RAIM 2012: LE PROGRAMME

Mercredi 20 juin

13h00 Accueil des participants

14h00 **SESSION CALCUL À HAUTE PERFORMANCE :**
– Fabienne JÉZÉQUEL (LIP6, Paris)

14h00 Bernard GOOSSENS (DALI, Perpignan)
Parallélisme dynamique

15h30 M. MARIN (DALI)
Implémentation of Rootfix and Leaffix primitive in OpenCL.

16h00 Pause

16h30 Édouard CANOT (SAGE, IRISA)
Solveur DAE et Calcul symbolique.

17h00 Mourad GOUICEM.
Correctly rounding transcendental functions with GPUs

17h30 **SESSION INTERVALLES :**
– Nathalie REVOL (LIP, ENS Lyon, Université de Lyon)

17h30 Philippe THÉVENY (LIP, ENS de Lyon, Université de Lyon)
Divers algorithmes de produits de matrices intervalles

18h00 Nathalie REVOL (INRIA, LIP, ENS de Lyon, Université de Lyon).
L'effort de normalisation IEEE-1788 de l'arithmétique par intervalles

18h30 Dominique MICHELUCCI (LE2I, Dijon)
Problème de Bernstein; Calcul par intervalles et fractales

19h00 Fin de la première journée

Jeudi 21 juin

8h45 **SESSION ARITHMÉTIQUE INDUSTRIELLE :**
– Philippe LANGLOIS (DALI / LIRMM, Perpignan)
8h45 Nicolas BRUNIE (LIP, et société Kalray)
Unité virgule flottante dans un processeur actuel
9h15 Duco Van AMSTEL (LIP / ENS Lyon, et Kalray)
Implémentation bit-slice de l'AES et de
la multiplication de matrices dans GF(2)

9h45 Pause

10h15 Christophe DENIS (EDF R&D, Clamart).
Étude de la qualité numérique de codes numériques industriels
10h45 Michel HUMMEL (Thalès Toulouse et CNES)
Présentation par Thalès d'un prototype d'outil d'anal yse dynamique
de la qualité numérique des codes Java, financé par le CNES

11h15 Pause

11h30 **OUVERTURE THÉMATIQUE:**
Arnaud TISSERAND (IRISA, Lannion)
Génération de nombres aléatoires "vrais" en matériel

12h30 Repas Montmuzard

14h00 **SESSION CRYPTOGRAPHIE :**
– Christophe NÈGRE (DALI / LIRMM, Perpignan).
14h00 Marine MINIER (INSA Lyon).
Les 10 ans de l'AES.
15h00 Thomas CHABRIER (IRISA, Lannion).
Protections arithmétiques contre certaines attaques
physiques de cryptosystème
Template attacks on hardware implementation of SD recoding for ECC
15h30 Thomas PLANTARD (Université de Wollongong)
Cryptographie sur les réseaux

16h00 Pause

16h30 Jérémy JEAN (ENS Paris), Thomas PEYRIN
et Maria NAYA-PLASENCIA.
Une attaque sur la fonction de hachage Grøstl.
17h00 Jean-Marc ROBERT (DALI / LIRMM, Perpignan).
Optimisations de l'implantation en C sur un processeur
Intel Core I7 de la multiplication scalaire sur
les courbes elliptiques binaires
17h30 **TABLE RONDE / ASSEMBLEE GENERALE DU GT**
18h00 Fin de la deuxième journée

Dîner à Dijon.

Vendredi 22 juin

8h15 **SESSION QUALITÉ NUMÉRIQUE :**
– Valérie MÉNISSIER-MORAIN (LIP6, Paris).

8h15 Andréas ENGE (INRIA, Bordeaux).
MPC, MPFRCX

9h15 Ioana PASCA (LIP, ENS Lyon, Université de Lyon.
Preuves formelles en Coq pour les modèles de Taylor

9h45 Pause

10h00 Christoph LAUTER et Valérie MÉNISSIER-MORAIN (LIP 6)
Sur la stabilité des modes d'arrondi.

