Proposition de sujet de thèse à l'IRIT

Xavier Thirioux
acadie, irit, enseeiht
xavier.thirioux@irit.fr

Érik Martin-Dorel
acadie, irit, ups
erik.martin-dorel@irit.fr

Février 2019

Titre Preuves formelles pour l'approximation polynomiale garantie

Contexte Les activités de recherche de l'équipe ACADIE se placent dans le domaine des méthodes formelles, comprenant plusieurs méthodologies dont l'utilisation d'assistants de preuve formelle. L'utilisation de ce type d'outil permet de spécifier, d'implanter et de vérifier des algorithmes issus de multiples domaines d'application en fournissant un haut niveau de garantie sur leur correction. En particulier, l'outil Coq [3] a été utilisé avec succès pour vérifier formellement des résultats clés en théorie des graphes [4], en théorie des groupes [5], en arithmétique flottante [1], ou encore en compilation certifiée [6].

Sujet Dans le projet TaMaDi/CoqApprox a été développé un composant formel d'approximation polynomiale certifiée pour des fonctions univariées [2, 8]. Ce composant a été intégré à la bibliothèque d'arithmétique d'intervalles CoqInterval [7], fournissant ainsi des tactiques pour prouver formellement et automatiquement des bornes sur des expressions réelles pouvant impliquer des fonctions élémentaires (cos, ln, etc.). Les tactiques en questions construisent dynamiquement des polynômes d'approximation de Taylor, munis d'une borne d'erreur certifiée, mais en se limitant à des polynômes en une variable.

D'autre part, une bibliothèque d'approximation polynômiale multivariée a été développée en OCaml [9], en s'appuyant sur la notion de tenseur et sur le typage expressif des GADT pour exprimer des garanties sur la bonne définition des opérations correspondantes. Mais les approximants de Taylor multivariés obtenus actuellement ne sont pas munis de garanties sur les bornes d'erreur.

Nous aimerions explorer plusieurs prolongements possibles de ces travaux :

— combiner certains aspects de ces deux approches pour obtenir des développements de Taylor multivariés avec borne d'erreur garantie ;
— réfléchir à des méthodes pour optimiser la précision des calculs dans l'environnement fonctionnel pur sous-jacent à Coq ;
— changer de domaine numérique pour représenter les erreurs plus finement qu'avec des intervalles ;
— considérer l'application de ces méthodologies à la résolution d'ODEs avec erreur garantie (dans le cas univarié).

Suivant les intérêts du candidat, le travail de thèse pourra s'attacher plus spécifiquement à certains de ces objectifs.

Pré-requis Le candidat doit avoir un intérêt pour la programmation fonctionnelle et la logique mathématique. Une expérience préalable de Coq ou d'un autre assistant de preuve est appréciée mais n'est pas nécessaire.

Informations pratiques La thèse, dirigée par Xavier Thirioux et co-encadrée par Érik Martin-Dorel, se déroulera au sein du département *fiabilité des systèmes et des logiciels* de l'Institut de Recherche en Informatique de Toulouse (IRIT).

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, *20th IEEE Symposium on Computer Arithmetic, ARITH 2011, Tübingen, Germany, 25-27 July 2011*, pages 243–252. IEEE Computer Society, 2011.

[2] Nicolas Brisebarre, Mioara Joldes, Érik Martin-Dorel, Micaela Mayero, Jean-Michel Muller, Ioana Pasca, Laurence Rideau, and Laurent Théry. Rigorous polynomial approximation using taylor models in coq. In Alwyn Goodloe and Suzette Person, editors, *NASA Formal Methods - 4th International Symposium, NFM 2012, Norfolk, VA, USA, April 3-5, 2012. Proceedings*, volume 7226 of *Lecture Notes in Computer Science*, pages 85–99. Springer, 2012.

[3] The Coq Development Team. *The Coq Proof Assistant : Reference Manual*, 2019. https://coq.inria.fr/distrib/current/refman/.

[4] Georges Gonthier. Formal Proof—The Four-Color Theorem. *Notices of the American Mathematical Society*, 55(11) :1382–1393, 2008.

[5] 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, Christine Paulin-Mohring, and David Pichardie, editors, *Interactive Theorem Proving - 4th International Conference, ITP 2013, Rennes, France, July 22-26, 2013. Proceedings*, volume 7998 of *Lecture Notes in Computer Science*, pages 163–179. Springer, 2013.

[6] Xavier Leroy. A formally verified compiler back-end. *J. Autom. Reasoning*, 43(4) :363–446, 2009.

[7] Érik Martin-Dorel and Guillaume Melquiond. Proving tight bounds on univariate expressions with elementary functions in coq. *J. Autom. Reasoning*, 57(3) :187–217, 2016.

[8] Érik Martin-Dorel, Laurence Rideau, Laurent Théry, Micaela Mayero, and Ioana Pasca. Certified, efficient and sharp univariate taylor models in COQ. In Nikolaj Bjørner, Viorel Negru, Tetsuo Ida, Tudor Jebelean, Dana Petcu, Stephen M. Watt, and Daniela Zaharie, editors, *15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2013, Timisoara, Romania, September 23-26, 2013*, pages 193–200. IEEE Computer Society, 2013.

[9] Xavier Thirioux. *Verifying Embedded Systems*. Habilitation à diriger des recherches, Institut National Polytechnique de Toulouse, Toulouse, France, September 2016.