DALI

Digits Architectures et Logiciels Informatiques

Effectifs au 30/06/2013 :
8 permanents (4 ETP)
4 doctorants (4 ETP)
2 post-docs (2 ETP)

Nombre de thèses soutenues entre le 01/01/2008 et le 30/06/2013 : 4

Responsable :
Matthieu Martel

Page Internet de l'équipe :
http://webdali.univ-perp.fr/

MICRO-ARCHITECTURE DES PROCESSEURS, SIMULATION D'UNITES DE CALCUL, ARITHMETIQUE DES ORDINATEURS, CALCUL CERTIFIE, SYNTHESE DE CODE, OPERATEURS CRYPTOGRAPHIQUES, LOGICIEL NUMERIQUE, CALCUL HAUTE PERFORMANCE.

Présentation

L'équipe DALI développe une thématique de recherche unifiée afin d'améliorer la qualité numérique et la haute performance des calculs. DALI permet l'interaction, rare en France au sein d'une même équipe, d'experts en micro-architecture et en arithmétique des ordinateurs.
Côté performances, nos travaux portent sur l'exploitation du potentiel de calcul toujours croissant des processeurs : élargissement des chemins (micro-architecture vectorielle), multiplication des cœurs (parallélisme de tâches), augmentation du parallélisme d'instructions. Côté arithmétique, la qualité numérique des applications de calcul scientifique et la sûreté de fonctionnement d'applications embarquées dépendent crucialement de la maîtrise de la précision finie et de l'arithmétique flottante en particulier. Il s'agit de contrôler et certifier les calculs (algorithmes, codes) mais aussi d'optimiser la précision des résultats. De nombreux logiciels, scientifiques ou embarqués, nécessitent d'améliorer la qualité numérique sans pour autant sacrifier la rapidité d'exécution. Ainsi se rejoignent amélioration de la performance et de la qualité numérique.

Evolution de l'équipe

Le principal fait marquant est l'entrée de DALI au LIRMM le 1er janvier 2011, choix qualifié de « gagnant-gagnant » par le dernier rapport AERES. Cela a permis d'augmenter la visibilité de l'équipe et de bénéficier de la dynamique d'une grande UMR. Sur la période concernée, DALI a intensifié ses collaborations internes, et depuis 2011, s'emploie à renforcer dans la durée celles avec le LIRMM. Par ailleurs, DALI a fortement accru son rayonnement : organisation d'écoles thématiques (Archi'11 et EJCIM'13), de conférences nationales (RAIM'11) et internationales (SAS'10), direction des GT Arithmétique (GDR IM) et multicœur (GDR ASR), détachement de 24 mois d'un membre de l'équipe à U. Waterloo, accueil de professeurs invités, nouvelles collaborations internationales. Activités contractuelles, développements logiciels et doctorats soutenus ont aussi augmenté.

Organisation et Vie de l'équipe

DALI a maintenu son positionnement scientifique resserré autour de la performance et de la précision des calculs, tout en satisfaisant les besoins d'enseignement d'une petite université pluridisciplinaire. Un MCF (doctorat ENS Lyon 2009) a été recruté en 2010. DALI a incité au dynamisme scientifique des membres de l'équipe et en particulier des plus jeunes qui ont tous co-encadré une thèse sur leur thématique dans la période. La vie scientifique de l'équipe profite de l'unité de lieu, de nouveaux locaux depuis 2013, de réunions d'équipe et d'un séminaire réguliers. Sur la période, ces activités ont été renforcées par la mise en place de « journées scientifiques hors labo » où la totalité des membres de l'équipe ont échangé autour de leurs travaux. L'intégration au LIRMM a constitué une ouverture importante, sans remettre en cause la dimension humaine de l'équipe : journée « mieux calculer» d'échange avec les équipes ARITH, TATOO et SYSMIC, ANR PAVOIS, participation à la mise en place régionale de l'ISN, implication dans la vie de la plateforme HPC@LR, etc. DALI est aussi significativement impliquée dans la vie de l'UPVD, e.g. deux VP sur la période.