10h30 Valérie MÉNISSIER-MORAIN.
Arithmétique compensée.

11h00 Laurent THÉVENOUX (DALI / LIRMM)
Transformation automatique de code pour optimiser la précision
et la vitesse des calculs en arithmétique flottante

11h30 Séthy MONTAN (EDF R&D, LIP6)
Une implémentation efficace de CADNA dans les BLAS:
exemple de la routine DgemmCADNA

12h00 Repas Montmuzard

13h30 **SESSION VIRGULE FIXE :**
– Laurent Stéphane DIDIER (LIP6, Paris) et Daniel MÉNARD (ENSSAT, IRIS, Renne

13h30 Daniel MÉNARD (ENSSAT, IRIS, Rennes)
Evaluation des performances des systèmes en virgule fixe

14h00 Benoît LOPEZ
Schémas d'évaluation de produits scalaire en arithmétique virgule fixe,
application aux filtres IIR.

14h30 Amine NAJAHI (DALI / LIRMM)
Synthesis of fixed-point programs based on instruction selection:
the case of polynomial evaluation

15h00 Clôture de RAIM 2012

Mercredi 20 juin 2012

SESSION CALCUL À HAUTE PERFORMANCE : Fabienne JÉZÉQUEL

Bernard GOOSSENS. Parallélisme dynamique

Le matériel met à notre disposition des processeurs multi-coeurs. Néanmoins, la duplication des coeurs ne sert qu'à augmenter le débit du système, en exécutant plusieurs threads simultanément. Pour diminuer la latence d'une application il faut la paralléliser à la main par un découpage en threads et exécuter les threads en parallèle sur les coeurs. Le cours montre que les applications sont naturellement parallèles et que c'est leur traduction architecturale qui ne l'est pas. Il fait le point sur la façon dont le matériel actuel récupère une partie du parallélisme initial par le renommage et la prédiction. On étudie ensuite le parallélisme d'instructions, parallélisme de grain fin dont sont truffées les applications. On montre ainsi que les processeurs d'aujourd'hui n'exploitent qu'à peine 5% du parallélisme disponible, le reste étant inaccessible. Enfin, le cours présente un algorithme matériel pour atteindre le parallélisme distant, exécutant les fonctions d'une application en parallèle sur les coeurs disponibles. Ainsi, on parallélise dynamiquement le code sans qu'il soit nécessaire de le modifier.

Manuel MARIN. Implémentation of Rootfix and Leaffix primitive in OpenCL

We are witnessing that the number of vehicle charging stations and renewable energy generators (solar or wind farm) connected to the electrical grid is rapidly growing. These new devices inject power requests on the grid that are highly correlated in time. This necessitates new techniques to manage the potential excesses of flow on the grid. The objective is to be able to determine the requests that can be satisfied according to the networks and request characteristics that are updated every second. This is called Power-Flow Analysis and is based on network simulation. In case of radial network, it involves Backward-Forward iterations over the considered tree. In this talk we will show how we have accelerated the Backward and Forward iterations based on an OpenCL implementation of rootfix and leaffix primitives. We will then present some speed-up we obtained and discuss about accuracy of the proposed method.

Édouard CANOT. Solveur DAE et Calcul symbolique

On présente un moyen permettant l'utilisation du calcul symbolique avec le calcul numérique.

De nombreux problèmes d'évolution en temps à résoudre numériquement (typiquement les systèmes d'équations provenant de systèmes couplés) sont de type PDAE (à Dérivées Partielles et Algébrique). Pour les systèmes raides, on a intérêt à discrétiser d'abord spatialement (méthode de lignes) pour arriver à un système DAE, qu'on résout avec un solveur DAE spécifique (par ex. DASSL). Les solveurs DAE nécessitent tous une jacobienne, pouvant être calculée numériquement par différences finies, ou être fournie par l'utilisateur. Lorsque le système d'équation est compliqué (formules mathématiques assez lourdes), il peut être intéressant d'utiliser un moteur de calcul formel (comme Maple) pour générer le code source correspondant à la jacobienne et qui est inclus directement dans le logiciel de simulation. L'avantage est double : éviter une erreur de codage à la main et obtenir un calcul plus précis.

