RAIM2013

6ème édition
LIP6 - UPMC - GDR-IM

Du 18 au 20 Novembre 2013
Institut Henri-Poincaré

Programme

Résumés et informations pratiques

Lundi 18 Novembre	
11h00	**Accueil (pause café, etc.)**
11h30	**Le développement du système PARI/GP (1983-2013)**, Karim Belabas (IMB, Univ. Bordeaux)
12h30	**Déjeuner**
	Session Arithmétique et Musique (resp. Moreno Andreatta)
14h00	**Introduction générale sur la recherche mathémusicale**, Moreno Andreatta (CNRS/IRCAM/UPMC)
14h30	**Quelques compléments sur la théorie des mots, les automates, les pavages et l'inconstance**, Jean-Paul Allouche (CNRS/UPMC)
14h45	**Le mot Lambda**, Emmanuel Amiot (CPGE, Perpignan)
15h30	**Sturmian involution, lattice-path-transformations and their application to the investigation of diatonicity**, Thomas Noll (ESMuC, Barcelona)
16h00	**Pause**
16h30	**Pavages rythmiques : aspects algébriques et algorithmiques**, Hélianthe Caure (ENS/UPMC/Ircam)
17h15	**Séries temporelles et orchestration**, Philippe Esling (UPMC/Ircam) et Carlos Agon (UPMC/Ircam)
18h00	**Discussion générale sur arithmétique, musique et informatique**
Mardi 19 Novembre	
	Session Industriels (resp. Laurent-Stéphane Didier)
9h00	**Plus de 10 ans de diffusion de la méthode B**, Etienne Prun (Clearsy)
9h45	**Contexte industriel de la conversion floating-point to fixed-point**, Fabrice Lemonnier (Thalès)
10h30	**Pause**
11h00	**Session Cryptographie (resp. Pascal Véron)**
	Attaques par fautes sur les couplages, exposé de Nadia El Mrabet (Paris 8), présenté par Philippe Guillot (Paris 8)
	Arithmétique co-Z sur courbes elliptiques, Marc Joye (Technicolor)
	Inversion modulaire RNS sur FPGA, Karim Bigou (Inria)
	A quasi-polynomial algorithm for discrete logarithm in finite fields, Razvan Barbulescu (Université de Lorraine)
12h30	**Déjeuner**
14h00	**Une petite histoire de l'arithmétique virgule flottante**, Jean-Michel Muller (ENS Lyon)
15h00	**Session Vérification et validation numérique (resp. Guillaume Melquiond, LRI/Inria)**
	Exposé long : Domaines abstraits génériques et spécifiques pour l'analyse statique par interprétation abstraite de programmes avec calculs en virgule flottante, Antoine Miné (CR CNRS, ENS)
	A formally-verified C compiler supporting floating-point arithmetic, Jacques-Henri Jourdan (doctorant Inria, Rocquencourt)
	Pause
	Formal proofs and certified computation in Coq for solving the Table Maker's Dilemma, Erik Martin-Dorel (postdoc Inria Saclay)
	Pourquoi faire simple quand on peut faire compliqué : calculer la racine carrée du carré, Sylvie Boldo (CR Inria Saclay, LRI)
17h30	**Point sur les projets de la communauté (Guillaume Revy, LIRMM)**
18h30	**AG**
19h30	**Repas à l'Ardoise (restaurant sur le campus de l'UPMC)**
Mercredi 20 Novembre	
	Session Intervalles (resp. Alexandre Goldsztejn, Lina)
9h00	**L'analyse par intervalles : Preuves non-linéaires assistées par ordinateur**, Alexandre Goldsztejn (Lina)
9h30	**Classification des applications lisses d'un domaine simplement connexe de R^2 dans R^2**, Nicolas Delanoue (LARIS, Université d'Angers)
10h00	**Quelques histoires sur les petits octogones optimaux et leurs preuves assistées par ordinateur**, Frédéric Messine (LAPLACE, ENSEEIHT, INP-T, Université de Toulouse)

