

Titre

Calcul automatisé de mesures de terminaison

Lieu

Laboratoire VERIMAG, Université Joseph Fourier, Grenoble

Encadrement

Saddek Bensalem et Jean-François Monin

saddek.bensalem@imag.fr jean-francois.monin@imag.fr

Contexte

Dans le contexte de la preuve de programme, les *fonctions de mesure* (ou simplement *mesures*) sont des fonctions dont le codomaine est muni d'un ordre bien fondé. Elles sont un outil puissant pour démontrer la terminaison d'un programme. Ainsi, en théorie des types, où les fonctions définies sont totales par construction, les versions récentes de Coq permettent de définir des fonctions par points fixes au moyen d'une mesure.

Dans un autre domaine, celui des systèmes embarqués et des applications critiques, la preuve de terminaison d'une boucle d'itération dans un programme est tout aussi indispensable pour garantir le bon comportement d'un système. Elle est également nécessaire quand on veut montrer des propriétés temporelles générales sur des systèmes infinis.

Bien que le problème général de la synthèse d'une fonction de mesure soit indécidable, des progrès récents permettent d'automatiser cette tâche, notamment dans le cadre impératif, en la ramenant à la résolution d'un ensemble fini de contraintes locales, dites *conditions de vérification*, analogues à des invariants inductifs. On peut citer principalement, les travaux de A. Bradley, B. Cook, P. Cousot ainsi que Podelski et Rebalchenko, qui ont donné lieu à des méthodes adaptées à différentes classes de boucles d'itérations.

Travail demandé

1. Théorique :
 - synthèse sur les différentes approches proposées ;
 - adaptation de résultats existants au cadre de la programmation fonctionnelle en théorie des types.
2. Pratique :
 - évaluation d'outils : Terminator proposé par B. Cook Microsoft research à Cambridge et Polyrank développé par A. Bradley à Stanford ;
 - connexion de l'un des deux outils cités ci-dessus à Coq pour compléter automatiquement des définitions de fonctions par point fixe à l'intérieur d'une classe non triviale.

Remarque

Possibilité de prolongation en thèse.