Laboratoire Informatique Robotique Microélectronique Montpellier

Activités scientifiques

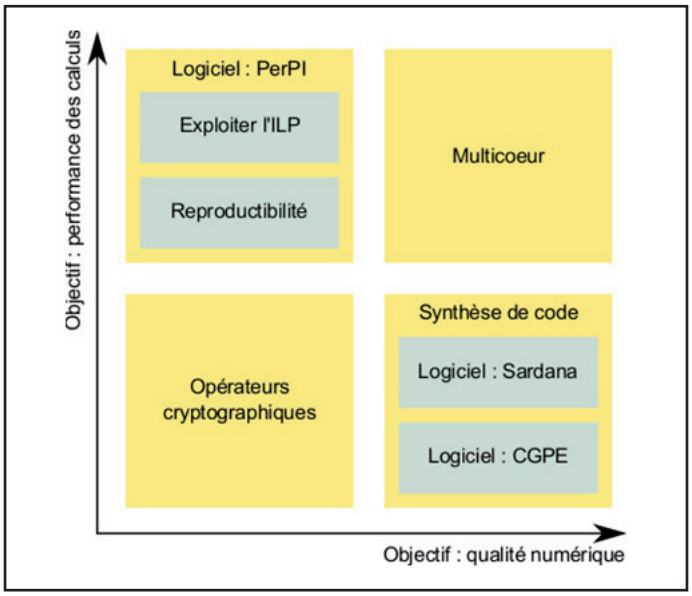
Thématique générale

La cohérence thématique des travaux de recherche sur l'amélioration de la qualité et de la performance des calculs est une des forces de l'équipe DALI.

L'amélioration de la performance des calculs est étroitement liée aux améliorations apportées aux micro-architectures. Celle-ci est réalisée suivant plusieurs directions, par élargissement des chemins (micro-architecture vectorielle), multiplication des cœurs (parallélisme de tâches), ou encore augmentation du parallélisme d'instructions (ILP). La qualité numérique des applications de calcul scientifique ou la sûreté de fonctionnement d'applications embarquées critiques dépendent crucialement de la maîtrise des effets de la précision finie des calculs — et de l'arithmétique flottante en particulier. Il s'agit alors de contrôler et valider les calculs (algorithmes, codes) mais aussi d'améliorer et optimiser la précision des calculs et des résultats.

Les travaux développés sur la période 2008-2013 sont organisés autour de 4 actions de recherche :

- **Action 1**. Mesure reproductible et analyse du potentiel de parallélisme et des performances.
- **Action 2**. Meilleure exploitation des nouvelles architectures multicœurs.
- **Action 3**. Implantation sûre et efficace de protocoles cryptographiques.
- **Action 4**. Synthèse de code pour l'implémentation de calculs précis, rapides et certifiés.



Action 1 : autour du logiciel PerPI

Notre approche de la performance des calculs s'appuie sur le parallélisme d'instructions (ILP). Le logiciel PerPI (Performance et Parallélisme d'Instructions) mesure le potentiel d'ILP. Les instructions indépendantes sont considérées comme parallélisables quel que soit leur éloignement réciproque [1]. On peut ainsi exhiber tout le parallélisme disponible, où qu'il se situe dans le flot d'exécution. PerPI nous permet de comprendre où sont les freins au parallélisme — ils viennent plus de l'architecture que de l'algorithme ou du programme — et déceler quantité de sources de parallélisme, notamment dans les nids de boucles et dans les fonctions une fois enlevée la sérialisation par la pile.

Trois thèses ont été soutenues sur ce thème. Celle de M. Bouache (2010) porte sur la simulation des processeurs, à la base du développement initial de PerPI. La thèse de A. El Moussaoui (2011) est consacrée à l'analyse d'ILP, sa nature, sa distribution et l'impact du compilateur. K. Chen (2012) étudie le profil de parallélisme des applications standard et propose un modèle de calcul innovant pour capturer le parallélisme massif détecté par PerPI. Dans ce modèle, toutes les étapes du traitement des instructions sont matériellement parallélisées, depuis l'extraction simultanée de plusieurs fonctions jusqu'à l'exécution par l'ensemble des cœurs de centaines d'instructions indépendantes. On accède ainsi à la parallélisation automatique de codes par le matériel.

Le calcul HPC s'appuie sur des bibliothèques mathématiques qui doivent être précises et performantes. Au niveau algorithmique, nous avons introduit la compensation pour l'évaluation polynomiale et la résolution de systèmes triangulaires [2]. Ces algorithmes produisent des résultats arbitrairement précis et validés, avec des vitesses d'exécution supérieures aux solutions existantes. Nous avons étudié leurs propriétés numériques et expliqué leur efficacité. PerPI permet aussi de caractériser le potentiel de performance des algorithmes numériques, et ce de manière reproductible contrairement aux approches classiques fondées sur le décompte des opérations ou des cycles machines.