Comme application, on montre des résultats concernant la simulation du transfert de chaleur dans un milieu poreux saturé en eau, avec changement de phase.

Mourad GOUICEM. Correctly rounding transcendental functions with GPUs

Since 1985, the IEEE 754 standard defines formats, rounding modes and basic operations for floating-point arithmetic. In 2008 the standard has been extended, and recommendations have been added about the rounding of some elementary functions such as trigonometric functions (cosine, sine, tangent and their inverses), exponential, and logarithm. However to guarantee the exact rounding of these functions one has to approximate them with a sufficient precision. Finding this precision is known as the Table Maker's Dilemma. To determine this precision, it is necessary to find the hardest-to-round argument of these functions. Lefèvre et al. proposed in 1998 an algorithm which improves the exhaustive search by computing a lower bound on the distance between a line segment and a grid. In this presentation, we will provide an improvement of this algorithm and show how to take advantage of massively parallel architectures (especially GPUs) for such computations. This enables a speed up of 52x on a NVIDIA Fermi GPU over one single high-end CPU Core.

SESSION INTERVALLES, Nathalie REVOL

Philippe THÉVENY. Divers algorithmes de produits de matrices intervalles

Le produit de matrices à coefficients intervalles est significativement plus lent que le produit de matrices à coefficients numériques, notamment à cause des changements nécessaires du mode d'arrondi. En réordonnant les opérations de l'algorithme naïf et en utilisant une représentation des intervalles par leur centre et leur rayon, il est possible de limiter le nombre de changements du mode d'arrondi et de se ramener à des appels à des fonctions BLAS de niveau 3. Plusieurs algorithmes de multiplications de matrices à coefficients intervalles de ce type existent dans la littérature, certains améliorant le temps d'exécution au détriment de la précision du résultat. Nous présentons ici une sélection de tels algorithmes et un ensemble de mesures expérimentales de leur précision. A partir de ces expériences numériques, nous analysons l'erreur mesurée qui est souvent très inférieure à la meilleure borne théorique.

Nathalie REVOL. L'effort de normalisation IEEE-1788 de l'arithmétique par intervalles

Depuis 2008, la communauté autour de l'arithmétique par intervalles a entrepris un effort collectif de normalisation de cette arithmétique. Je montrerai pourquoi cet effort est nécessaire et quels sont les grands principes qui sous-tendent les décisions prises. Je donnerai aussi, schématiquement, un aperçu des domaines et des décisions déjà prises : la majorité des discussions a porté jusqu'à présent sur la définition mathématique des intervalles et des opérations – arithmétiques ou ensemblistes – sur les intervalles. En particulier, le traitement des exceptions telles que $\sqrt{[-1,2]}$ a donné lieu à des discussions très nourries. Enfin, les implications de ces décisions sur l'implantation seront également développées.

Dominique MICHELUCCI. Problème de Bernstein; calcul par intervalles et fractales

Premier exposé. Calculer le coefficient le plus petit (ou le plus grand) dans la base tensorielle de Bernstein pour un polynôme de taille polynômiale en le nombre de variables dans la base canonique est NP-dur. La preuve utilise une réduction de 3SAT à ce problème.

Deuxième exposé. En modélisation géométrique, les objets géométriques sont souvent représentés par des fonctions, dites de Rvachev: la fonction est négative pour un point à l'intérieur de l'objet, positive pour un point hors de l'objet, et nulle pour un point sur la frontière de l'objet. L'exposé propose des fonctions de Rvachev pour des fractales ; ces fonctions sont "fractales" : continues mais presque nulle part différentiables. Elles peuvent être calculées par intervalles.

