Séparation d'automates finis

Application à l'abstraction par prédicats de systèmes infinis

Thématique : Théorie des automates

Laboratoire : Laboratoire Bordelais de Recherche en Informatique (LaBRI)
UMR CNRS 5800 – Université Bordeaux 1 – ENSEIRB
351, cours de la Libération, 33405 Talence Cedex, FRANCE

Équipe : Modélisation, Vérification et Test de Systèmes Informatisés (MVTsi)

Encadrants : Frédéric Herbreteau (`Frederic.Herbreteau@labri.fr`)
Jérôme Leroux (`Jerome.Leroux@labri.fr`)
Grégoire Sutre (`Gregoire.Sutre@labri.fr`)

Directeur de laboratoire : Serge Dulucq (`Serge.Dulucq@labri.fr`)

Présentation générale du domaine

Dans des secteurs d'activités tels que les transports, l'énergie, etc., les systèmes informatisés gèrent des tâches de plus en plus complexes et critiques (au sens où la moindre défaillance peut être catastrophique). Il est donc indispensable de s'assurer, au préalable, que de tels systèmes vont se comporter correctement, même (et surtout !) dans les cas imprévus. C'est le but des méthodes formelles de spécification et de vérification.

Ce stage se situe dans le cadre de la *vérification par abstraction*. Cette approche, qui trouve ses origines dans le cadre général de l'*interprétation abstraite*, procède généralement comme suit : afin de montrer qu'une propriété (de sûreté) est satisfaite par le système considéré, on se contente de montrer qu'elle est satisfaite par une *abstraction* du système, c'est-à-dire un modèle de taille réduite dont les comportements "couvrent" ceux du système considéré. La construction (et le raffinement) automatique d'abstractions a fait récemment l'objet de recherches intensives.

Objectifs du stage

Afin de construire de façon quasi-automatique des abstractions, Graf et Saïdi ont proposé en 1997 la méthode d'*abstraction par prédicats*. L'abstraction est ici obtenue automatiquement à partir d'un ensemble de *prédicats*, qui tentent de capturer les aspects essentiels du système. Si l'abstraction ainsi construite est trop grossière, alors l'ajout de prédicats permet de la *raffiner*. Les techniques de *raffinement guidé par contre-exemple* permettent de découvrir automatiquement de nouveaux prédicats en exploitant les (faux) contre-exemples fournis par l'étape de vérification.

Ce stage s'inscrit dans le projet Persée de l'ACI Sécurité Informatique, où on cherche notamment à développer des techniques de raffinement d'abstractions pour la vérification de *systèmes infinis hétérogènes* (c'est-à-dire des automates finis munis de variables entières, de files de communication, etc.). Ici, les prédicats sont remplacés par des *automates finis* (dénotant des langages réguliers). Afin de garder une approche efficace, on souhaite simplifier les automates obtenus lors du raffinement guidé par contre-exemple. Cela se traduit formellement par le problème de *séparation* suivant : étant donnés deux automates $\mathcal{A}$ et $\mathcal{B}$ tels que $L(\mathcal{A}) \subseteq L(\mathcal{B})$, trouver un automate "simple" $\mathcal{C}$ tel que $L(\mathcal{A}) \subseteq L(\mathcal{C}) \subseteq L(\mathcal{B})$.

L'objectif du stage consiste dans un premier temps à développer des techniques de séparation pour les automates finis. Dans un deuxième temps, on appliquera ces techniques au raffinement d'abstraction de systèmes infinis hétérogènes.

Compétences espérées

Connaissances en théorie des automates et en logique.