Équipe Arénaire

Arithmétique des ordinateurs

LIP, CNRS-ÉNS Lyon-INRIA-UCBL

Composition

Direction : G. Villard (CR CNRS).

– 4 chercheurs : C.-P. Jeannerod (CR INRIA), J.-M. Muller (DR CNRS), N. Revol (CR INRIA), G. Villard (CR CNRS)
– 2 enseignants-chercheurs : N. Brisebarre (MCF, Univ. St-Étienne), F. de Dinechin (MCF, ENS Lyon)
– 1 post-doctorant : I. Toli (Post-doc INRIA)
– 7 doctorants : F. Cháves, J. Detrey, C. Lauter, G. Melquiond, R. Michard, S. K. Raina, N. Veyrat-Charvillon
– 2 ingénieurs : É. Bechetoille (Ing. ass. INRIA), S. Torres (IR MENESR, 30 %)
– 1 assistante de projet : Sylvie Boyer (INRIA)

Départs 2005 : J.-L. Beuchat (Post-doc. FNS), M. Daumas (CR CNRS), A. Tisserand (CR INRIA).

Description

Objectif général : rendre les arithmétiques **rigoureuses** et **plus efficaces** (en matériel et en logiciel).

Spécificité : l'expertise d'Arénaire embrasse la plupart des aspects de l'arithmétique des ordinateurs, des plus théoriques aux plus appliqués (mathématiques, informatique, circuits intégrés).

Nos recherches portent sur le développement et l'implantation de **nouveaux algorithmes** visant à améliorer les performances (coût, vitesse, précision, fiabilité, . . .) des opérateurs arithmétiques .
La complexité des méthodes amène naturellement à l'élaboration d'**outils modernes d'aide à la conception et de validation**.
Au travers d'applications diverses, notre travail sur les opérateurs prend aussi en compte des contraintes spécifiques auxquelles ils peuvent être soumis (taille de code, précision adaptative, . . .).

Outils de conception et validation

– Approximation de fonctions : polynômes et fractions rationnelles à coefficients contraints
– Erreurs (arrondi, méthode) : calcul, contrôle, encadrement, certification de résultats, validation
– Arithmétique d'intervalles, modèles de Taylor
– Erreurs (bugs), preuve : Coq, PVS

Opérateurs arithmétiques

Algorithmes et implantations logicielles et matérielles des
– opérations de base (virgules fixe et flottante) : $+, -, \times, /, \sqrt{}$, *fused multiply-and-add*, . . .
– arithmétique sur les corps finis
– opérations d'intervalles
– évaluation et arrondi correct des fonctions élémentaires ($\sqrt[3]{}, \log, \exp, \ldots$)

Applications

– Optimisation globale
– Algèbre linéaire : complexité algorithmique, matrices polynomiales (contrôle linéaire), matrices numériques, entières
– Cryptographie à clé publique et signature électronique

Production et activités des membres d'Arénaire

– Bibliothèques C, C++, Coq, PVS, VHDL
  • **logiciel** : Boost (intervalles), CRLibm (arrondi correct), Flip (flottants pour l'embarqué), Gappa (calcul d'erreur et preuve), LinBox (algèbre linéaire), MEPLib (approximation contrainte), MPCheck (qualité des fonctions élémentaires), MPFI (intervalles), NASA Langley PVS Libraries (modèles de Taylor), PFF (preuve formelle sur les flottants)
  • **matériel** : Divgen (générateur de diviseurs), FPLibrary (arithmétique réelle pour FPGA), HOTBM (méthodes à base de tables)
– Standardisation : actions pour une révision de la norme IEEE 754 (arrondi correct), actions pour intégrer l'arithmétique d'intervalles dans la norme ISO C++
– Présidence de steering/program committees de conférences (ARITH, ISSAC, . . .), organisation de colloques et d'écoles (RNC, ARCHI, Sympa, . . .)
– Publication de livres, d'articles dans des journaux internationaux (IEEE TC, ACM TOMS, TCS, JSC, J. Complexity, Reliab. Comput., ...), d'articles dans les actes de conférences internationales (ARITH, ISSAC, ASAP, ...)
– Enseignements : dépt. informatique fondamentale de l'ENS Lyon, master cryptologie de l'UCB Lyon, INSA Lyon, Univ. St-Étienne
– Actions de dissémination, actions «femmes et science»

Collaborations

Partenariats industriels : ST Microelectronics et Région Rhône-Alpes, Intel, CEA CENG Leti, ST Microelectronics et pôle de compétitivité Minalogic

Secteur académique :

– ACI cryptologie, sécurité informatique, nouv. interfaces des mathématiques : INRIA Rocquencourt, Univ. Montpellier, Univ. St-Étienne
– Projet GECKO (ANR) : École Polytechnique, INRIA Rocquencourt, Univ. Nice Sophia-Antipolis, Univ. Toulouse 3
– Action Arinews (GDR ALP-ARP) : Univ. Montpellier, Univ. Nancy, Univ. Paris 6, Univ. Perpignan et CEA
– Roxane : INRIA Sophia, Univ. Paris 11, Imag Grenoble
– Groupe de travail "Méthodes ensemblistes" (GDR MACS)
– Projet Algorithmes hybrides et adaptatifs : Imag Grenoble, INRIA Rhône-Alpes
– LinBox : 8 institutions Canada (2), France (2), USA (4)
– Mathlogaps (Prog. UE Marie Curie) : Univ. Leeds, Univ. Manchester (GB), Univ. Lyon 1, Univ. L. Maximilians München (All.)
– PICS CNRS/NIA-NASA/Univ. Berkeley/École Polytechnique
– Univ. Calgary (Canada)
– UC Los Angeles, Irvine (USA)
– Univ. Odense (Danemark)
– Univ. Santiago de Compostela (Espagne)
– Univ. Waterloo (Canada)