Département d'Informatique de l'Ecole Normale Supérieure

Traces, Propriétés et Hyperpropriétés

Encadrement & Contact : Xavier RIVAL
e-mail : rival@di.ens.fr
tél : 01 44 32 21 50

Description de l'objet du mémoire :

La vérification de programmes a pour but de s'assurer que des propriétés sémantiques importantes sont satisfaites. On peut citer des propriétés de *sûreté* (qui expriment qu'un certain "mauvais" comportement ne sera jamais observé), de *vivacité* (qui expriment qu'un certain comportement souhaitable sera finalement observé) ou bien des propriétés de *sécurité* (qui expriment par exemple qu'un attaquant ne peut pas déduire des informations confidentielles en observant uniquement des informations publiques). Selon les propriétés concernées, les techniques de vérification qui peuvent être mises en oeuvre ne sont pas les mêmes.

Le but de ce sujet est d'étudier les principales classes de propriétés sémantiques des programmes. Tout d'abord, les *propriétés de traces* [1] incluent la plupart des notions usuelles de correction fonctionnelle (absence d'erreurs, préservation d'invariants, terminaison...), et peuvent être décomposées de manière très naturelle et esthétique à l'aide des notions de sûreté et de vivacité. les propriétés de sécurité ne rentrent pas dans ce cadre, et nécessitent un cadre plus général. La notion d'*hyperpropriété* [2] permet de construire une classification très générale des propriétés de programmes, qui décrit également les propriétés de sécurité classiques, comme l'absence de fuites d'informations, mais aussi des propriétés plus inattendues, comme l'absence de bridage logiciels de systèmes à des fins frauduleuses (affaire de triche aux émissions de véhicules diesel Volkswage).

Références bibliographiques :

1 Bowen Alpern and Fred B. Schneider.
Recognizing Safety and Liveness.
In *Distributed Computing*, 2(3), pages 117–126, 1987.

2 Michael R. Clarkson and Fred B. Schneider.
Hyperproperties.
In *Computer Security Foundations Symposium (CSF)*, pages 51–65, IEEE Computer Society, 2008.