Sujet de Stage Master recherche
Approche incrémentale et modulaire pour la vérification de propriétés temporelles linéaires sur les réseaux de Petri

Kais Klai et Laure Petrucci

LIPN, CNRS UMR 7030
Université Paris 13
99 avenue Jean-Baptiste Clément
F-93430 Villetaneuse, France
{kais.klai,laure.petrucci}@lipn.univ-paris13.fr

1 Contexte scientifique et problématique

La mise au point des applications distribuées critiques est un problème complexe pour lequel il est recommandé d'utiliser des techniques de description formelle afin de spécifier sans ambiguité le comportement des applications considérées. Il faut aussi des outils de vérification automatique ou semi-automatique afin de valider le bon fonctionnement de ces applications. L'évolution des systèmes distribués se caractérise par une complexité croissante et un rôle toujours plus critique. La vérification de leurs propriétés est reconnue comme un problème difficile du fait de l'explosion combinatoire de leur espace d'états. Les logiciels orchestrant de tels systèmes doivent réagir correctement et en particulier face aux situations critiques. Les méthodes formelles de spécification de systèmes ont pour objectif d'assurer la fiabilité de ces logiciels, c'est-à-dire leur bonne spécification et l'absence d'erreur. Idéalement, pour concevoir le logiciel d'un système concurrent donné, il faudrait spécifier formellement ce système à l'aide d'un modèle mathématique à partir duquel on pourrait raisonner et vérifier les propriétés attendues. En réalité, ce processus se heurte à plusieurs problèmes d'ordre pratique et théorique. Un premier obstacle apparaît au niveau de la définition du langage de spécification utilisé. Si celui-ci est trop expressif, alors on ne peut pas, mathématiquement, l'analyser automatiquement. Les réseaux de Petri sont reconnus pour être suffisamment expressifs pour décrire la réalité des systèmes, tout en restant raisonnablement analysables. Un second obstacle est l'explosion combinatoire des états possibles des systèmes. Malgré les avancées spectaculaires de la technologie des ordinateurs, il arrive que l'on soit incapable d'analyser intégralement des systèmes par manque d'espace mémoire ou de temps. Lors des deux dernières décennies, plusieurs chercheurs se sont intéressés à ce problème (voir à titre d'exemple [6,1,2,3]) et ont proposé des techniques pour le combattre. Parmi elles, la vérification modulaire représente une approche prometteuse qui tire profit de la modularité intrinsèque dans les systèmes concurrents. En se basant sur le principe de "diviser pour règner", le système est réparti en composants et chacun de ces composants est analysé indépendamment des autres. La vérification du système global est donc déduite de la vérification de ses composants pris séparément.

2 Objectif du stage

Il s'agit d'étudier et implémenter une technique de vérification (présentée dans [4]) pour analyser des réseaux de Petri qui est basée sur une approche incrémentale [1] et des techniques modulaires [5,3]. L'objectif consiste à exploiter à la fois la structure du réseau de Petri modélisant le système et la propriété à vérifier dans le cadre d'une approche modulaire et incrémentale de vérification. Il s'agit d'une approche heuristique dont la mise en œuvre devrait nous permettre de répondre à plusieurs questions intéressantes. Par exemple, étant donnés un modèle de réseaux de Petri et une propriété à vérifier, est-il possible de vérifier la propriété modulairement ? Et si oui quel est, parmi plusieurs schémas de décomposition possibles, celui qui permet de vérifier la propriété avec le moindre coût (en temps et espace mémoire) ?

3 Profil souhaité

Le candidat recherché devra avoir des connaissances de base sur le modèle des réseaux de Petri, sur la logique temporelle linéaire et sur la vérification de systèmes (model-checking). Il devra également maîtriser un language de programmation.

Références

1. S. Haddad, J-M. Ilié, and K. Klai. An incremental verification technique using decomposition of Petri nets. In *Proc. of the IEEE SMC'02 - Systems, Man and Cybernetics, Hammamet, Tunisia*, 2002.
2. Serge Haddad, Jean-Michel Ilié, and Kais Klai. Design and evaluation of a symbolic and abstraction-based model checker. In *ATVA*, volume 3299 of *Lecture Notes in Computer Science*, pages 196–210. Springer, 2004.
3. Kais Klai, Serge Haddad, and Jean-Michel Ilié. Modular verification of Petri nets properties : A structure-based approach. In *FORTE*, volume 3731 of *Lecture Notes in Computer Science*, pages 189–203. Springer, 2005.
4. Kais Klai, Laure Petrucci, and Michel Reniers. An incremental and modular technique for checking LTL-X properties of Petri nets. In *FORTE*, volume 4574 of *Lecture Notes in Computer Science*, pages 280–295. Springer, 2007.
5. Charles Lakos and Laure Petrucci. Modular analysis of systems composed of semiautonomous subsystems. In *4th International Conference on Application of Concurrency to System Design (ACSD 2004), 16-18 June 2004, Hamilton, Canada*, pages 185–196, 2004.
6. L. Petrucci. Design and validation of a controller. In *Proc of the 4th World Multiconference on Systemics, Cybernetics and Informatics (SCI'2000), Orlando, FL, USA*, volume VIII, pages 684–688, 2000.