification

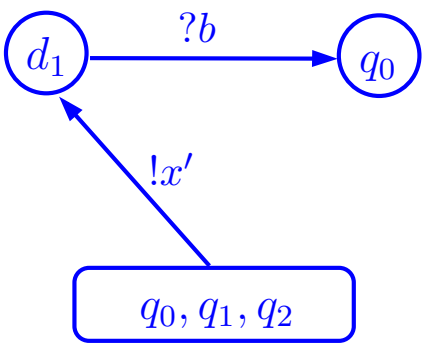
- Ajout de silence : boucles étiquetées par $!\delta$ dans chaque état de silence



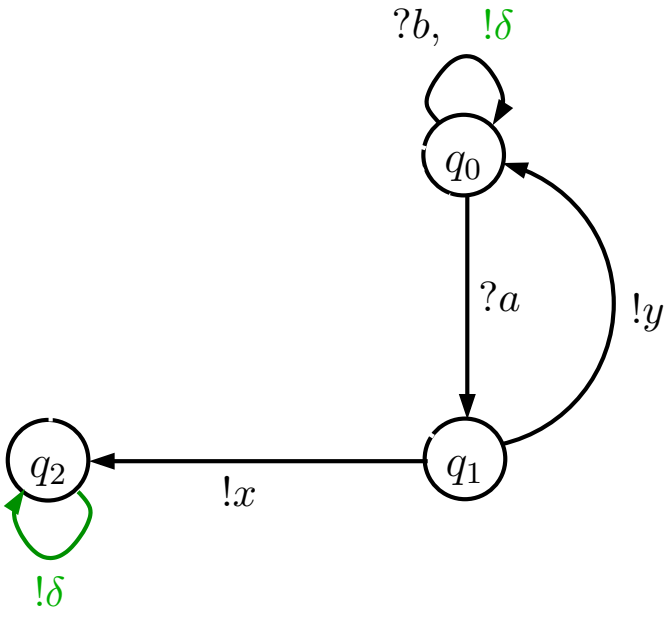
Automate suspendu S^{δ}

TRACON : augmentation de la spécification

- Intégration d'états dégradés et transitions du meta-graphe de sorties acceptables



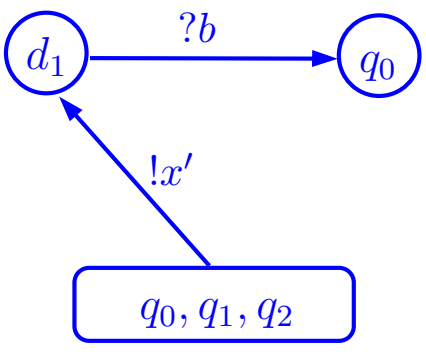
Meta-graphe de sorties acceptables



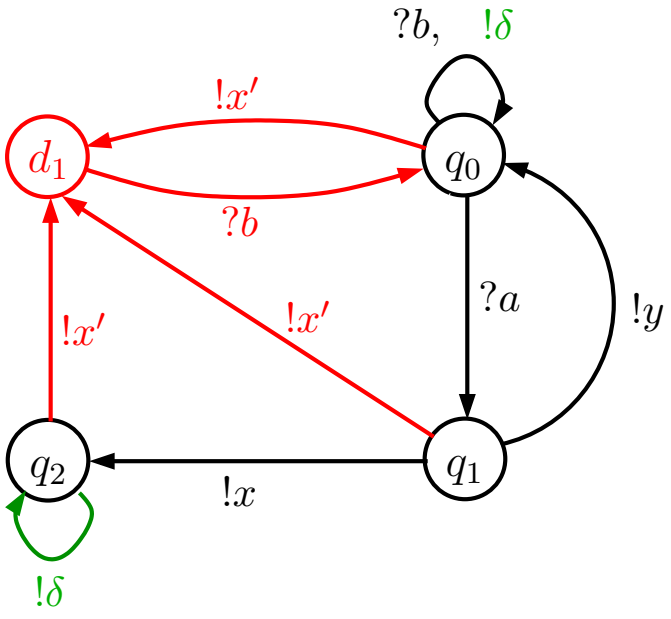
Automate suspendu S^{δ}

TRACON : augmentation de la spécification

- Intégration d'états dégradés et transitions du meta-graphe de sorties acceptables



