L'association

femmes & mathématiques

en partenariat avec
la Mission pour la Place des Femmes du CNRS
organise le

13ème Forum des Jeunes Mathématicien-ne-s

Du 13 au 15 novembre 2013,
à l'Institut de Science Financière et Assurances
et à l'Ecole Normale Supérieure de Lyon.

Mathématiques et informatique en interaction.

Ouvert aux étudiantes de masters d'informatique et de mathématiques, sur inscription (gratuite mais obligatoire).

Site, inscription et programme : `http://forum2013.sciencesconf.org/`

Avec le soutien de l'INSMI, l'INS2I, la MIPADI du MESR, l'INRIA, le GDR IM, le Labex MILyon, l'ICJ, la FST et l'ISFA de l'Université Lyon 1, l'ENS de Lyon, le LIP, l'UMPA.

PROGRAMME

Mercredi 13 novembre 2013

Amphithéâtre G2 de l'ISFA
(50 avenue Tony Garnier, métro Stade de Gerland) jusqu'à 17h30
ENS de Lyon site Monod, amphithéâtre B
(46 allée d'Italie, métro Debourg, 3e étage Nord)

9h-9h30	Ouverture
9h30 - 10h30	Mireille Bousquet Mélou : *Familles de graphes à mineurs exclus : une introduction à la combinatoire énumérative et analytique* (conférence inaugurale)
10h30 - 11h	pause
11h - 11h30	Cheng Wan : *Coalition et délégation dans les jeux de congestion*
11h30 - 12h	Katia Jaffres-Runser : *RECAST : Telling Apart Social and Random Relationships in Dynamic Networks*
12h - 13h	Natalia Vacherand : *Présentation du programme européen INTEGER : Institutional Transformation for Effecting Gender Equality in Research*
14h30 - 15h	Alice Jacquot : *Génération aléatoire d'arbres binaires et unaires-binaires par un processus de croissance locale*
15h - 15h30	Bérénice Oger : *Hyperarbres décorés et code de Prüfer*
15h30 - 16h	pause
16h00 - 17h30	Muriel Salle : *Introduction à la notion de genre*
17h30-19h	Job meeting avec Véronique Garat, Claire Moreau, Marie-Pierre Stuchlik
19h	pot d'accueil (salle passerelle, ENS de Lyon site Monod)

Jeudi 14 novembre 2013

Amphithéâtre G2 de l'ISFA
(50 avenue Tony Garnier, métro Stade de Gerland) jusqu'à 17h30
ENS de Lyon site Descartes, amphithéâtre Kantor
(15 parvis René Descartes, métro Debourg)

9h15- 10h45	Anne Canteaut : *Comment concevoir un algorithme de chiffrement sûr et efficace* (mini-cours)
10h45 - 11h15	pause
11h15 - 11h45	Adeline Pierrot : *Trier des permutations avec des piles en série - Un algorithme polynomial de décision dans le cas de deux piles connectées en série*
11h45 - 12h15	Mioara Joldes : *Searching for sinks of Hénon map using a multiple-precision GPU arithmetic library*
12h15 - 12h45	Florence Bertails : *Simulation de clothoïdes dynamiques 3d*
14h - 15h	Catuscia Palamidessi : *Quantitative Aspects in Information Protection* (conférence invitée)
15h - 15h30	Adeline Langlois : *Autour de la difficulté du problème Learning With Errors*
15h30 - 16h	Tania Richmond : *Le décodage des codes de Goppa appliqué à la cryptographie asymétrique*
16h - 16h30	Joëlle Roué : *Amélioration des critères de résistance aux attaques différentielles*
16h30 - 17h	pause
17h-18h30	Sylvie Benzoni, Vincent Borrelli, Christine Leininger, Malika More et Laura Pallez : *Table ronde sur la vulgarisation en mathématiques et en informatique*, animée par Aleksandra Bogdanovic-Guillon
19h	Comédie des Ondes : *Elle est mathophile !* de et par Anne Rougée (théâtre Kantor, ENS de Lyon site Descartes)

Vendredi 15 novembre 2013

Salle 3302 et Amphithéâtre G2 de l'ISFA
(50 avenue Tony Garnier, métro Stade de Gerland)

9h-11h	Claire Morandeau (Soledev) : *Atelier mentorat* en salle 3302
11h -11h30	pause
11h30 - 12h30	Frédérique Bassino : *Énumération asymptotique d'automates finis* (conférence invitée)
14h - 15h	Isabelle Guérin-Lassous : *Comment candidater aux postes académiques*
15h - 15h30	Sophia Knight : *Modalities in constraint-based process calculi*
15h30 - 16h	Marie Kerjean : *L'analyse fonctionnelle du point de vue de la logique linéaire*
16h - 16h30	Nathalie Aubrun : *Liens entre calculabilité et dynamique symbolique*
17h	clôture du Forum

