

Robustesse des systèmes quantitatifs : vérification et synthèse

Ocan Sankur

Université Libre de Bruxelles

Candidature : Poste de CR2, CNRS

Centres : IRISA (Rennes), IRCCyN, LINA (Nantes)

Mon parcours



Juin 2013 -

Post-doc à l'**Université Libre de Bruxelles**, Belgique



Précédemment :

2010-2013 Thèse au **LSV, ENS Cachan**

2007-2010 Licence-Master **ENS Ulm**

Master parisien de recherche en informatique

2009 Séjour de 6 mois à **Brown University**



- 2005 Istanbul



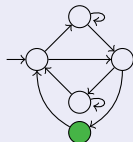
Candidature : IRISA (Rennes), IRCCyN et LINA (Nantes)

Méthodes formelles

Assurer la **correction** des systèmes informatiques est difficile :
par ex. les systèmes embarqués : contraintes temps réel, incertitudes

Solution : méthodes formelles

Model checking



\models ?



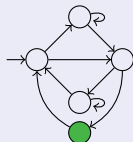
est accessible

Méthodes formelles

Assurer la **correction** des systèmes informatiques est difficile :
par ex. les systèmes embarqués : contraintes temps réel, incertitudes

Solution : méthodes formelles

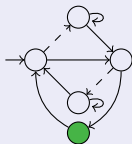
Model checking



$\models ?$

● est accessible

Synthèse de contrôleur



$\parallel \boxed{?} \models ?$

● est accessible

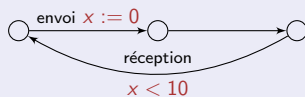
Méthodes formelles

Assurer la **correction** des systèmes informatiques est difficile :
par ex. les systèmes embarqués : contraintes temps réel, incertitudes

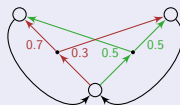
Plus récent :

Systèmes quantitatifs

Automates temporisés



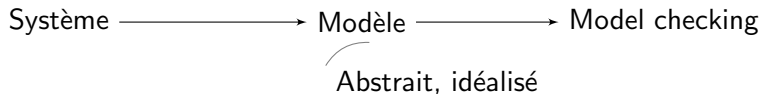
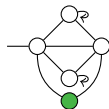
Processus de décision markoviens



Formalismes standards pour les systèmes temporisés et probabilistes

Robustesse dans le model checking

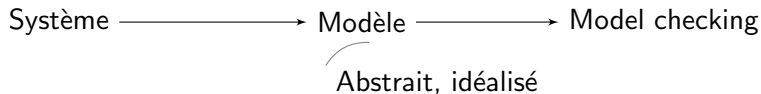
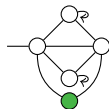
Model checking :




► Vérification des comportements *nominaux*

Robustesse dans le model checking

Model checking :



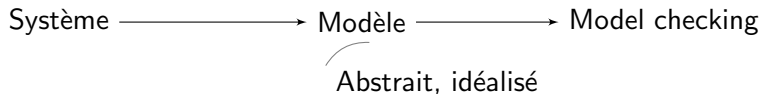
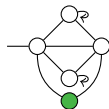
► Vérification des comportements *nominaux*

Par exemple : Les horloges 


- Modèle idéalisé : précision infinie
- Système réel : précision limitée

Robustesse dans le model checking

Model checking :



► Vérification des comportements *nominaux*

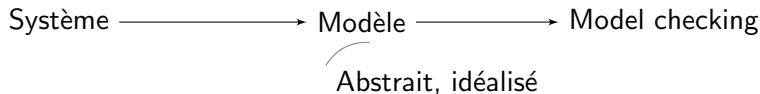
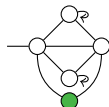
Par exemple : Les horloges 

- Modèle idéalisé : précision infinie
- Système réel : précision limitée

correction du modèle idéalisé \Rightarrow ? correction du système

Robustesse dans le model checking

Model checking :



► Vérification des comportements *nominaux*

Par exemple : Les horloges

- Modèle idéalisé : précision infinie
- Système réel : précision limitée

Robustesse

Le modèle doit pouvoir résister aux petites erreurs

- ① Robustesse: exemple
- ② Travaux antérieurs: systèmes temporisés
- ③ Programme de recherche

Motivation pour la robustesse : Ordonnancement

Scénario



► Temps de terminaison : 6

Vérifiable par un automate temporisé

Motivation pour la robustesse : Ordonnancement

Scénario



► Temps de terminaison : 6

Vérifiable par un automate temporisé

⚠ Anomalie temporelle

“Une baisse de temps d’exécution peut retarder le temps de terminaison”

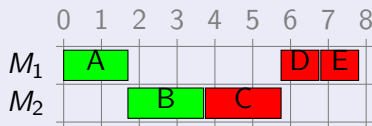
Motivation pour la robustesse : Ordonnancement

Scénario



► Temps de terminaison : 6
Vérifiable par un automate temporisé

⚡ De manière inattendue : A termine en 1.99.