10h30	**Pause**
11h00	**Session Calcul symbolique et numérique (Guillaume Moroz, Loria/Inria)**
	Computing Real Roots of Real Polynomials, Michael Sagraloff (MPI-Inf)
	A quadratically convergent algorithm for Structured Low-Rank Approximation, Pierre-Jean Spaenlehauer (MPIM)
	Searching for sinks of Henon map using a multiple-precision GPU arithmetic library, Mioara Joldes (LAAS, CNRS)
	Scindage binaire " tronqué " et complexité en espace de l'évaluation de fonctions D-finies, Marc Mezzarobba (LIP6, UPMC)
12h30	**Déjeuner**
14h00	**Reproductibilité numérique**
	Reproductibilité numérique et calculs parallèles : impacts sur les algorithmes en arithmétique par intervalles, Nathalie Revol (AriC, ENS Lyon)
	Est-ce que le climat d'un modèle climatique est le même sur différents calculateurs?, Marie-Alice Foujols (IPSL)
16h30	**Fin des RAIM**

Résumés des différents exposés

Lundi 18 Novembre

Le développement du système PARI/GP (1983-2013), Karim Belabas(IMB, Univ. Bordeaux)
PARI/GP (http://pari.math.u-bordeaux.fr) est un logiciel spécialisé en théorie des nombres, développé depuis une trentaine d'années à l'université de Bordeaux 1. À l'origine outil d'expérience pour la recherche en algorithmique arithmétique, le système a connu une grande variété d'utilisateurs et d'utilisations bien au delà de ce que ses concepteurs avaient prévu. Après une rapide présentation du logiciel et de ses capacités, je reviendrai sur l'évolution du système et de son développement, puis sur nos projets en cours.

Session Arithmétique et Musique (resp. Moreno Andreatta)

Introduction générale sur la recherche mathémusicale, Moreno Andreatta (CNRS/IRCAM/UPMC)
Introduction générale sur la recherche mathémusicale et quelques compléments sur la théorie des mots, les automates, les pavages et l'inconstance (Moreno Andreatta et Jean-Paul Allouche) Dans la première partie, nous donnerons un aperçu de la richesse des rapports entre mathématiques et musique en décrivant quelques problèmes théoriques posés par la musique ayant permis d'obtenir de nouveaux résultats en mathématiques (ou, le cas échéant, des nouvelles interprétations, à partir de la musique, de résultats connus en mathématique). Une discussion sur la dynamique "mathémusicale" sous-jacente à ces problèmes permettra de mieux saisir les différences entre ce type de recherche et une simple application d'outils mathématiques en musique. Dans la deuxième partie de cette introduction on donnera quelques compléments sur les principaux concepts théoriques abordés dans les différentes présentations, en insistant, en particulier, sur leur composante maths/info.

Quelques compléments sur la théorie des mots, les automates, les pavages et l'inconstance, Jean-Paul Allouche (CNRS/UPMC)
Introduction générale sur la recherche mathémusicale et quelques compléments sur la théorie des mots, les automates, les pavages et l'inconstance (Moreno Andreatta et Jean-Paul Allouche) Dans la première partie, nous donnerons un aperçu de la richesse des rapports entre mathématiques et musique en décrivant quelques problèmes théoriques posés par la musique ayant permis d'obtenir de nouveaux résultats en mathématiques (ou, le cas échéant, des nouvelles interprétations, à partir de la musique, de résultats connus en mathématique). Une discussion sur la dynamique "mathémusicale" sous-jacente à ces problèmes permettra de mieux saisir les différences entre ce type de recherche et une simple application d'outils mathématiques en musique. Dans la deuxième partie de cette introduction on donnera quelques compléments sur les principaux concepts théoriques abordés dans les différentes présentations, en insistant, en particulier, sur leur composante maths/info.

Le mot Lambda, Emmanuel Amiot (CPGE, Perpignan)
Le monoïde des produits de puissances de 2 et de 3, connu depuis l'antiquité et utilisé au Moyen-âge pour organiser l'univers des notes musicales, recèle des propriétés remarquables en théorie des mots et notamment une densité maximale en palindromes.