Jeudi 21 juin

SESSION ARITHMÉTIQUE INDUSTRIELLE – Philippe LANGLOIS

Christophe DENIS. Étude de la qualité numérique de codes numériques industriels

Le résultat d'un code de simulation numérique subit plusieurs approximations effectuées lors de la modélisation mathématique du problème physique, de la discrétisation du modèle mathématique et de la résolution numérique en arithmétique flottante. Les deux premières approximations sont bien connues et maîtrisées par l'ingénieur numéricien. L'usage de l'arithmétique flottante génère des erreurs d'arrondi à chaque expression arithmétique flottante ce qui peut entraîner des pertes de propriétés mathématiques. Par exemple, l'addition flottante n'est plus associative. L'étude de la qualité numérique (c'est-à-dire sa capacité à produire des résultats précis malgré les erreurs d'arrondi) indique si le calcul flottant s'est effectué sans perte de précision indépendamment des autres approximations. La qualité numérique d'un code est primordiale pour des codes industriels tels que ceux développés à EDF R&D. Ceci est encore plus important sur des architectures massivement parallèles où des trillions d'opérations arithmétiques flottantes sont exécutées chaque seconde. L'exposé présente les travaux menés au sein d'EDF R&D sur le contrôle de la qualité numérique de codes de calculs industriels.

Michel HUMMEL. Un prototype d'outil d'analyse dynamique

Le prototype JQNUM permet d'injecter dans le byteCode Java des perturbations dans les calculs flottants suivant des règles de perturbations, par exemple :

- Le passage en arithmétique stochastique (Arrondi aléatoire)
- Le passage en précision paramétrée (Réduction de la précision)
- Le passage en précision étendue (Base 10000, précision ajustable).

L'analyse des résultats générés par l'exécution du byteCode perturbé permet d'estimer la qualité numérique du code analysé. Par exemple couplé à l'algorithme de recherche nommé DeltaDebugging , JQNUM peut permettre de détecter quels sont les éléments d'un code (classes, méthodes, instructions/lignes de code) qui génèrent des instabilités numériques.

Nicolas BRUNIE. Unité virgule flottante dans un processeur actuel

Depuis la norme IEEE-754 de 1985 les unités flottantes se sont généralisées dans presque tous les types de processeurs. Incontournables dans les processeurs récents, mme dans le monde de l'embarqué, elles n'en restent pas moins coûteuses en silicium et en latence, et donc un domaine de recherche encore actif. Après une courte introduction sur l'état de l'art des FPUs, nous présenterons l'unité virgule flottante du K1 de Kalray, un processeur embarqué haute performance. Nous détaillerons l'implémentation de cette FPU pour le support de la simple et de la double précision. Nous traiterons ensuite de l'intégration d'opérateurs exotiques : un FMA précision mixte pour l'accumulation en grande précision, un produit scalaire en dimension 2 pour l'accélération de l'arithmétique complexe (entre autres). Nous verrons comment les contraintes inhérentes un processeur embarqué ont guidé les choix architecturaux lors de la mise au point de cette FPU.

Duco Van AMSTEL. Implémentation bit-slice de l'AES et du produit matriciel dans GF(2)

Avec la croissance des besoins en terme de sécurité des données dans le monde de l'Internet il y a aussi une forte demande de méthodes avancées et efficaces pour effectuer l'encodage et le décodage des informations associés à ce besoin. Que l'application recherchée soit l'encodage de grandes bases de données ou encore la sécurisation d'une connections réseau, les critères d'évaluation à considérer pour mesurer l'efficacité d'une méthode sont les mêmes. Ces critères sont la vitesse d'encodage atteinte, le coût énergétique de l'opération et enfin la résistance aux attaques cryptographiques de nature logicielle ou matérielle.

Pour cette étude nous avons choisi l'algorithme du Advanced Encryption Standard (AES) puisqu'il constitue une des fonctions cryptographiques actuelles les plus répandues. Parmi de nombreuses méthodes d'implémentation différentes, la technique du "bit-slice" est relativement peu étudiée et méconnue. En faisant usage de la nouvelle architecture proposée par Kalray, nous montrerons une implémentation bit-slice efficace de l'AES. Si la vitesse d'encodage atteinte est dépassée par certaines implémentations, l'efficacité énergétique de notre méthode est, elle, inégalée.