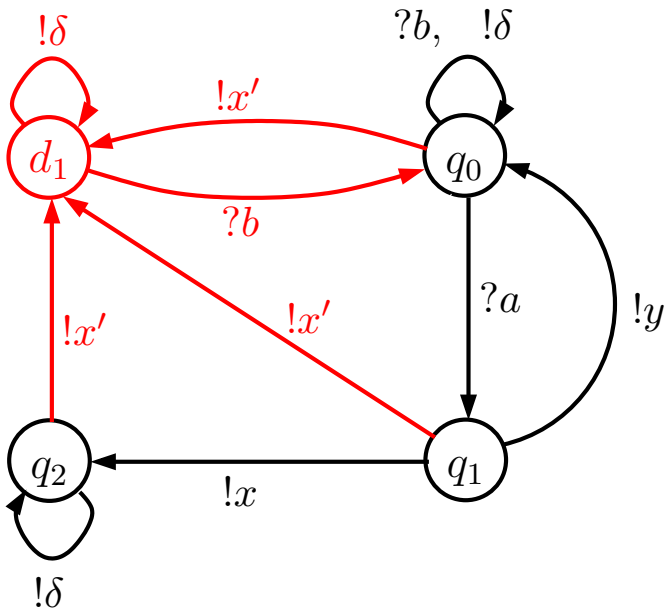
Meta-graphe de sorties acceptables



$S' = S^{\delta}$ avec sorties acceptables

TRACON : augmentation de la spécification

- Mise à jour de silence et déterminisation.



Spécification semi-augmentée S'_A

- **Spécification Semi-augmentée** (S'_A) décrit le comportement du système en présence d'aléas contrôlables et non représentables.
- S'_A est coloriée avec **deux couleurs**

TRACON : Génération des tests de robustesse

Principe

- Référence : spécification semi-augmentée (S'_A) + ***Robust***
- Cas de test incluant les aléa.
- Cas de test : interactions entre le testeur et l'IUT, et le testeur et le contrôleur d'aléas.

TRACON : Génération des tests de robustesse

Principe

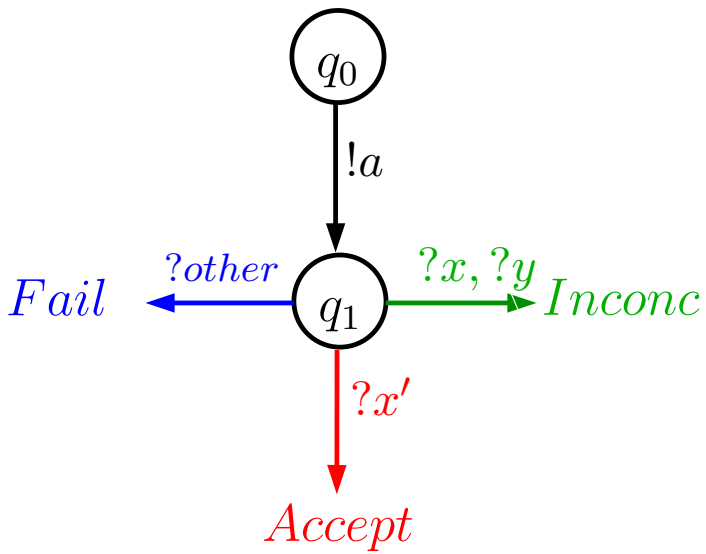
- Référence : spécification semi-augmentée (S'_A) + ***Robust***
- Cas de test incluant les aléa.
- Cas de test : interactions entre le testeur et l'IUT, et le testeur et le contrôleur d'aléas.

Méthode proposée

1. Génération d'un cas de test de robustesse non contrôlable
2. Construction de graphe des cas de test de robustesse contrôlables
3. Sélection d'un cas de test de robustesse contrôlable