► Temps de terminaison : 7.99

⚠ Anomalie temporelle

“Une baisse de temps d’exécution peut retarder le temps de terminaison”

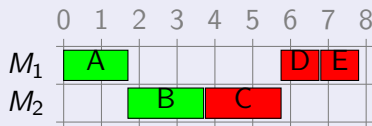
Motivation pour la robustesse : Ordonnancement

Scénario



► Temps de terminaison : 6
Vérifiable par un automate temporisé

⚡ De manière inattendue : A termine en 1.99.



► Temps de terminaison : 7.99

⚠ Anomalie temporelle

“Une baisse de temps d'exécution peut retarder le temps de terminaison”

Conclusion : L'analyse sur un modèle idéaliste n'est pas robuste

Travaux antérieurs :

- Approche par modélisation

Altisen, Tripakis 2005, Chatterjee, Henzinger, Prabhu 2005 + études de cas

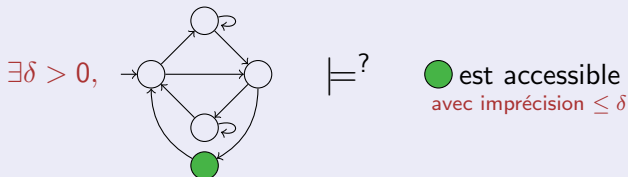
→ souvent source supplémentaire d'explosion d'états

- Approche sémantique

Gupta, Henzinger, Jagadeesan 1997, Puri 1998, De Wulf, Doyen, Markey, Raskin 2004

Ma contribution : Cadre pour la vérification, synthèse et implémentation robuste des automates temporisés

Model checking robuste



FORMATS11, MFCS11, FSTTCS11, TACAS15

Outil: Symrob: analyse *infinitesimale* efficace (TACAS'15)

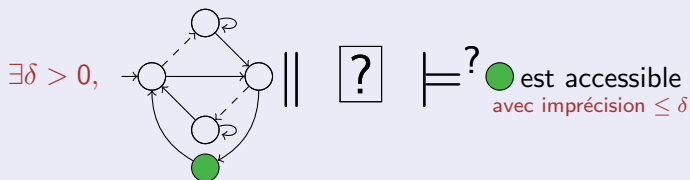
Logiciel libre, intégré avec Uppaal

- Calcule une valeur de δ (pas nécessairement maximal).
- Plusieurs études de cas classiques: efficacité comparable au model checking exacte

Robustesse des systèmes temporisés

Model checking robuste

Synthèse de contrôleur robuste



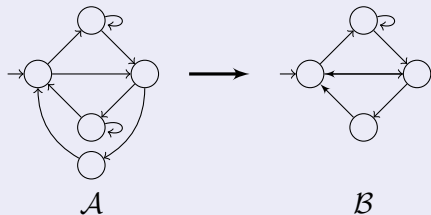
ICALP12, CONCUR13, FORMATS13

Robustesse des systèmes temporisés

Model checking robuste

Synthèse de contrôleur robuste

Implémentation robuste



$$\exists \delta > 0 \quad \mathcal{B} \sim \mathcal{A}$$

|
avec imprécision $\leq \delta$

Shrinktech : Outils d'implémentation robuste

Logiciel libre, intégré avec Kronos

Inform. and Comput., FSTTCS11, CONCUR11

CAV 2013 (Tool paper)

→ Synthèse de $\sim 10^5$ paramètres

Développer une théorie **robuste** de la vérification formelle et de synthèse pour les systèmes quantitatifs

Algorithmes efficaces et outils

Garantir la spécification même si le modèle n'est pas exacte

- Tolérance aux perturbations:
 - ▶ Systèmes temporisés: imprécisions temporelles, déviations d'horloges
 - ▶ Systèmes probabilistes: imprécisions dans les probabilités
- Tolérance à un environnement imprécis