Sturmian involution, lattice-path-transformations and their application to the investigation of diatonicity, Thomas Noll (ESMuC, Barcelona)
By some means or other music theorists account for the fact that diatonic tone relations have a double articulation, namely by major and minor steps on the one hand and by fifths and fourths on the other. The conceptualization of diatonic modes in the middle ages and in the Renaissance involves the classification of the species of the fifth and the fourth, where these intervals are filled by major and minor steps in different ways. In each mode the species of the fourth is a prefix or suffix of the corresponding species of the fifth. The discipline of algebraic combinatorics on words offers promising possibilities to accomplish the music-theoretical conceptualisation mathematically. Christoffel Words and their conjugates are well suited to represent the modal species and special Sturmian morphisms offer an elegant transformational account to their further investigation. A joint paper by Valérie Berthé, Aldo de Luca and Christophe Reutenauer, entitled "On an involution of Christoffel Words and Sturmain Morphisms" (European Journal of Combinatorics, 29(2), 2008) offers findings which are particularly interesting for the music-theoretical interpretation of this double articulation. In my talk I will focuss on the discussion of the linear lattice path transformations, which are induced by special Sturmian morphisms as well as on their duals. For a preparatory reading I recommend the comented slides from a public lecture, which I delivered in July at the Max Planck Institute for Mathematics in Bonn: http://www.mpim-bonn.mpg.de/de/node/4822

Pavages rythmiques : aspects algébriques et algorithmiques, Hélianthe Caure (ENS/UPMC/Ircam)

Les pavages rythmiques, abstraction de la notion musicale de canon, touchent à des problèmes subtils de combinatoire, d'algèbre, et d'algorithmique. On utilise la notion de pavage dans les corps finis, simple, pour tenter de comprendre le pavage des entiers.

Séries temporelles et orchestration, Philippe Esling (UPMC/Ircam) et Carlos Agon (UPMC/Ircam)

L'orchestration est l'art de l'écriture pour orchestre, mêlant les spécificités acoustiques de chaque instrument. Nous approchons ce problème comme l'évaluation des caractéristiques de combinaisons instrumentales s'approchant au plus d'une cible, par des critères de similarité flexibles et multidimensionnels. Malgré la combinatoire explosive, notre méthode permet de proposer un ensemble de solutions approchées où certaines zones de l'espace sont favorisées au détriment d'autres. Ainsi, les solutions définissent le front de Pareto d'un problème d'optimisation multicritères. Nos récentes avancées permettent l'utilisation structures temporelles, grâce à des techniques d'analyse des séries temporelles et des mesures de similarité non-linéaires. En s'inspirant de la perception musicale, nous introduisons un classificateur novateur basé sur les hypervolumes dominés de solutions multi-objectives (HV-MOTS), qui surpasse les méthodes existantes sur un large éventail de problèmes tels que la climatologie, le diagnostic médical et la robotique. Cette approche nous permet de construire un système d'identification biométrique basée sur les sons produit par les battements de coeur. Nous ouvrons sur des problématiques globales de l'analyse temporelle, le rapport entre différentes échelles du macro-temps (phrases musicales) au micro-temps (propriétés acoustique), la granularité temporelle, les interactions signal-symbolique et le continuum des échelles temporelles.

Mardi 19 Novembre

Session Industriels (resp. Laurent-Stéphane Didier)

Plus de 10 ans de diffusion de la méthode B, Etienne Prun (Clearsy)

La méthode B tire sa légitimité du développement d'outils approuvés et utilisés à grande échelle, dans le monde industriel et universitaire, tels que l'Atelier B. ClearSy est détenteur de cet atelier logiciel et se charge de sa diffusion, des évolutions, de la maintenance de sa plateforme de développement. L'Atelier B constitue une référence pour le développement de logiciels prouvés. Après un bref historique nous présenterons quelques projets types d'application, tant pour la réalisation et la preuve de logiciels, que la preuve de systèmes. Nous finirons par les développements en cours sur l'AtelierB ainsi que les pistes d'améliorations envisagées.

Contexte industriel de la conversion floating-point to fixed-point, Fabrice Lemonnier (Thalès)

L'écart entre la validation d'un algorithme en flottant double précision (Matlab) et son implémentation dans un système embarqué reste toujours aussi problématique pour un industriel. Outre la performance, les contraintes de l'embarqué sont généralement le volume, la consommation, etc. Afin de tenir ces contraintes il est généralement nécessaire de faire une conversion floating-point to fixed-point afin de réduire la complexité de l'architecture. Cela ajoute plusieurs semaines voire plusieurs mois de conception donc du coût et du temps. Une expertise un peu particulière est nécessaire pour faire la jonction entre ces 2 mondes qui généralement ne se comprennent pas. C'est pourquoi il est nécessaire de se munir d'outils capable de faire la conversion automatique en tenant compte des contraintes de dynamique, précision et rapport signal à bruit.