Résumés

Nathalie Aubrun : *Liens entre Calculabilité et Dynamique Symbolique*

Dans cet exposé on présentera les liens forts qui existent entre la théorie de la calculabilité et la dynamique symbolique. Ces liens peuvent être mis en évidence à travers des constructions classiques (pavage de Robinson et pavage de Kari-Culik) que nous présenterons dans un premier temps, puis nous verrons des exemples de résultats concernant les objets d'étude de la dynamique symbolique, les décalages, dans lesquels apparaissent des contraintes liées à la calculabilité.

Frédérique Bassino : *Enumération asymptotique d'automates finis*

Cet exposé portera sur l'énumération d'automates finis. Les automates peuvent être vus comme des graphes orientés dont les arêtes sont étiquetées sur un alphabet fini et dont deux sous-ensembles de sommets sont distingués (l'ensemble respectivement des états initiaux et des états terminaux). Les automates (resp. minimaux) constituent une représentation (resp. canonique) des langages rationnels et de ce fait jouent un rôle important en informatique.

Nous présenterons des résultats concernant l'énumération des automates détermnistes et accessibles, ie dans lesquels tout état peut-être atteint par un chemin partant de l'unique état initial. Nous déterminerons ensuite précisément la proportion asymptotique d'automates minimaux parmi les automates déterministes accessibles et complets. Ces résultats ont des conséquences en terme de complexité en moyenne d'algorithmes.

Toutes ces estimations peuvent être obtenue grâce à une interprétation combinatoire des propriétés structurelles des automates et à des bijections qui permettent de se ramener à l'étude combinatoire de tableaux particuliers.

Nous conclurons en présentant quelques problèmes ouverts.
Cet exposé s'appuie sur des travaux communs avec Julien David, Cyril Nicaud et Andrea Sportiello.

Florence Bertails-Descoubes : *Simulation de clothoïdes dynamiques 3d*
Les boucles de cheveux, les vrilles de vigne ou encore les rubans enroulés sont autant d'objets longilignes et flexibles qui se caractérisent par une forme lisse arbitrairement incurvée, et par des déformations mécaniques fortement non-linéaires. Afin de capturer la richesse de la forme et du mouvement de ces structures, nous proposons un nouveau modèle dynamique de tige défini par un profil de courbure linéaire par morceaux. Pour calculer la géométrie et la dynamique de cette nouvelle primitive, nous introduisons un schéma d'intégration en espace dédié, à base de séries entières, qui s'avère beaucoup plus performant que les intégrateurs classiques. Nous avons appliqué notre approche pour simuler divers scénarios réputés difficiles, comme le déroulement d'un ruban frisé, l'animation de cheveux ondulés ou bouclés, ou encore la croissance en spirale de plantes grimpantes.

Mireille Bousquet-Mélou : *Familles de graphes à mineurs exclus : une introduction à la combinatoire énumérative et analytique*
Soit A une classe de graphes étiquetés, fermée pour l'extraction de mineurs. Soit G_n un graphe aléatoire de taille n pris uniformément dans A. Quand n est grand, quelle est la probabilité que G_n soit connexe ? Plus généralement, combien de composantes connexes a-t-il ? Et quelle est la taille de ces composantes ? Grâce aux travaux de McDiarmid et de ses collaborateurs, ces questions sont désormais résolues lorsque tous les mineurs interdits sont 2-connexes. C'est par exemple le cas pour les graphes planaires.
Nous étudions une collection de classes définies par l'interdiction de mineurs dont certains ne sont pas 2-connexes, et montrons que leur propriétés asymptotiques peuvent être très différentes de celles obtenues dans le cas de mineurs 2-connexes.
Ces résultats utilisent de nombreux outils classiques de combinatoire : des séries génératrices pour l'énumération exacte, des techniques d'analyse complexe (analyse de singularités, méthode de col) pour l'obtention de résultats asymptotiques et de lois limites.
Cet exposé fournira donc l'occasion d'un petit panorama de ces techniques, très largement utilisées pour l'étude de structures discrètes en mathématiques et informatique.