Quelques fonctionnalités recherchées:

- **Analyse de sensibilité:** quantifier les perturbations *maximales* tolérées par un système
- **Mesures quantitatives:** quantifier la robustesse d'un système par la probabilité d'erreur, et le *temps moyen à l'erreur*
- **Compositionnalité:** garantir la robustesse à partir de celle des composantes

But: Outils de nouvelle génération pour la vérification et synthèse robuste
Efficacité comparable aux méthodes existantes

Projet: Systèmes temporisés

Quelques fonctionnalités recherchées:

- **Analyse de sensibilité:** quantifier les perturbations *maximales* tolérées par un système
- **Mesures quantitatives:** quantifier la robustesse d'un système par la probabilité d'erreur, et le *temps moyen à l'erreur*
- **Compositionnalité:** garantir la robustesse à partir de celle des composantes

Quelques pistes court-moyen terme

- Analyse infinitésimale (cf thèse) → analyse maximale
- Analyse des systèmes distribués
- Stabilité pour la synthèse
- Application: système d'accompagnement musical Antescofo (Ircam)

IRISA (SUMO) :

- Test et *enforcement* de systèmes temp.
- Systèmes distribués, approche compositionnelle
- Systèmes temporisés stochastiques
- Alstom Transport : régulation robuste des horaires de trains

Robustesse, réalisabilité,
implémentabilité

Déviations d'horloges,
robustesse compositionnelle

+ Participation commune à l'ANR ImpRo 2011-2014

IRISA (SUMO) :

- Test et *enforcement* de systèmes temp.
- Systèmes distribués, approche compositionnelle
- Systèmes temporisés stochastiques
- Alstom Transport : régulation robuste des horaires de trains

Robustesse, réalisabilité,
implémentabilité

Déviations d'horloges,
robustesse compositionnelle

+ Participation commune à l'ANR ImpRo 2011-2014

IRCCyN (STR) - LINA (Aelos):

- Vérification symbolique des systèmes temporisés
- Synthèse de paramètres
- Systèmes distribués

Algorithmes symboliques,
Algorithmes robustes

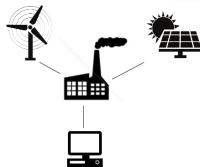
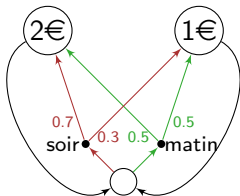
Déviations d'horloges

+ ANR PACS 2014-2018

Projet: systèmes probabilistes

Approche classique: Optimiser la performance en moyenne
le coût en moyenne, la probabilité d'atteindre un état etc.

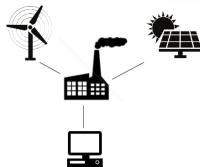
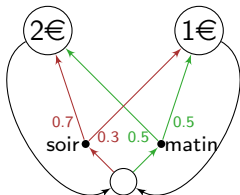
Exemple



Projet: systèmes probabilistes

Approche classique: Optimiser la performance en moyenne
le coût en moyenne, la probabilité d'atteindre un état etc.

Exemple



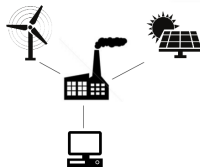
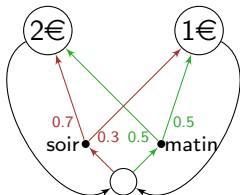
Dichotomie

- modèles probabilistes: garanties en moyenne → performance
- modèles non-déterministes: garanties strictes → spéc. critique

Projet: systèmes probabilistes

Approche classique: Optimiser la performance en moyenne
le coût en moyenne, la probabilité d'atteindre un état etc.

Exemple



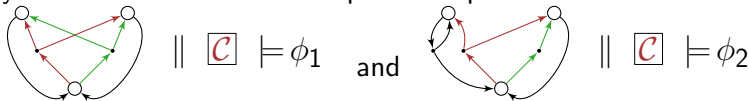
Dichotomie

- modèles probabilistes: garanties en moyenne → performance
- modèles non-déterministes: garanties strictes → spéc. critique

But: Synthèse **multi-objectif** avec des garanties **strictes** et en **moyenne**.

