ÉCHANGE DE CERTIFICATS DE CALCULS ARITHMÉTIQUES

ÉQUIPE CELTIQUE
IRISA/INRIA RENNES BRETAGNE ATLANTIQUE
FRÉDÉRIC BESSON FLORENT KIRCHNER

MOTS-CLÉS : Méthodes formelles, arithmétique non-linéaire, bases de données, programmation fonctionnelle.

RAHD [3] est un logiciel qui utilise une batterie de techniques hétérogènes pour décider efficacement de la satisfiabilité de formules arithmétiques. En pratique, étant donné un ensemble de relations entre polynômes à coefficients réels, l'outil permet de valider (ou d'invalider) l'existence d'un ensemble de valeurs pour les variables des polynômes, telles que ces relations soient vérifiées. En somme, si l'on se donne $p_{i,j} \in \mathbb{R}[\vec{x}]$ polynômes, et que l'on choisit $\bowtie_{i,j} \in \{=, >, \geq\}$, RAHD résout des formules de la forme :

$$\langle \mathbb{R}, +, -, \times, >, 0, 1 \rangle \models \exists \vec{x} \bigwedge_{i=1}^{c} \bigvee_{j=1}^{l_c} p_{i,j}(\vec{x}) \bowtie_{i,j} 0 \ .$$

Il est particulièrement efficace sur des formules comportant un très grand nombre de variables et de polynômes.

Il faut toutefois noter qu'il est rare qu'un problème purement arithmétique se présente à l'attention des ingénieurs et des scientifiques. Le plus souvent, il ne constituera qu'une des facettes d'un système plus important. Par exemple, dans le cas de la vérification d'un composant de navigation aéronautique, RAHD pourra être utilisé pour effectuer un calcul de trajectoire de vol, mais il faudra trouver un autre moyen de prendre en compte l'état des systèmes de commande, du trafic aérien, des consignes des contrôleurs au sol, etc.

On peut adresser ce problème en couplant RAHD avec des outils plus généralistes, comme Coq [4], PVS, ou Isabelle, qui permettent d'étudier un large éventail de propriétés sur un système donné. L'équipe Celtique, en coopération avec les chercheurs d'Édinbourg [2], a proposé d'intégrer RAHD à Coq par le biais d'une base de données de formules, appelée Extended Case Database (ECDB). L'implémentation prototypale de l'ECDB a été récemment complétée, de même que l'ajout des points d'accès nécessaires dans RAHD et Coq.

Le but de ce stage est de participer à l'implémentation en Caml du protocole de communication reliant les « têtes de pont » logicielles de l'ECDB et de Coq. Une première approche pourra utiliser des *Berkeley TCP sockets* afin de réaliser la liaison [1]. Un candidat efficace pourra être également conduit à s'intéresser à la notion de certificats arithmétiques, à leur représentation dans l'ECDB, et à leur vérification en Coq.

Ce sujet requiert à la fois de manipuler des concepts mathématiques avancés, et de relever le défi d'efficacité attaché à l'implémentation des algorithmes associés. Le travail sera conduit en liaison serrée avec une équipe de recherche jeune et dynamique : le candidat devra démontrer un goût prononcé pour les interactions scientifiques.

Références

[1] Brian Hall. *Beej's Guide to Network Programming*. Jorgensen Publishing, 2009. `beej.us/guide/bgnet`.

[2] Florent Kirchner and Grant Passmore. Thinking outside the (arithmetic) box : Certifying RAHD computations. Short paper, Logics for System Analysis, 2010.

[3] Grant Passmore and Paul Jackson. Combined decision techniques for the existential theory of the reals. In Jacques Carette, Lucas Dixon, Claudio Sacerdoti Coen, and Stephen Watt, editors, *Calculemus/MKM*, volume 5625 of *LNCS*, pages 122–137, Heidelberg, 2009. Springer.

[4] The Coq Development Team. *Coq, Reference Manual, Version 8.3*, 2011.