Afin d'atteindre notre résultat sur l'AES, il y a eu besoin de perfectionner la méthode utilisée pour les multiplication de matrices du corps de Galois GF(2); ceci constitue une deuxième moitié du travail qui sera exposé et qui fera appel à la fois à une instruction machine novatrice ainsi qu'à de la spécialisation hybride de code.

Arnaud TISSERAND. Génération de nombres aléatoires "vrais" en matériel

La génération de nombres aléatoires est nécessaire dans de nombreuses applications. Les générateurs aléatoires "vrais" (ou TRNG) utilisent une source de bruit physique et sont théoriquement non-déterministes contrairement aux générateurs pseudo-aléatoires (ou PRNG) qui utilisent des algorithmes déterministes. Nous introduirons quelques techniques de conception de TRNG en circuit intégré. Les variations de certains paramètres de l'environnement du TRNG (naturelles ou lors d'attaques physiques) peuvent provoquer des baisses importantes de la qualité de l'aléa produit. Nous présenterons quelques résultats d'implantation matérielle et de mesures de différents TRNG et de dispositifs d'évaluation en-ligne de leur qualité sur des circuits intégrés.

SESSION CRYPTOGRAPHIE – Christophe NÈGRE

Marine MINIER. Les 10 ans de l'AES

Les 10 ans de l'AES (Advanced Encryption Standard). Nous ferons le point sur l'état des recherches concernant la cryptanalyse de l'AES. Nous décrirons dans une première partie cet algorithme, et nous nous intéresserons ensuite à trois périodes de la vie de cet algorithme : les années d'incertitudes (2001-2004), l'âge d'or (2005-2008) et finalement ce qu'on pourrait considérer comme les premières alertes (2009-2011).

Thomas CHABRIER. Protections arithmétiques contre certaines attaques

In elliptic curve cryptography (ECC), arithmetic is a key element for designing efficient and secure cryptosystems. Finite fields arithmetic units should be fast to perform numerous and various computations (additions, subtractions, multiplications, inversions in the field) on large numbers (160-600 bits). For cost reasons, arithmetic operators should also be area, memory and power efficient. Finally, for security reasons, they should not reveal internal information during physical attacks such as side channel analysis.

In this work, we study FPGA implementations of various recoding schemes for secure ECC coprocessors. In ECC protocols, the main operation is the scalar multiplication [k]P where k is a large integer (160-600 bits) and P a point on the elliptic curve. In order to prevent from side channel analysis, k should be recoded at run time. We propose on-the-fly random recodings of the scalar digits using signed digit (SD) representation. The redundancy level of this representation allows to randomly choose among several representations of the key digits.

Side channel attacks pose a serious threat to implementation of cryptographic algorithms. Template attacks apply advanced statistical methods and can break implementations secure against other forms of side channel attacks. The University College of Cork (UCC) designed a generic architecture for ECC operations. We first perform this attack on an unsecure implementation based on this design and on a secure implementation using the SD representation, where the representation of the scalar k is randomly changed.

Thomas PLANTARD. Cryptographie sur les réseaux

Le chiffrement homomorphique permet d'évaluer des fonctions arbitraires sur des données chiffrées sans les déchiffrer. Après 30 ans, le problème de pouvoir créer un tel système a finalement été récemment résolu par Craig Gentry en utilisant les réseaux Euclidiens. Dû à son potentiel immédiat en raison du développement entre autres du "cloud computing", le chiffrement homomorphique a connu un développement impressionnant. Nous parlerons de ces développements ainsi que des principaux problèmes et challenges.