En 2013, l'UPVD finance un BQR pour obtenir et partager des mesures de performance reproductibles et fournir des BLAS numériquement reproductibles pour le HPC. DALI et SYSMIC participent ensemble au projet Mont-Blanc 2 (projet IP, 7ième PCRD).

Action 2 : architectures multicœurs

L'arrivée des architectures multicœurs et en particulier des GPU, a révolutionné le HPC. S'il est désormais possible d'effectuer plus de calcul et plus vite, de nouvelles contraintes apparaissent aux niveaux matériel et logiciel pour offrir des garanties sur les résultats produits.

Nous avons mesuré comment les différents schémas de calcul impactent la qualité des résultats produits pour différentes applications : smartgrid (thèse de M. Marin), synthèse d'images (thèse de S. Collange, CR INRIA), bioinformatique (ANR BioWic). Ces mesures ont permis de confronter accélération obtenue et précision lors de l'utilisation des GPU.

Au niveau de la représentation de l'information, nous avons proposé une bibliothèque par intervalle en CUDA désormais intégrée dans le SDK CUDA de NVidia. Nous avons complété ce travail sur les différents formats de représentation des nombres en proposant une

implémentation vectorielle du format logarithmique (LNS) exploitant les unités de filtrages des GPU. Au niveau matériel, nous avons poursuivi le développement de Barra, simulateur de GPU, en intégrant les architectures GT200. Pour le HPC, le vieillissement des GPU pose des problèmes de fiabilité des calculs. Nous étudions les erreurs induites par ce vieillissement et comment fiabiliser les calculs.

Action 3 : protocoles cryptographiques

Les différents protocoles fondés sur les courbes elliptiques gagnent constamment en attractivité grâce à leurs tailles de clefs réduites et leurs nouvelles fonctionnalités. Le cœur de notre recherche consiste à améliorer efficacité et sécurité de leurs implantations [3]. Sur la période 2008-2013 nos travaux se sont structurés autour d'une collaboration avec l'U. Waterloo (Canada) et de l'étude de contre-mesures face aux attaques matérielles (ANR PAVOIS).

Concernant la performance des implantations (collaboration avec l'U. Waterloo), nous utilisons une formulation de la multiplication dans les corps binaires en un produit matrice-de-Toeplitz vecteur. Une réorganisation des calculs a permis d'obtenir un multiplieur plus performant. Dans le cadre de l'ANR PAVOIS, nous travaillons sur des implantations cryptographiques basées sur l'algorithme de Montgomery qui ne laissent fuir aucune information sensible par analyse de consommation et par injection de fautes (thèse de J.-M. Robert).

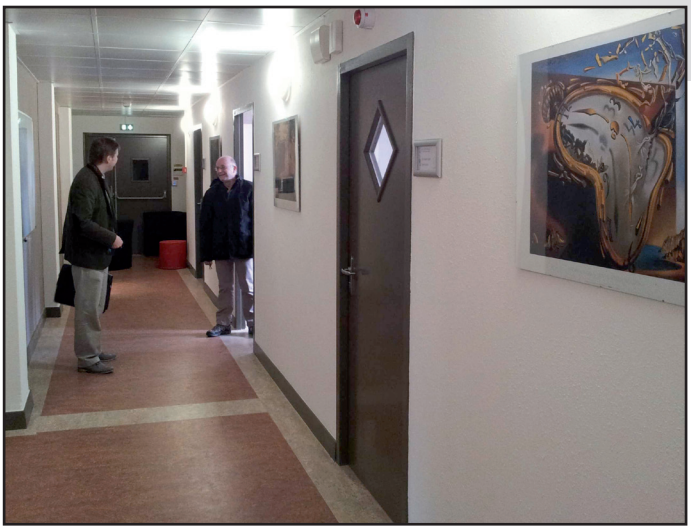
Action 4 : synthèse de code

La diversité des architectures matérielles actuelles, de leurs unités de calculs et des arithmétiques qu'elles supportent impose de proposer des outils de synthèse de codes. Étant donné un problème numérique (expression mathématique, algorithme, code numérique pré-existant), nous souhaitons produire une implantation qui soit à la fois rapide, suffisamment précise et certifiée. Au sein de DALI, cette activité se décline en trois axes.

