Estimation du degré d'opacité d'un système à secret

Encadrants

Eric Fabre (Contact)
Mail : fabre@irisa.fr
Téléphone : 02 99 84 73 26

Herve Marchand
Mail : herve.marchand@inria.fr

Structure d'accueil

Ville : Rennes
Désignation de l'établissement : Laboratoire
Nom de l'établissement : INRIA
Équipe : SUMO

Mots-clés :

- automate stochastique
- opacité
- diagnosticabilité

Description :

On considère un système sur lequel une propriété de secret est définie. Ce système est partiellement ouvert : pour ses interactions avec l'extérieur, il produit des événements observables, voire accepte des entrées, ce qui permet de deviner partiellement quels sont ses comportements internes. Il s'agit alors de déterminer si le "secret" du système est préservé lors de ses interactions (problème de l'opacité), et de mesurer la fuite d'information sur ce secret (problème de la quantification de l'opacité).

Formellement, on se place dans le cadre des systèmes à événements discrets, modélisés par un automate, un automate stochastique (ou une chaîne de Markov), un automate à poids... Dans un premier temps, on pourra supposer que le système n'accepte pas d'entrées, mais exécute une trajectoire cachée dont certaines transitions produisent des observables. La propriété secrète est exprimée par une partition sur l'ensemble des trajectoires. On dit que le secret est révélé si, au vu des observations collectées, l'observateur peut dire à quel ensemble appartient la trajectoire cachée. Au contraire, si l'ambiguité demeure dans tous les cas, le système est dit opaque. Dans de nombreux cas toutefois, le système pourra être faiblement opaque, dans le sens où, vu les observables, il est beaucoup plus vraisemblable que la trajectoire cachée soit dans un groupe plutôt que dans l'autre. Bien que le système soit opaque, il y a donc fuite d'information sur le secret : l'observateur n'obtient pas tous les bits

manquants pour découvrir la propriété secrète, mais il en obtient tout de même une partie. Lorsque le système peut accepter des entrées, on voit immédiatement qu'un problème de stratégie se pose, pour collecter le maximum d'informations sur le secret en pilotant partiellement le système.

L'objectif de ce stage est de formaliser correctement cette (ou ces) question(s), et de proposer une solution algorithmique pour estimer le degré d'opacité d'un système. Selon les progrès réalisés, on pourra aller jusqu'au problème de calcul d'une stratégie optimale pour extraire le maximum d'information d'un système ouvert. On s'appuiera pour cela sur un ensemble de résultats classiques pour mesurer des propriétés sur les automates à poids ou les automates stochastiques (notamment pour mesurer les volumes d'ensembles de trajectoires), et eventuellement sur la théorie de l'information.

Bibliographie :

- B. Bérard, J. Mullins, M. Sassolas : "Quantifying Opacity," 7th International Conference on Quantitative Evaluation of Systems (QEST 2010), Williamsburg, Virginia, USA, pp. 263-272, 2010.
- Corinna Cortes, Mehryar Mohri, Ashish Rastogi, and Michael Riley : "On the computation of the relative entropy of probabilistic automata," International Journal of Foundations of Computer Science, 19(1):219-242, 2008.