Anne Canteaut : *Comment concevoir un algorithme de chiffrement sûr et efficace*
Les algorithmes de chiffrement, qui visent à protéger la confidentialité des données, se répartissent en deux grandes familles : les algorithmes symétriques, ou à clef secrète, qui nécessitent le partage d'un secret par les deux protagonistes, et les algorithmes à clef publique dans lesquels les clefs secrètes restent connues d'un seul acteur. De l'extérieur, cette classification pourrait laisser penser que les techniques symétriques seraient devenues obsolètes avec l'apparition de la cryptographie à clef publique et du célèbre algorithme RSA. Elles sont pourtant très largement répandues car elles sont les seules qui atteignent les débits de chiffrement requis par la plupart des applications et qui permettent une mise en œuvre par des circuits de taille raisonnable. Ainsi, ce sont des algorithmes à clef secrète qui assurent la confidentialité des échanges dans les téléphones portables, les cartes de crédit, les réseaux sans fil...

La conception d'un bon algorithme symétrique nécessite naturellement un enchaînement de phases de défense et d'attaque. Mais un travail poussé de formalisation de chaque attaque permet de mettre en évidence les propriétés structurelles qui la rendent opérationnelle. Ceci conduit alors à la construction d'objets qui permettent de lui résister de manière certaine. L'objectif de cet exposé est de décrire cette démarche de conception à travers l'exemple de l'AES, algorithme standard de chiffrement par blocs, conçu en 1997 par Joan Daemen et Vincent Rijmen, pour montrer que la conception d'un tel algorithme fait appel à la fois à des aspects très pratiques (coût d'implémentation...) et à des travaux fondamentaux de mathématiques discrètes.

Alice Jacquot : *Génération aléatoire d'arbres binaires et unaires-binaires par un processus de croissance locale*

Une manière d'obtenir des générateurs aléatoires d'objets combinatoires efficaces est de trouver une décomposition simple de grands objets en objets plus petits. Une décomposition bijective permet de garantir l'uniformité de la génération aléatoire, et donc la représentativité des objets ainsi engendrés. Je présente succinctement ici des travaux effectués avec Axel Bacher et Olivier Bodini, tiré d'un article en cours de rédaction. Nous nous intéressons à la génération aléatoire d'arbres binaires et unaires-binaires par un processus de modification locale, ce qui est plus « simple » au sens de la complexité algorithmique qu'un processus branchant.

Katia Jaffrès-Runser : *RECAST : Telling Apart Social and Random Relationships in Dynamic Networks*

The ability to accurately spot random and social relationships in dynamic networks is essential to network applications that rely on human routines, such as, e.g., opportunistic routing. This work introduces a strategy to analyze users' interactions in mobile networks where users act according to their interests and activity dynamics. This strategy, named Random rElationship ClASsifier sTrategy (RECAST), allows classifying users' wireless interactions, separating random interactions from different kinds of social ties. To that end, RECAST observes how the real system differs from an equivalent one where entities' decisions are completely random. We evaluate the effectiveness of the RECAST classification on real-world user contact datasets collected in diverse networking contexts. Our analysis unveils significant differences among the dynamics of users' wireless interactions in the datasets, which we leverage to unveil the impact of social ties on opportunistic routing.

Mioara Joldes : *Searching for sinks of Henon map using a multiple-precision GPU arithmetic library* (with Valentina Popescu and Warwick Tucker)

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. Our target application is locating invariant sets for chaotic dynamical systems. In particular, we focus on rigorously proving the existence of stable periodic orbits for the Hénon map for parameter values close to the classical ones. For that, we present a multiple-precision floating-point arithmetic library using the CUDA programming language for the NVIDIA GPU platform.

Marie Kerjean : *L'analyse fonctionnelle du point de vue de la Logique Linéaire*
Nous présentons un nouveau modèle de la Logique Linéaire, constitué d'espaces réflexifs. Nous introduisons d'abord les constructions de la Logique Linéaire à travers des intuitions tirées de l'algèbre linéaire, puis celles de la Logique Linéaire Différentielle. Les espaces réflexifs ainsi agencés valident l'analogie entre la Logique Linéaire Différentielle et l'analyse. La construction de ce modèle est l'occasion d'un nouvel intérêt pour les bornologies sur les espaces vectoriels localement convexes, et d'étudier les séries entières entre ces derniers.

Sophia Knight : *Modalities in Constraint-based Process Calculi*
We will describe the role that modal logic can play in concurrency theory, by using modal formulas as programming constructs in a constraint-based process calculus. We introduce spatial and epistemic process calculi for reasoning about spatial information and knowledge distributed among the agents of a system. We introduce domain-theoretical structures to represent spatial and epistemic information. Finally we provide operational and denotational techniques for reasoning about the potentially infinite behaviour of spatial and epistemic processes.