TRACON : Génération d'un RTC non contrôlable

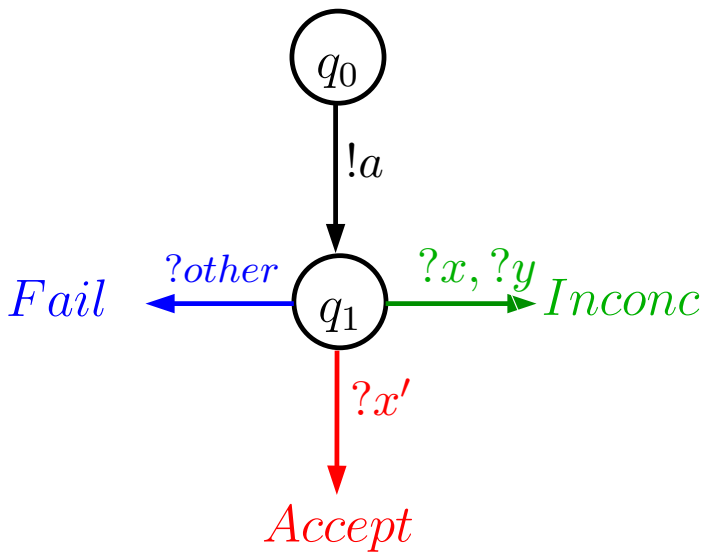
- A partir d'un objectif de test de robustesse RTP et la spécification semi-augmentée S'_A, on applique les mêmes étapes de la méthode TRACOR pour générer un RTC.



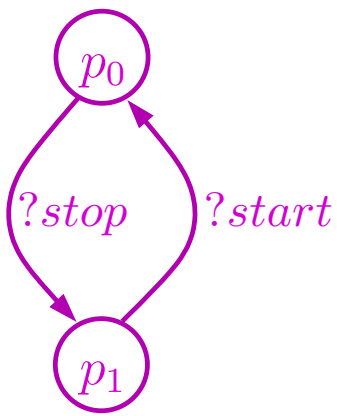
RTC non contrôlable

TRACON : Génération d'un RTC non contrôlable

- Le contrôleur d'aléas (HC) est un IOLTS permettant de démarrer et d'arrêter l'exécution d'un aléa non représentable à l'aide des commandes **start** et **stop**