Session Cryptographie (resp. Pascal Véron)

Attaques par fautes sur les couplages, exposé de Nadia El Mrabet (Paris 8), présenté par Philippe Guillot (Paris 8)

Les couplages sont un outil mathématique permettant de mettre en oeuvre des cryptosystèmes originaux comme la cryptographie basée sur l'identité ou de simplifier des protocoles existants comme l'échange de clé Diffie Hellman entre trois parties. A l'heure actuelle, les implémentations les plus efficaces de couplages sont celles réalisées via l'algorithme de Miller. Les attaques par fautes sont des attaques permettant de retrouver de l'information sur un secret utilisé lors de l'exécution d'un algorithme. Lors de la mise en place d'un protocole basé sur l'identité, un des arguments du couplage est secret. Dans cette présentation, nous allons introduire rapidement les couplages et l'algorithme de Miller avant de mettre en évidence les faiblesses théoriques des couplages soumis à des attaques par fautes.

Arithmétique co-Z sur courbes elliptiques, Marc Joye (Technicolor)
En 2007, Meloni a proposé un nouveau type d'arithmétique permettant d'additionner des points projectifs sur une courbe elliptique, partageant la même coordonnée en Z. Dans cet exposé nous expliquons comment l'addition conjuguée de points et d'autres astuces d'implantation permettent d'obtenir des algorithmes de multiplication de points efficaces en utilisant l'arithmétique co-Z. Par ailleurs, les implantations ainsi obtenues sont régulières, offrant une protection naturelle contre certaines attaques.

Inversion modulaire RNS sur FPGA, Karim Bigou (Inria)
Asymmetric cryptographic systems such as RSA or elliptic curve cryptography (ECC) have strong arithmetic requirements over large values (few hundred of bits). The residue number system (RNS) provides efficient arithmetic operations with a high level of internal parallelism. A new modular inversion operator in RNS has been designed and implemented on FPGA (work presented at CHES 2013). The computation time of this operation has been significantly reduced (from 6 to 8 times for our implementations) for a very small area overhead compared to the state-of-art architecture RNS for ECC.

A quasi-polynomial algorithm for discrete logarithm in finite fields, Razvan Barbulescu (Université de Lorraine)
The difficulty of computing discrete logarithms in fields $GF(q^k)$ depends on the relative sizes of k and q but up to recently all the cases had a sub-exponential complexity of type $L(1/3)$, similar to the factorization problem. Following the recent algorithm of Joux of complexity $L(1/4+o(1))$ our algorithm has a complexity of $n^{O(logn)}$ where n is the bit-size of the input, when q is very small. For larger values of q the algorithm overpasses the Function Field Sieve except for the case when $q = L(1/3)$ with respect to q^k. The impact of the algorithm is to drastically reduce the security of pairing-based crypto-systems of small characteristic.

Une petite histoire de l'arithmétique virgule flottante, Jean-Michel Muller (ENS Lyon)
L'histoire de l'arithmétique virgule flottante est une longue histoire, qui nous mène des babyloniens aux derniers processeurs, en passant pas Archimède, Descartes, Leonardo Torres, Konrad Zuse, William Kahan et quelques autres, en alternant brillantes trouvailles et grosses bêtises. J'essaierai de donner un coup de projecteur sur certaines étapes importantes, sans prétendre ni à l'exhaustivité ni à l'objectivité.

Session Vérification et validation numérique (resp. Guillaume Melquiond, LRI/Inria)

Exposé long : Domaines abstraits génériques et spécifiques pour l'analyse statique par interprétation abstraite de programmes avec calculs en virgule flottante, Antoine Miné (CR CNRS, ENS)
L'interprétation abstraite permet de définir des analyses statiques de programmes à la fois automatiques, approchées (pour garantir l'efficacité) et sûres (toute propriété inférée est vraie, l'approximation se traduisant au pire par l'inférence de propriétés plus faibles). L'analyse est définie par le choix d'un domaine abstrait, c'est à dire d'une classe de propriétés d'intérêt munie d'une représentation machine et d'algorithmes pour la manipuler. Traditionnellement, les domaines abstraits de propriétés numériques sont définis pour des calculs en entiers ou en rationnels. Dans cet exposé, nous étudierons la construction de domaines numériques abstraits adaptés aux calculs en virgule flottante. Il s'agit d'abord d'enrichir les domaines génériques existants (comme celui, célèbre, des polyèdres) par des opérateurs tenant compte des erreurs d'arrondi dans le programme analysé. Nous étudierons également les algorithmes permettant l'implantation sûre de ces domaines en flottant, afin d'obtenir un analyseur plus efficace. Enfin, nous montrerons comment certains calculs idiomatiques faisant intervenir une connaissance fine de la représentation machine des flottants peuvent être analysés grâce à des domaines abstraits de prédicats dédiés.

