

Année 2011–2012
Proposition de stage de master 2

TITRE : Vérification formelle d'un calcul multiprécision de π

LIEU : Équipe-Projet Proval
PCRI - Bâtiment 650
Université Paris 11
91405 Orsay cedex, France

PERSONNES ENCADRANT LE STAGE LOCALEMENT :

Sylvie Boldo
Tél: 01 74 85 42 26
Email : sylvie.boldo@inria.fr

Guillaume Melquiond
Tél: 01 74 85 42 86
Email : guillaume.melquiond@inria.fr

CONTEXTE :

L'équipe-projet ProVal propose des méthodes et outils de développement logiciel faisant une large place à la preuve de programmes assistée par ordinateurs. L'un des axes de recherche concerne la vérification de programmes utilisant l'arithmétique à virgule flottante.

Cette arithmétique est une approximation de l'arithmétique usuelle sur les nombres réels. Les calculs y sont effectués en précision finie ; les résultats intermédiaires ne sont pas représentés exactement. Cela cause des erreurs dites d'arrondi qui peuvent se propager, s'amplifier et potentiellement faire diverger les résultats.

L'une des approches pour certifier un programme est la vérification déductive, c'est-à-dire la preuve de propriétés logiques extraites du programme. Cela s'appuie sur une base de théorèmes formellement prouvés avec le système Coq.

OBJET DU STAGE :

Pour augmenter la précision de certains calculs, il existe des bibliothèques de calcul dites « multiprécision », pour lesquelles chaque résultat est calculé avec une précision choisie par l'utilisateur. Une propriété souhaitable est que le résultat soit correct jusqu'au dernier bit renvoyé, c'est la garantie qu'offre la bibliothèque MPFR¹ [2].

Pour garantir cela sans sacrifier les performances, il faut des algorithmes perfectionnés. Leur correction repose sur une preuve papier [3] si complexe que même des experts peuvent ne pas en être complètement sûrs. Une preuve

1. <http://www.mpfr.org/>

formelle permettrait d'augmenter la confiance en de tels algorithmes puisque la vérification serait alors laissée à l'ordinateur.

Un exemple d'application est le calcul de π par MPFR dont la preuve papier tient en une demi-page. Avec les bibliothèques et automatisations actuelles, la preuve formelle correspondante serait extrêmement longue. L'objectif de ce stage est de développer un jeu de théorèmes qui rende possibles et aisées de telles preuves. Le but est de vérifier l'algorithme de calcul de π aussi facilement que sur papier, c'est-à-dire que la preuve formelle ne doit pas ajouter de difficultés autres que celles présentes dans la preuve papier (à supposer que la preuve papier soit juste). En particulier, cela inclut à la fois des propriétés de type numérique (propagation d'erreur) et de type mathématique (convergence).

Les développements de ce stage seront faits en Coq et se baseront sur la bibliothèque Flocq² [1].

Références

- [1] Sylvie Boldo and Guillaume Melquiond. Flocq: A unified library for proving floating-point algorithms in Coq. In Elisardo Antelo, David Hough, and Paolo Ienne, editors, *Proceedings of the 20th IEEE Symposium on Computer Arithmetic*, pages 243–252, Tübingen, Germany, 2011.
- [2] Laurent Fousse, Guillaume Hanrot, Vincent Lefèvre, Patrick Pélissier, and Paul Zimmermann. MPFR: A multiple-precision binary floating-point library with correct rounding. *ACM Transactions on Mathematical Software*, 33(2):13:1–13:15, June 2007.
- [3] The MPFR team. The MPFR Library: Algorithms and Proofs. <http://www.mpfr.org/algorithms.pdf>.

2. <http://flocq.gforge.inria.fr/>