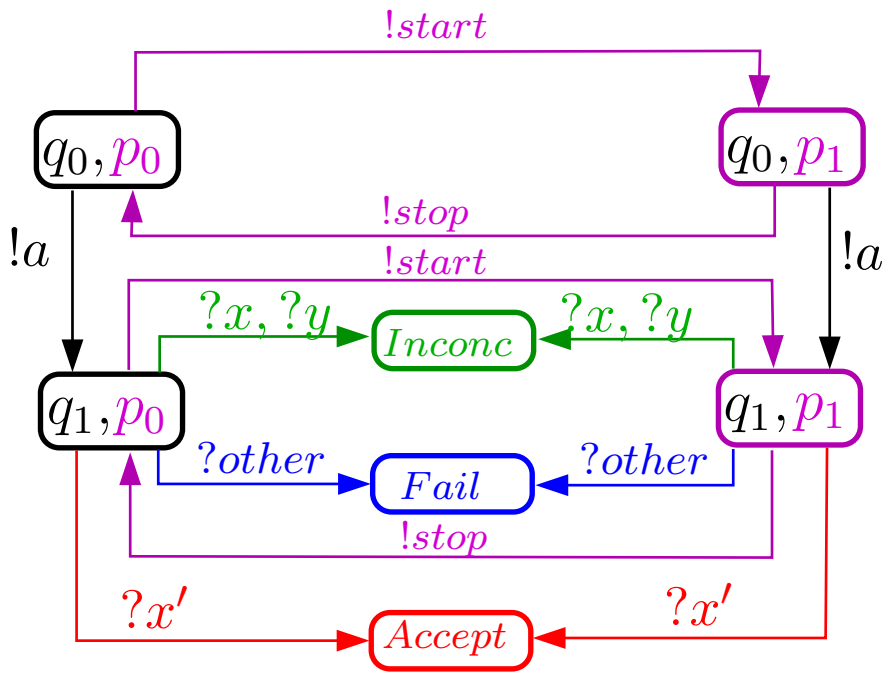
RTC non contrôlable



Contrôleur d'aléas

TRACON : Graphe des RTC contrôlables

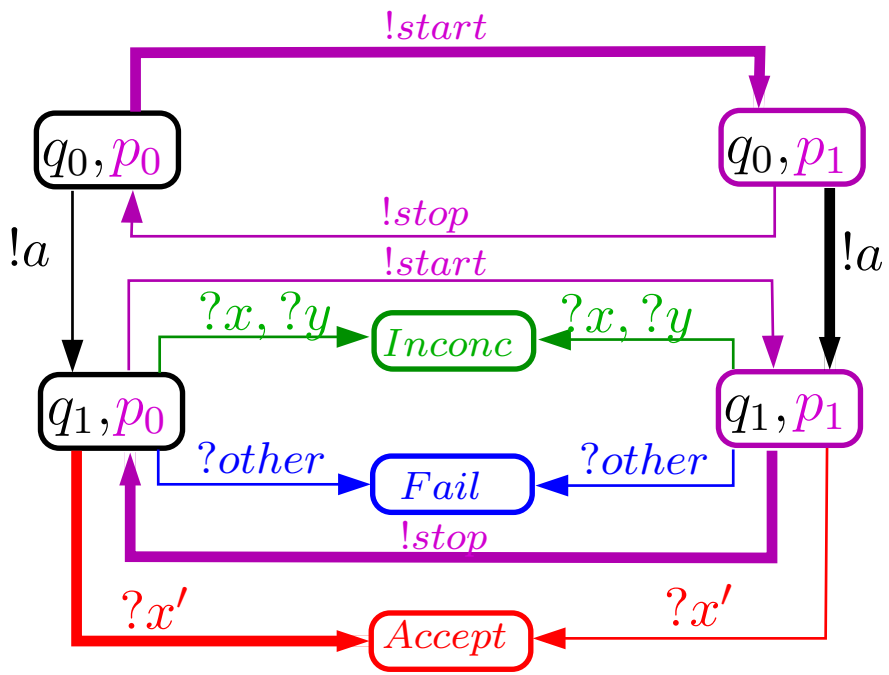
▶ Le graphe des cas de test de robustesse contrôlables CRTCG décrit toutes les interactions possibles entre le testeur et l'IUT et entre le testeur et le contrôleur d'aléas.



CRTCG

TRACON : Sélection d'un RTC contrôlable

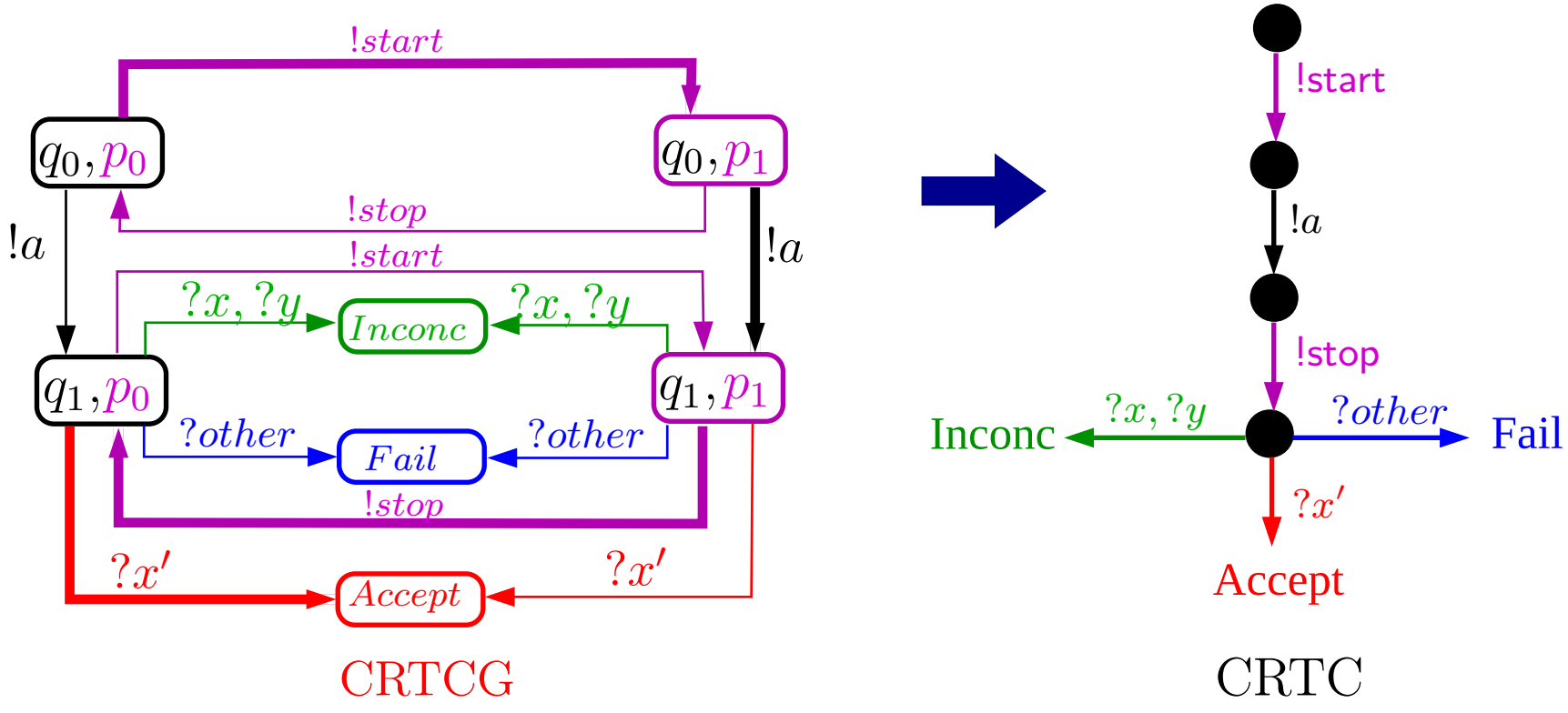
- Un cas de test de robustesse contrôlables CRTC est un sous graphe de CRTCG permettant d'interdire, dans tout état, le choix entre deux sorties ou entre sorties et entrées