Adeline Langlois : *Autour de la difficulté du Problème Learning with Errors*
Nous montrons que le problème « Learning With Errors » (LWE), très utilisé en cryptographie reposant sur les réseaux Euclidiens, est au moins aussi difficile à résoudre que les problèmes pires-cas standards sur les réseaux Euclidiens, même avec un module polynomial. Les techniques utilisées pour prouver ce résultat sont liées au compromis entre la dimension et le module que l'on retrouve dans les instances du problème LWE, ce qui permet de mieux comprendre le problème. Les preuves sont inspirées de techniques utilisées dans différentes constructions cryptographiques récentes, en particulier pour le chiffrement homomorphe.

Bérénice Oger : *Hyperarbres décorés et code de Prüfer*
Nous introduisons une nouvelle sorte d'arbres, appelés *arbres en boîtes*, pour dénombrer des variations d'hyperarbres, dits *décorés*, où les arêtes sont munies d'une structure additionnelle. Par une bijection utilisant un code de Prüfer, nous dénombrons les arbres en boîtes, ce qui nous permet d'obtenir des expressions explicites des séries génératrices des hyperarbres décorés.

Catuscia Palamidessi : *Quantitative Aspects in Information Protection*
One of the concerns in the use of computer systems is to avoid the leakage of secret information through public outputs. Ideally we would like systems to be completely secure, but in practice this goal is often impossible to achieve. Therefore, it is important to devise methods to define and reason about the amount of leakage. In this talk, we illustrate various quantitative approaches to information leakage which have been recently developed in the area of security. We then make a connection with differential privacy, which is a very successful notion of privacy emerged from the area of statistical databases.
Finally, we generalize the notion of differential privacy so to make it applicable to domains other than databases. We start form the observation that the standard notion of differential privacy relies on the notion of Hamming distance on the set of databases, and

we extend it to arbitrary metric spaces. We show various examples, and we revise some of the fundamental results of differential privacy in this extended setting. As particular case studies, we consider applications to location-based services, and to smart meters.

Adeline Pierrot : *Trier des permutations avec des piles en série : un algorithme polynomial de décision dans le cas de deux piles connectées en série*
On présente un algorithme polynomial décidant si une permutation donnée en entrée est triable par deux piles connectées en série. L'existence d'un algorithme polynomial résolvant cette question est un problème longtemps resté ouvert depuis l'introduction du tri par piles par Knuth dans les années 60. On le clôt en introduisant une nouvelle notion, le tri par sas, qui est une restriction du tri par piles général. On résout d'abord le problème de décision dans le cas particulier du tri par sas, en utilisant un codage des procédures de tri par un bi-coloriage des permutations. Puis on résout le problème général en montrant qu'une procédure de tri général correspond à plusieurs étapes de tri pas sas qui doivent être compatibles.

Tania Richmond : *Le décodage des codes de Goppa appliqué à la cryptographie asymétrique*
Pour sécuriser les systèmes de communication, nous utilisons la Cryptographie. Pour corriger un maximum d'erreurs possible lors des transmissions, nous utilisons les codes correcteurs d'erreurs (et la Théorie des Codes). C'est dans ce contexte que se placent mes recherches de thèse. De plus, je m'intéresse à la façon dont les algorithmes sont traduits en programmes, que ce soit en logiciel ou en circuits pour le matériel. Grâce à cela, des failles de sécurité peuvent être trouvées, et mon but est de proposer des contre-mesures.

Joëlle Roué : *Amélioration des critères de résistance aux attaques différentielles* (avec Anne Canteaut)
Ce travail établit une nouvelle borne supérieure sur l'espérance de la probabilité d'une différentielle sur deux tours dans un chiffrement SPN, de même type que le standard AES. Cette borne permet de raffiner les critères de conception classiques : en particulier, sa valeur diffère généralement pour des fonctions équivalentes par transformation affine. Nous montrons également que les involutions sont, au sein d'une même classe, celles qui résistent le moins bien aux attaques différentielles.

Cheng Wan : *Coalition et délégation dans les jeux de congestion*
Nous examinons l'impact des comportements stratégiques comme coopération et délégation dans les jeux de congestion dans un réseau. Nous montrons que la formation des coalitions par les joueurs non-atomiques bénéficie à tous dans les réseaux de deux sommets et d'arcs parallèles, et que la formation des coalitions par des joueurs composites bénéficie aux autres et à la société en cas de deux arcs. Dans le cadre des jeux divisibles en entiers, nous introduisons une nouvelle classe de jeux appelés jeux de délégation et nous y définissons les notions d'équilibre puis nous montrons leur existence par construction. Nous comparons cette approche avec des notions comme équilibre parfait en sous-jeux et induction en amont/aval.