Jérémy JEAN, Thomas PEYRIN et Maria NAYA-PLASENCIA. Une attaque sur la fonction de hachage Grøstl

Keywords: Hash Function, Cryptanalysis, SHA-3, Grøstl, Rebound Attack. Grøstl is one of the five finalist hash functions of the SHA-3 competition. For entering this final phase, the designers have tweaked the submitted versions. This tweak renders

inapplicable the best known distinguishers on the compression function presented by Peyrin that exploited the internal permutation properties. Since the beginning of the final round, very few analysis have been published on Grøstl. Currently, the best known rebound-based results on the permutation and the compression function for the 256-bit version work up to 8 rounds, and up to 7 rounds for the 512-bit version. In this paper, we present new rebound distinguishers that work on a higher number of rounds for the permutations of both 256 and 512-bit versions of this finalist, that is 9 and 10 respectively. Our distinguishers make use of an algorithm that we propose for solving three fully active states in the middle of the differential characteristic, while the Super-Sbox technique only handles two.

Jean-Marc ROBERT. Optimisations de l'implantation en C sur un processeur

Optimisations de l'implantation en c sur un processeur Intel Core I7 de la multiplication scalaire sur les courbes elliptiques binaires. Nous rappellerons les meilleurs algorithmes pour l'arithmétique du corps GF(2^n) et de la courbe E. Nous parlerons alors d'optimisations du code exploitant les spécificités du processeur Intel Core I7. Nous présenterons ensuite des optimisations du code C pour les opérations AB,AC et AB+CD. Nous terminerons l'exposé par une comparaison des différents temps de calculs obtenus.

Vendredi 22 juin

SESSION QUALITÉ NUMÉRIQUE – Valérie MÉNISSIER-MORAIN

Andréas ENGE. MPC, MPFRCX

GNU MPC est une bibliothèque C pour l'arithmétique des nombres complexes. Elle calcule avec des nombres à précision arbitraire et fournit un arrondi exact de chaque opération atomique, en suivant les mêmes principes que la bibliothèque GNU MPFR pour les nombres réels.

L'exposé présente GNU MPC et ses ressemblances et quelques différences avec MPFR. Nous abordons la représentation des nombres et les principales fonctionnalités implantées. Nous discutons également quelques algorithmes choisis pour obtenir des implantations à la fois efficaces et fournissant un arrondi correct. Finalement, l'utilisation dans MPFRCX, bibliothèque pour l'arithmétique rapide de polynôme à coefficients dans MPFR ou MPC, est présentée.

Ioana PASCA. Preuves formelles en Coq pour les modèles de Taylor

One of the most common and practical ways of representing a real function on machines is by using a polynomial approximation. It is then important to properly handle the error introduced by such an approximation. The purpose of this work is to offer guaranteed error bounds for a specific kind of rigorous polynomial approximation called Taylor model. We carry out this work in the Coq proof assistant, with a special focus on genericity and efficiency for our implementation. We give an abstract interface for rigorous polynomial approximations, and we instantiate this interface to the case of Taylor models with interval coefficients, while providing all the machinery

for computing them. We compare the performances of our implementation in Coq with those of the Sollya tool, which contains an implementation of Taylor models in C. We prove correct our implementation of Taylor models with respect to the axiomatic formalisation of real functions available in Coq's standard library.

Christoph LAUTER et Valérie MÉNISSIER-MORAIN. Sur la stabilité des modes d'arrondi

Nous expliquerons tout d'abord pourquoi avoir un mode d'arrondi stable est tellement important pour une arithmétique fiable, en particulier pour l'arithmétique d'intervalles.

Nous montrerons ensuite combien cette stabilité du mode d'arrondi n'est pas assurée à l'heure actuelle.

Valérie MÉNISSIER-MORAIN. Arithmétique compensée

Inventée dans les années 1960, remise au goût du jour au milieu des années 2000, l'arithmétique compensée est toujours un moyen rapide et peu onéreux d'avoir une précision plus grande du résultat d'un calcul à base d'additions et de multiplications sans doubler la taille de la représentation des nombres tout au long du calcul.

Nous ferons ici une présentation intuitive de cette technique et montrerons l'étendue de ses applications.

Séthy MONTAN. Une implémentation efficace de CADNA dans les BLAS

Mots clés : CADNA, Arithmétique stochastique discrète, CESTAC, BLAS.