CRTCG

TRACON : Sélection d'un RTC contrôlable

- Un cas de test de robustesse contrôlables CRTC est un sous graphe de CRTCG permettant d'interdire, dans tout état, le choix entre deux sorties ou entre sorties et entrées



Plan

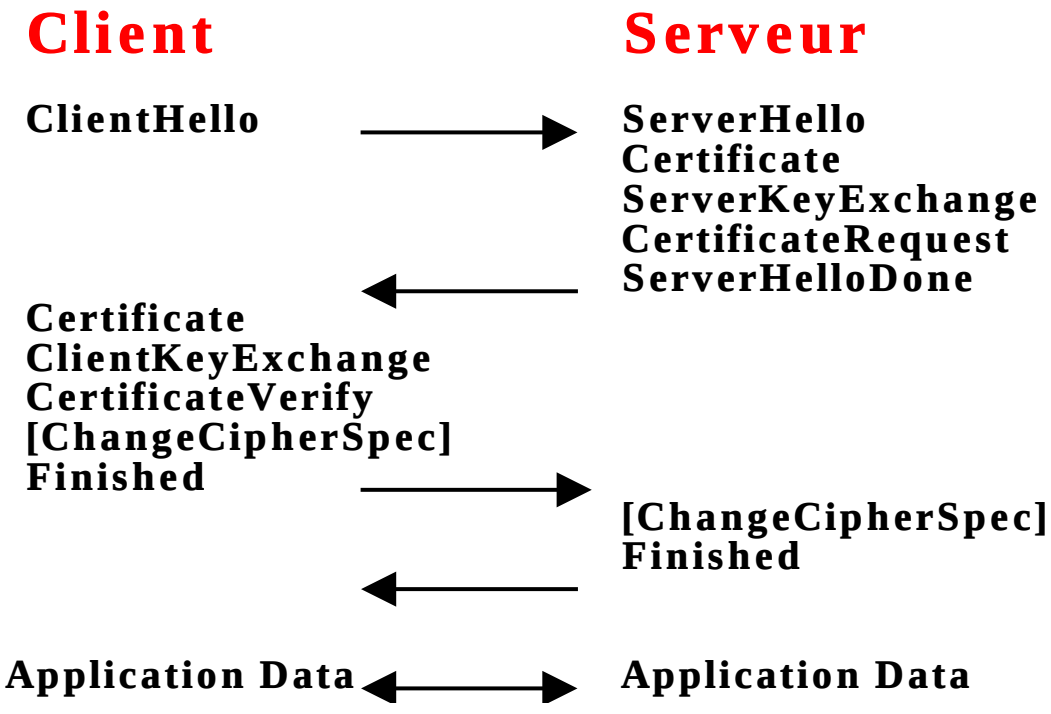
L'outil RTCG

RTCG [5] : Robustness Test Case Generator

- Automatisation des méthodes TRACON et TRACOR
- Spécifications : SDL ou DOT
- Cas de test : TTCN-3 et XML
- Représentation graphique des résultats (GraphViz)

[5] F. SAAD KHORCHEF, A. ROLLET and R. CASTANET. A Framework and a Tool for Robustness Testing of communicating Software, ACM SAC 2007 (accepted paper)

Le protocole SSL Handshake



Expérimentation avec TGSE

- spécification nominale : RFC 2246 ;
- spécification augmentée : 20 états et 176 transitions ;

