Formalisation effective des réels algébriques avec Coq

L'assistant à la preuve Coq permet, outre la vérification de programmes, la formalisation de notions mathématiques. Des théorèmes de plus en plus difficiles ont ainsi pu être formellement vérifiés (d'Alembert-Gauss, quatre couleurs, et plus récemment Feit-Thompson [3]) et des librairies réutilisables ont été développées (C-CoRN, SSReflect).

Une des particularités de Coq est qu'il permet de manipuler à la fois de telles notions mathématiques et des algorithmes qui y ont recourt, dans un formalisme homogène.

Nous nous intéressons aux nombres réels algébriques, c'est-à-dire les réels qui sont racines de polynômes à coefficients rationnels. Ces nombres ont des propriétés intéressantes : ils forment un corps que l'on peut construire, dont on peut effectivement implémenter les opérations et qui dispose d'une égalité décidable. Il s'agit de plus d'un corps réels clos archimédien.

Ces réels algébriques sont ainsi couramment utilisés en calcul formel et en mathématiques constructives. En particulier, dans la récente preuve du théorème de Feit-Thompson [3], ils remplacent avantageusement les réels. Ils y sont décrits de manière constructive, à partir des polynômes et des suites de Cauchy [1].

L'objectif du stage proposé est de passer cette description de référence des réels algébriques à une implémentation plus efficace (toujours dans Coq), proche de celles utilisées dans les logiciels de calcul formel. La correction de cette seconde implémentation sera prouvée vis-à-vis de la première, suivant une méthodologie basée sur des raffinements [2].

Ce sujet est varié : il met en jeu à la fois des développements formels (séries formelles, représentation de Newton des polynômes) et des problématiques de programmation fonctionnelle pour implémenter les algorithmes, notamment pour la somme et le produit de réels algébriques.

Ce stage aura lieu au sein de l'équipe MARELLE, à l'INRIA Sophia-Antipolis, qui a participé activement à la preuve du théorème de Feit-Thompson, sous la responsabilité de Yves Bertot et Cyril Cohen.

Références

[1] Cyril Cohen. Construction of real algebraic numbers in Coq. In *ITP - 3rd International Conference on Interactive Theorem Proving - 2012*, 2012. Available from : `http://hal.inria.fr/hal-00671809`.

[2] Maxime Dénès, Anders Mortberg, and Vincent Siles. A refinement-based approach to computational algebra in COQ. In *ITP - 3rd International Conference on Interactive Theorem Proving - 2012*, 2012. Available from : `http://hal.inria.fr/hal-00734505`.

[3] Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, Russell O'Connor, Sidi Ould Biha, Ioana Pasca, Laurence Rideau, Alexey Solovyev, Enrico Tassi, and Laurent Théry. A Machine-Checked Proof of the Odd Order Theorem. In Sandrine Blazy and Christine Paulin and David Pichardie, editor, *ITP 2013, 4th Conference on Interactive Theorem Proving*, volume 7998 of *LNCS*, pages 163–179, Rennes, France, July 2013. Springer. Available from : `https://hal.inria.fr/hal-00816699`, `doi:10.1007/978-3-642-39634-2_14`.