A formally-verified C compiler supporting floating-point arithmetic, Jacques-Henri Jourdan (doctorant Inria, Rocquencourt)
L'arithmétique à virgule flottante selon la norme IEEE-754 obéit à des règles complexes et comprenant de nombreux cas : pour n'en citer que quelques-uns, on peut parler des différents modes d'arrondi, des infinis ou du signe de zéro. Par conséquent, étant donné un programme source qui manipule des nombres flottants, il est important que la façon dont il est compilé vers un exécutable soit prévisible et n'introduise pas de bugs. Dans cet exposé, nous expliquerons en quoi l'implantation d'un compilateur garantissant une telle propriété est un défi. Nous présenterons ensuite notre approche : l'ajout au compilateur formellement vérifié Compcert d'une formalisation des flottants, grâce à la bibliothèque Flocq. Cela nous permet ainsi d'obtenir un compilateur qui apporte des garanties formelles de conservation sémantique entre le programme source, écrit en C, et le programme assembleur généré pour la plateforme destination (ARM, PowerPC ou x86-SSE2), même en présence de calculs flottants.

Formal proofs and certified computation in Coq for solving the Table Maker's Dilemma, Erik Martin-Dorel (postdoc Inria Saclay)
The IEEE 754-2008 standard for floating-point arithmetic recommends to implement elementary functions (exp, sin, etc.) with correct rounding. But for doing this in an efficient and reliable manner, one has to solve the so-called Table Maker's Dilemma for each considered function. The Lefèvre and Stehlé-Lefèvre-Zimmermann (SLZ) algorithms have been designed to solve this problem. But the corresponding calculations are very long (several years of CPU time) and are performed using heavily optimized implementations of complex algorithms: this inevitably casts doubt on the correctness of their results. Hence the need to use formal tools such as the Coq proof assistant, to provide strong guarantees on the results of these algorithms. In this talk, I will present the works carried out in the TaMaDi project , with a special focus on the certification of the SLZ algorithm. I will present the methodology and the Coq libraries that have been developed to this aim.

Pourquoi faire simple quand on peut faire compliqué : calculer la racine carrée du carré, Sylvie Boldo (CR Inria Saclay, LRI)
Quand on souhaite calculer $x/\sqrt{x^2+y^2}$, c'est pour avoir une valeur inférieure à 1. Étant données les possibles erreurs d'arrondis, on voudrait (si possible) être sûr que cette valeur est toujours inférieure à 1. Or, le pire cas consiste à considérer $x/\sqrt{x^2}$ et donc à comparer x avec la racine carrée de son carré (calculée en arithmétique flottante). Cet exposé montrera des propriétés formellement prouvées en Coq concernant la valeur de $\sqrt{x^2}$. De façon surprenante, ces propriétés dépendront grandement de la valeur de la base de numération.

Mercredi 20 Novembre
Session Intervalles (resp. Alexandre Goldsztejn, Lina)

L'analyse par intervalles : Preuves non-linéaires assistées par ordinateur, Alexandre Goldsztejn (Lina)
L'arithmétique des intervalles permet d'encadrer l'image directe d'intervalles par des fonctions (éventuellement non-linéaires), tout en prenant en compte les erreurs d'arrondi de manière rigoureuse. De ce fait, l'analyse par intervalles est utilisée dans de nombreuses preuves assistées par ordinateurs mettant en jeux des propriétés de fonctions non-linéaires. Cela inclut la preuve de conjectures mathématiques, citons par exemple la résolution du 14ème problème de Smale par Warwick Tucker, ou la résolution de la conjecture de Kepler par Thomas Hales. L'analyse par intervalles a aussi donné naissance à de nouvelles méthodes permettant de calculer l'ensemble atteignable d'un système dynamique, de prouver sa stabilité, de déterminer la connexité de l'espace de travail d'un robot, etc. Cette session introduira l'analyse par intervalles sous l'angle des preuves assistées par ordinateurs, et sera l'occasion de présenter deux exposés sur la classification des fonctions lisses et sur quelques conjectures des petits octogones.