1. **Entrées invalides (omises dans RFC 2246)** [10] :
   - UNSUPPORTED-AUTHENTICATION-TYPE-ERROR
   - UNEXPECTED-MESSAGE-ERROR
2. **Entrées inopportunes**
3. **Comportement acceptable** :
   1. fermeture de connexion (CLOSE-CONNECTION) en cas de réception d'une entrée invalide
   2. ignorer la réception d'entrées inopportunes (boucles étiquetées par les entrées inopportunes dans tout état)

[10] J. Bradley and N. Davies, "Analysis of The SSL Protocol", *Technical Report CSTR-95-021, Communications Research Group, University of Bristol*, 1995

Expérimentation avec TGSE [6]

- **RTP1** : fermeture de connexion en cas de détection d'une anomalie de certificat
- **RTP2** : fermeture de connexion en cas d'anomalie au niveau des suites de chiffrement (cipher suite)
- **RTP3** : fermeture de connexion en cas de réception d'un message d'erreur inattendu

[6] F. SAAD KHORCHEF, I. BERRADA, A. ROLLET and R. CASTANET. "Automated Robustness Testing for Reactive Systems : Application to Communicating Protocols", I2CS 2006, LNCS, Neuchâtel.

Expérimentation avec TGSE [6]

- **RTP1** : fermeture de connexion en cas de détection d'une anomalie de certificat
- **RTP2** : fermeture de connexion en cas d'anomalie au niveau des suites de chiffrement (cipher suite)
- **RTP3** : fermeture de connexion en cas de réception d'un message d'erreur inattendu

Objectif de test de robustesse	RTC size	CPU Time(s)
RTP1	53	0.9618
RTP2	10	0.3599
RTP3	20	0.15797

[6] F. SAAD KHORCHEF, I. BERRADA, A. ROLLET and R. CASTANET. "Automated Robustness Testing for Reactive Systems : Application to Communicating Protocols", I2CS 2006, LNCS, Neuchâtel.

Expérimentation avec RTCG [5]

- Méthode TRACOR
  - Construction automatique de la spécification augmentée
  - Application de la méthode proposée pour la génération des cas de test de robustesse

- **Résultats obtenus avec RTCG**

Propriété	Taille RTC	Temps CPU (ms)
RTP1	11	1.7965
RTP2	14	2.6807
RTP3	19	4.4749

[5] F. SAAD KHORCHEF, A. ROLLET and R. CASTANET. "A Framework and a Tool for Robustness Testing of communicating Software", ACM SAC 2007 (accepted paper)

Méthode TRACON

Méthode TRACON

- Construction automatique de la spécification semi-augmentée
- application de la méthode proposée pour la génération des cas de test de robustesse

Méthode TRACON

Méthode TRACON

- Construction automatique de la spécification semi-augmentée
- application de la méthode proposée pour la génération des cas de test de robustesse

CRTC en TTCN-3

```
text case SSL−CRTC runs on SSL−IUT
{ timer ReponseTimer := 100E−3 ;
  ReponseTimer.start ;
  alt {   []   ReponseTimer.timout
               { setverdict(fail);
                 stop  }
          [] Tester.receive(client−hello);
               { setverdict(pass)};
                 ReponseTimer.stop;
                 Tester.send(server−hello);
                 Tester.send(start);
                 Tester.send(client−master−key);
                 Tester.send(client−finished);
                 ReponseTimer.start ;
                 alt {   []   ReponseTimer.timout
                              { setverdict(inconc);
                                stop  }
                         [] Tester.receive(Server−verify);
                              {   setverdict(pass);
                                  ReponseTimer.stop;
                                  Tester.send(stop);
                                  ReponseTimer.start ;
                                  alt {  ....    }
                         [else]  {  setverdict(fail) ;
                                    stop  }
}}}}
```

Plan

Conclusion et perspectives

Conclusion

- Approche formelle composée de deux méthodes pour la génération des tests de robustesse : méthodes TRACOR et TRACON
- Implémentation de l'approche proposée dans l'outil RTCG
- Une étude de cas sur les protocoles SSL Handshake et TCP

Perspectives

- Utilisation des RTPs acycliques (en cours)
- Robustesse de systèmes complexes (passage à l'échelle)
- Test de robustesse des systèmes temps-réel (en cours)
- Test de robustesse symbolique