ProvenMPFR
(proposition de stage L3)

Lieu. INRIA/LORIA, Nancy, `www.loria.fr`.

Encadrant. Paul Zimmermann, directeur de recherche, équipe Caramba, `Paul.Zimmermann@inria.fr` (collaboration avec Karthik Bhargavan, équipe Prosecco, Inria Paris).

Contexte. GNU MPFR [1] est une bibliothèque de calcul flottant en précision arbitraire avec une sémantique bien précise. Pour chaque opération, on garantit qu'elle renvoie le résultat le plus proche de la valeur en précision infinie selon l'arrondi indiqué par l'utilisateur. C'est ce qu'on appelle l'*arrondi correct*. MPFR garantit l'arrondi correct non seulement pour les opérations arithmétiques de base — comme demandé par le standard IEEE 754 [2] — mais aussi pour toutes les fonctions mathématiques (sinus, exponentielle, logarithme, ...)

La garantie de l'arrondi correct repose sur la correction des algorithmes implantés dans MPFR, qui sont documentés dans `https://www.mpfr.org/algorithms.pdf`, et sur l'implantation correcte de ces algorithmes en langage C.

Objectif du stage. Le but du stage est de mettre en œuvre des outils de preuve formelle pour obtenir une meilleure garantie de la correction de la bibliothèque MPFR. En 2018, Jianyang Pan a prouvé la correction de la fonction `mpfr_add1sp1` qui additionne deux nombres flottants de même précision $p < 64$, et stocke leur somme dans une variable de précision p également. Ce travail [1] a été effectué avec le langage F^*, et le code extrait est aussi efficace que le code originel (non-prouvé) de MPFR. Ce code certifié est dès à présent distribué avec MPFR.

Selon ses compétences et affinités, la/le stagiaire poursuivra le travail initié par Jianyang Pan avec F^* (qui avait aussi partiellement prouvé la fonction `mpfr_mul_1` multipliant deux nombres flottants de même précision $p < 64$), et/ou pourra explorer d'autres pistes. L'objectif ultime reste dans tous les cas de prouver non seulement les algorithmes sur le papier, mais le vrai code en langage C utilisé par la bibliothèque MPFR, si possible avec la même efficacité que le code originel. Le code prouvé correct lors de ce stage sera distribué avec la bibliothèque MPFR.

Références

[1] Fousse, L., Hanrot, G., Lefèvre, V., Pélissier, P., and Zimmermann, P. MPFR : A multiple-precision binary floating-point library with correct rounding. *ACM Trans. Math. Softw. 33*, 2 (2007), article 13.

[2] IEEE standard for binary floating-point arithmetic. Tech. Rep. ANSI-IEEE Standard 754-1985, New York, 1985. approved March 21, 1985 : IEEE Standards Board, approved July 26, 1985 : American National Standards Institute, 18 pages.

1. `https://github.com/project-everest/hacl-star/tree/dev_mpfr/code/mpfr`