Classification des applications lisses d'un domaine simplement connexe de R^2 dans R^2, Nicolas Delanoue (LARIS, Université d'Angers)
L'analyse et la classification des applications lisses trouvent de nombreuses applications en robotique (planification de trajectoires, conception de robots manipulateurs sériels et parallèles...). D'un point de vue mathématique, la classification des applications lisses, modulo des difféomorphismes sur l'espace source et sur l'espace but, est directement connectée aux singularités de celles-ci. Durant l'exposé, je rappellerai dans un premier temps le théorème de transversalité de Thom et certains de ses corollaires (Théorème de Withney, Théorie de Morse, ...). Dans un second temps, je proposerai un algorithme, basé sur le calcul par intervalles, capable de construire un invariant global. Plus précisément, étant donné une application lisse f d'un domaine simplement connexe de R^2 dans R^2, la méthode calcule un graphe planaire topologiquement équivalent au contour apparent de f.

Quelques histoires sur les petits octogones optimaux et leurs preuves assistées par ordinateur, Frédéric Messine (LAPLACE, ENSEEIHT, INP-T, Université de Toulouse)
Nous verrons dans cet exposé comment des problèmes de géométrie plane, ouverts pour la plupart depuis 1922, peuvent être résolus à l'aide d'un ordinateur et de codes déterministes d'optimisation globale. En effet, dans la famille des petits polygones convexes ("petits" dans le sens où la distance maximale entre 2 sommets est 1), on peut se poser la question suivante : Les petits polygones réguliers sont-ils de périmètre maximal, de surface maximale ou de largeur maximale ? En fait, l'intuition nous trompe et nous ferait dire oui ! Cependant, il n'en ai rien dès lors que le nombre de sommets est pair. Nous présenterons donc une petite famille particulière de petits octogones optimaux et nous montrerons comment certifier ces solutions numériques à epsilon près (en utilisant entre autre un code d'optimisation globale basée sur l'arithmétique d'intervalles).

Session Calcul symbolique et numérique (Guillaume Moroz, Loria/Inria)

Computing Real Roots of Real Polynomials, Michael Sagraloff (MPI-Inf)
Computing the real roots of a polynomial is a fundamental problem of computational algebra. We describe a variant of the Descartes method that isolates the real roots of any real square-free polynomial given through coefficient oracles. A coefficient oracle provides arbitrarily good approximations of the coefficients. The bit complexity of the algorithm matches the complexity of the best algorithm known, and the algorithm is simpler than this algorithm. The algorithm derives its speed from the combination of Descartes method with Newton iteration. Our algorithm can also be used to further refine the isolating intervals to an arbitrary small size. The complexity of root refinement is nearly optimal.

A quadratically convergent algorithm for Structured Low-Rank Approximation, Pierre-Jean Spaenlehauer (MPIM)
Linear sections of determinantal varieties appear with different flavors in a wide range of applications in Engineering Sciences. In particular, low-rank structured matrices (e.g. Hankel, Toeplitz, Sylvester,...) play an important role in signal analysis, or in several areas of symbolic/numeric computation. Given an linear/affine space of matrices E with real entries, a data matrix U in E, and a target rank r, the Structured Low-Rank Approximation Problem consists in computing a matrix M in E which is close to U (with respect to the Frobenius norm) and has rank at most r. We propose an SVD-based numerical iteration which converges locally towards such a matrix, and which relies on algebraic properties of determinantal varieties. This iteration combines features of the alternating projections algorithm and of Newton's method, leading to a proven quadratic rate of convergence under mild tranversality assumptions between E and the variety of matrices of rank at most r. We also present experimental results in the context of important problems in symbolic/numeric computations: approximate univariate GCD (in that case, E is a linear space of Sylvester matrices) and matrix completion (E is the affine space obtained by fixing some entries of matrices to given values). Joint work with Éric Schost (Western University, London, Canada).

Searching for sinks of Henon map using a multiple-precision GPU arithmetic library, Mioara Joldes (LAAS, CNRS)

GPUs represent nowadays an important development hardware platform for many scientific computing applications that demand massive parallel computations, but currently GPU-tuned multiple precision arithmetic libraries are scarce. We develop a multiple-precision floating-point arithmetic library using the CUDA programming language for the NVidia GPU platform. In our case, we are currently using this library for locating invariant sets for chaotic dynamical systems. I will detail the numerical study, GPU implementation and a posteriori validation of existence of stable periodic orbits (sinks) for the Henon map for parameter values close to the canonical ones. This is a joint work with V. Popescu and W. Tucker.