Le premier axe concerne les travaux sur la transformation automatique de codes pour l'évaluation d'expressions en arithmétique flottante [4]. En supposant qu'un programme renverrait un résultat exact dans l'arithmétique réelle, nous modifions ses calculs afin que le résultat calculé soit le plus proche possible du résultat idéal. Ces travaux ont été réalisés dans les projets Sardanes (FNRAE 2009-2012) et Compil'HD (prix « chercheur d'avenir de la région LR 2010-2013) qui ont permis de financer les thèses de A. Ioualalen (2012) et L. Thévenoux. Les techniques mises en place ont été implantées dans l'outil SARDANA. Ils se poursuivent depuis 2013 dans l'ANR CAFEIN (en partenariat avec Rockwell-Collins, Prover, l'ONERA, le CEA et l'ENSTA).

Le deuxième axe se situe au niveau des briques numériques, e.g. fonctions élémentaires [5], et consiste en l'extension de l'outil CGPE. Ces travaux sont réalisés dans le projet ANR DEFIS (2011-2015 en partenariat avec Thales, InPixal, l'IRISA et le LIP6), qui finance la thèse de A. Najahi. Initialement destiné à la synthèse automatique de codes rapides et certifiés pour l'évaluation polynomiale en virgule fixe, l'outil CGPE permet aujourd'hui de produire des codes pour évaluer d'autres problèmes (e.g. sommation, produit scalaire), utilisant au mieux les instructions de l'architecture cible.

Pour la virgule flottante, nos travaux concernent l'amélioration de la précision à l'aide de transformations sans erreur. Ce troisième axe rejoint la thèse de L. Thévenoux, pour la synthèse de codes avec compromis performance-précision. L'enjeu est de déterminer quelles parties de code transformer sans trop impacter les performances de l'application.



Locaux de l'équipe DALI - Université de Perpignan Via Domitia

Faits marquants

- Intégration de l'équipe DALI au LIRMM le 1er janvier 2011.
- Organisation de 4 manifestations scientifiques : 17th Static Analysis Symposium (SAS'10), Ecole thématique Archi'11, Rencontres Arithmétique et Informatique Mathématique (RAIM'11), Ecole jeunes chercheurs du GDR Informatique Mathématique (EJCIM'13).
- Obtention du Prix « chercheur d'avenir » de la région Languedoc-Roussillon en 2010.
- Best Poster Award DASIP'2012, Karlsruhe, Germany.
- Inclusion d'une bibliothèque de calcul par intervalles au SDK CUDA de NVidia.

Partenariats

Partenaires industriels : Actility, Airbus, Inpixal, Prover, Rockwell-Collins, Thales, Total.

Projets collaboratifs : ANR Blanc EvaFlo (2006-2010), Projet DPAC MASSANE (2007-2010), ANR ARPEGE (2009-2011), Projet FNRAE SARDANES (2009-2012), Projet Chercheur d'avenir Compil'HD (2010-2012), ANR INS DEFIS (2011-2014), ANR INS CAFEIN (2012-2015), PEPS QUARENUM (2013).

Collaborations académiques

Collaborations nationales : CEA-LIST, ENSTA, EXASCALE, IRISA, LIENS, LIP, LIP6, LRI, LSIS, ONERA.

Collaborations internationales : Universitat de Girona, Technical University Hamburg, University of Malaysia Sabah, Mississippi State University, Microsoft Research Redmond, Rice University, Tokyo WCU, University of Waterloo (Canada), University of Wollongong, University of Waseda.

Publications majeures

- Bernard Goossens and David Parello, Limits of Instruction-Level Parallelism Capture, International Conference on Computational Science (ALCHEMY Workshop), 2013, to appear.
- Stef Graillat, Philippe Langlois, and Nicolas Louvet. Algorithms for accurate, validated and fast computations with polynomials. Japan Journal of Industrial and Applied Mathematics, 26(2,3):191-214, 2009.
- Anwar Hasan, Nicolas Meloni, Ashkan Namin, and Christophe Negre,Block Recombination Approach for Subquadratic Space Complexity Binary Field Multiplication based on Toeplitz Matrix-Vector Product ,IEEE Transactions on Computers, Vol 61(2), pages 151-163, 2012.
- Arnault Ioualalen and Matthieu Martel, A New Abstract Domain for the Representation of Mathematically Equivalent Expressions, Static Analysis Symposium, SAS'12, Lecture Notes in Computer Science, Volume 7460, pages 75-93, Springer-Verlag, 2012.
- Claude-Pierre Jeannerod, Hervé Knochel, Christophe Monat, and Guillaume Revy, Computing floating-point square roots via bivariate polynomial evaluation, IEEE Transactions on Computers, Vol. 60(2), pages 214-227, February 2011.

Journée DALI organisée au LIRMM le 6 mars 2012