Le résultat d'un code de simulation numérique subit plusieurs approximations effectuées lors de la modélisation mathématique du problème physique, de la discrétisation du modèle mathématique et de la résolution numérique. Ces algorithmes numériques sont généralement conçus pour les nombres réels, mais sont exécutés sur des ordinateurs en utilisant l'arithmétique flottante. Cette arithmétique influence fortement la fiabilité des résultats des calculs numériques en raison des erreurs d'arrondi qu'elle y introduit.

La fiabilité d'un code est primordiale pour des codes industriels tels que ceux développés à EDF R&D. La bibliothèque CADNA, développée par le LIP6, permet d'étudier l'effet de la propagation de ces erreurs dans un programme séquentiel. Afin d'étudier le comportement numérique d'un code, il faut que celui-ci soit entièrement instrumenté. Les codes de calcul scientifique tels que ceux développés à EDF R&D (Code_Aster, TELEMAC) font appel à des bibliothèques externes (MPI, BLACS, BLAS, LAPACK), il est donc nécessaire d'instrumenter ces dernières en implémentant des extensions compatibles avec l'outil de validation numérique CADNA. La complexité algorithmique et la taille des logiciels de calcul numérique impliquent d'importants temps d'exécution. Pour mener ces études dans des temps raisonnables, il est important de rechercher des solutions pour diminuer l'impact de CADNA sur les performances de ces bibliothèques. A titre d'exemple, l'implémentation directe de CADNA dans la routine DGEMM des BLAS, introduit un important surcoût (supérieur à 1000 pour une matrice carrée de taille 1024). Notre présentation a pour objet d'exposer les raisons de ce surcoût ainsi que la méthodologie pour la réduire.

SESSION VIRGULE FIXE – Laurent Stéphane DIDIER et Daniel MÉNARD

Daniel MÉNARD. Evaluation des performances des systèmes en virgule fixe

L'utilisation d'une arithmétique en précision finie conduit à une erreur entre les valeurs en précision finie et en précision infinie. Cette erreur va dégrader les performances de l'application, c.-à-d. la qualité du résultat fourni par l'application. Dans cet exposé, nous présentons une approche permettant d'analyser les effets de la précision finie sur les performances de l'application. Cette approche combine une approche analytique et par simulation. L'approche analytique permet de déterminer la puissance du bruit de quantification en sortie des sous-systèmes composés d'opérations dont le modèle de bruit est linéaire. Pour les opérations à modèle de bruit non-linéaire telles que les opérations de décision, des techniques basées sur la simulation sont utilisées. L'idée est de simuler uniquement lorsque les valeurs en précision finie conduisent à une décision différente de celle en précision infinie.

Benoît LOPEZ. Schémas d'évaluation de produits scalaire en arithmétique virgule fixe

Schémas d'évaluation de produits scalaire en arithmétique virgule fixe, application aux filtres IIR.

Amine NAJAHI. Synthesis of fixed-point programs based on instruction selection

Synthesis of fixed-point programs based on instruction selection: the case of polynomial evaluation. Polynomial evaluation appears frequently in computer arithmetic as a building block of many useful functions. However, the number of schemes that can be used to evaluate a polynomial is exponential with respect to its degree. For this reason, picking a scheme with nice properties such as low latency and tight evaluation error is tedious. To tackle this problem, we developed CGPE, a tool dedicated to the generation of fast and certified codes for polynomial evaluation in fixed-point arithmetic. CGPE starts by computing DAGs that represent different ways of evaluating a polynomial, before applying a series of filters to eliminate the ones that fail to achieve some well chosen criteria.

In this talk, we introduce an extension of CGPE, which relies on techniques that were initially designed for the problem of instruction selection. This extension consists in providing CGPE with different tiles (themselves based on instructions available on the target architecture), and making it rely on a tiling selection algorithm to produce optimized code. This step is backed by a numerical filter which automatically eliminates DAGs with poor numerical quality.

Our tool was successfully validated on the ST231 processor core, for which we were able to automatically reproduce results that used to be obtained through a lengthy handmade process. Moreover, the modularity of our approach will enable us to target new architectures and produce code that is optimized according to different criteria.