Scindage binaire " tronqué " et complexité en espace de l'évaluation de fonctions D-finies, Marc Mezzarobba (LIP6, UPMC)

Un algorithme dû à Chudnovsky et Chudnovsky permet d'évaluer avec une erreur bornée par 2^{-p} n'importe quelle fonction analytique solution d'une équation différentielle linéaire à coefficients polynomiaux en temps $O(p\mathrm{fff}lg(p)^(3 + o(1)))$. L'algorithme, à base de scindage binaire, utilise $\Theta(p\mathrm{fff}lg(p))$ mots de mémoire, ce qui est comparativement beaucoup. Or, pour des problèmes qui peuvent être vus comme des cas particuliers de celui considéré par Chudnovsky et Chudnovsky, Gourdon et Sebah ont décrit une modification de la méthode de scindage binaire qui limite sa consommation mémoire et la rend considérablement plus efficace en pratique. Dans cet exposé, j'expliquerai comment ce scindage binaire " tronqué ", une fois généralisé et accompagné de bornes d'erreur, permet d'obtenir une complexité en espace linéaire dans le cas général sans changer la borne de complexité en temps.

Reproductibilité numérique

Reproductibilité numérique et calculs parallèles : impacts sur les algorithmes en arithmétique par intervalles, Nathalie Revol (AriC, ENS Lyon)

Par "reproductibilité numérique", on entend le fait d'obtenir le même résultat en effectuant le calcul numérique plusieurs fois, soit sur la même plateforme, soit sur des plateformes différentes, avec un nombre variable d'unités de calculs, des environnements d'exécution différents, des charges de calcul diverses etc. La question de la reproductibilité numérique se pose surtout dans le cadre de simulations numériques à haute performance (numerical HPC). La question centrale dans cet exposé est celle de la reproductibilité numérique pour des calculs parallèles en arithmétique par intervalles, en utilisant l'arithmétique flottante pour implanter l'arithmétique par intervalles. En effet, obtenir des résultats numériques de façon reproductible est important afin de pouvoir tester et mettre au point les prpgrammes. Cependant, on pourrait penser de prime abord que, tant que les résultats calculés sont des intervalles contenant les résultats exacts, il importe peu que ces résultats soient reproductibles au bit près. Il semblerait suffisant que la propriété d'inclusion, qui est la propriété essentielle de l'arithmétique par intervalles, soit préservée et que ce soit le cas même en l'absence de reproductibilité numérique. Or ce n'est pas toujours le cas : nous analyserons les phénomènes qui menacent la propriété d'inclusion et nous proposerons des pistes pour surmonter ces menaces, en prenant l'exemple du produit de matrices à coefficients intervalles.

Est-ce que le climat d'un modèle climatique est le même sur différents calculateurs?, Marie-Alice Foujols (IPSL)

Le 15 décembre 2012, mercure, le NEC SX-9 dédié aux simulations climatiques de l'IPSL depuis sa mise en route en avril 2009, a été définitivement arrêté. Une grande partie des simulations imposées dans le cadre du protocole CMIP5 (Coupled Model Intercomparison Project 5th phase), destinées notamment à la science qui sera présentée dans le prochain rapport du GIEC (Groupe Intergouvernemental d'Experts du Climat ; le prochain rapport sera le cinquième réalisé par le GIEC), ont été réalisées sur ce calculateur. De plus, leur valorisation dans le cadre des recherches en cours et à venir constitue un enjeu majeur. Pouvons-nous changer de calculateur au milieu d'une étude? Est-ce que le climat simulé par le modèle est le même lorsque il tourne sur différents calculateurs ?

Informations pratiques

Réseau WIFI à l'IHP

Nom du réseau : IHP0
Code : MissionToMars

Brasserie L'Ardoise

Sur le parvis Jussieu, entre les tours 25 et 26

0144273429 ou 0144272665
http://www.upmc.fr/fr/espace_des_personnels/pour_vous/restauration/brasserie_l_ardoise.html

Le campus de l'UPMC

Se rendre de l'IHP à l'UPMC (et vice-versa)

Temps de parcours : 11 minutes à pied
Distance : 900 mètres