Synthèse pour scénarios multiples

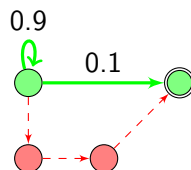
Plusieurs scénarios possibles :

Synthétiser un contrôleur unique \mathcal{C} tel que“Performance garantie **pour tout** scénario”

Projet: Systèmes probabilistes (suite)

Quelques objectifs

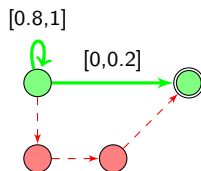
- 1 Scénarios multiples + adversaire antagoniste
itération de valeur, objectifs quantitatifs,
- 2 MDP à intervalles : incertitude sur les probabilités
garanties pour **toute** réalisation



Projet: Systèmes probabilistes (suite)

Quelques objectifs

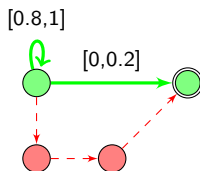
- 1 Scénarios multiples + adversaire antagoniste
itération de valeur, objectifs quantitatifs,
- 2 MDP à intervalles : incertitude sur les probabilités
garanties pour **toute** réalisation



Projet: Systèmes probabilistes (suite)

Quelques objectifs

- 1 Scénarios multiples + adversaire antagoniste
itération de valeur, objectifs quantitatifs,
- 2 MDP à intervalles : incertitude sur les probabilités
garanties pour **toute** réalisation



Long-terme: un cadre pour la synthèse de contrôleurs:

- 1 Garanties strictes: $\phi_1 \wedge \dots \wedge \phi_n$ contre un adversaire
- 2 Optimiser les probabilités: ψ_1, \dots, ψ_m pour tout scénario
- 3 Garantie de performance: coût moyen, coût total multi-dimensionnel

IRISA (SUMO) :

- Diagnostic et opacité probabiliste
- Systèmes à observation partielle
- Approximation des chaînes de Markov
ANR Stoch-MC 2014

Scénarios multiples

IRCCyN & LINA :

- Systèmes probabilistes à contraintes
- Contrats probabilistes

MDP à intervalles

Candidature : IRISA (SUMO), IRCCyN (STR), LINA (Aelos)

● Collaborations internationales

- ▶ Jean-François Raskin (ULB)

[FSTTCS14, SYNT14, VMCAI15], 3 soumissions: CAV, ICALP

Premier prix à la *compétition de synthèse de contrôleur* LICS-CAV'14

- ▶ Kim G. Larsen (Aalborg University, Danemark) [CONCUR11]
- ▶ Stefan Göller (LSV, CNRS - anciennement Bremen U.) [CONCUR12]
- ▶ Krishnendu Chatterjee (IST Austria, Autriche)
- ▶ S. Akshay, A. Trivedi (IIT Bombay, Inde)

● Autres collaborations en France

- ▶ Pierre-Alain Reynier (Uni. Aix-Marseille) [CONCUR13-14]
- ▶ Florent Jacquemard (INRIA - IRCAM), Études de cas en musique
- ▶ Claire Mathieu (ENS Ulm & CNRS - Brown University) [STACS10]

● Responsabilités

- ▶ **Comité de programme FORMATS14**,
- ▶ Relectures Inform. and Comput., TCS, ICALP, STACS, LICS, ...

Candidature : IRISA (SUMO), IRCCyN (STR), LINA (Aelos)

● Collaborations internationales

- ▶ Jean-François Raskin (ULB)

[FSTTCS14, SYNT14, VMCAI15], 3 soumissions: CAV, ICALP

Premier prix à la *compétition de synthèse de contrôleur* LICS-CAV'14

- ▶ Kim G. Larsen (Aalborg University, Danemark) [CONCUR11]
- ▶ Stefan Göller (LSV, CNRS - anciennement Bremen U.) [CONCUR12]
- ▶ Krishnendu Chatterjee (IST Austria, Autriche)
- ▶ S. Akshay, A. Trivedi (IIT Bombay, Inde)

● Autres collaborations en France

- ▶ Pierre-Alain Reynier (Uni. Aix-Marseille) [CONCUR13-14]
- ▶ Florent Jacquemard (INRIA - IRCAM), Études de cas en musique
- ▶ Claire Mathieu (ENS Ulm & CNRS - Brown University) [STACS10]

● Responsabilités

- ▶ **Comité de programme FORMATS14**,
- ▶ Relectures Inform. and Comput., TCS, ICALP, STACS, LICS, ...

Merci