Programme des Journées de l'Informatique Mathématique (JNIM 2013)
Les 21 et 22 janvier 2013 à l'ENS Lyon
Amphi Mérieux, situé sur le site Monod.

Lundi 21 janvier

10H30 - 11H : accueil autour d'un café.

11H -12H. David Coeurjolly (Liris, Lyon) (**Conférence invitée).** *Géométrie discrète pour l'analyse de formes*

12H15 - 13H. Guillaume Chapuy (LIAFA, Univ Paris 7) pour le GT Alea. *Treillis de Tamari, intervalles, et énumération*

13H - 14H30. Déjeuner

14H30 - 15H15. Nicolas Markey (LSV, ENS Cachan) pour les GT Vérification et Jeux. *Logiques temporelles pour les systèmes multi-agents*
15H15 - 16H : Sylvie Boldo (Inria Saclay) pour le GT Arith. *Validation formelle de programmes numériques.*

16H - 16H30. Pause café

16H30 - 17H15. Damien Pous (LIP, ENS Lyon) pour le GT GeoCal. *Checking NFA equivalence with bisimulations up to congruence*

17H15 - 18H30. Discussion autour du GdR IM
18H30 - 20H. Buffet

Mardi 22 janvier

9H - 10H. Anca Muscholl (Labri, Bordeaux) (**Conférence invitée).** *Games and synthesis: going distributed*

10H15 - 11H. Louis Esperet (GScop, Grenoble) pour le GT Graphes. *Applications d'une preuve algorithmique du Lemme Local de Lovasz*

11H - 11H30. Pause café

11H30 - 12H15. Gregory Kucherov (LIGM, Marne-la-Vallée) pour le GT Comatege. *Seed-based sequence search: some theory and some applications*
12H15 - 13H. Laurent Vuillon (LAMA, Université de Savoie) pour le GT GeoDis. *Pavages, polytopes et polycubes*

13H - 14H30. Déjeuner

14H30 - 15H15. Yann Strozecki (PRISM, Versailles) pour le GT CMF. *Problèmes d'énumération, méta-algorithmes et complexité*
15H15 - 16H. Vadim Lyubashevsky (Inria/ENS Ulm) pour le GT C2. *Lattice Based Crypto: Answering Questions You Don't Understand*

Résumés des exposés (ordre alphabétique)

Sylvie Boldo (Inria Saclay) *Validation formelle de programmes numériques.* (Travail commun avec François Clément, Jean-Christophe Filliâtre, Micaela Mayero, Guillaume Melquiond, et Pierre Weis)

Cet exposé montrera les résultats du projet FOST: nous avons formellement prouvé un programme C implémentant un schéma numérique simple pour la résolution de l'équation des ondes acoustiques en dimension 1. Nous avons annoté ce programme et l'avons complètement prouvé. Cela inclut l'absence d'erreur à l'exécution, la majoration mathématique usuelle de l'erreur de méthode due au schéma numérique et bien sûr une borne sur les erreurs d'arrondi.

Guillaume Chapuy (CNRS et LIAFA, Univ Paris 7) *Treillis de Tamari, intervalles, et énumération.* (Travail commun avec Mireille Bousquet-Mélou (Bordeaux) et Louis-François Préville-Ratelle (Talca).)

L'ensemble des arbres binaires de taille n est muni d'une structure d'ordre partiel, le "Treillis de Tamari". En 2010, François Bergeron a présenté plusieurs conjectures concernant l'énumération d'intervalles dans ce treillis, motivées par des considérations de combinatoire algébrique.
Étonnamment, la résolution de ces conjectures emprunte plusieurs techniques au domaine de l'énumération des cartes planaires, notamment l'écriture d'équations à variables catalytiques. J'essaierai d'expliquer ce que sont ces équations dans le cas «classique», ce que l'on sait en dire, et à quelles difficultés nouvelles nous avons été confrontés, notamment à une variante «différentielle» de ces équations. Je conclurai avec quelques perspectives. D'une part, une meilleure compréhension de ces nouvelles équations «différentielles-catalytiques» est souhaitable. D'autre part, l'étude des intervalles de Tamari aléatoires semble, par analogie avec les cartes planaires, devenir un sujet abordable.

David Coeurjolly (Liris, Lyon) *Géométrie discrète pour l'analyse de formes*

La géométrie discrète s'intéresse à la résolution de problèmes géométriques en exploitant les spécificités du support sur lequel la donnée est définie. L'appellation anglo-saxonne "digital geometry" est sans doute plus explicite car elle met l'accent sur le
caractère régulier de ce support (partie de Z^n, réseau, ...). Pour continuer sur la terminologie, cette thématique rejoint les disciplines de "discrete geometry" ou géométrie algorithmique dans le sens où les objets sont décrits en extension de manière finie. Cette thématique s'intègre, au moins d'un point de vue historique, dans l'analyse de formes dans des images numériques 2D ou 3D mais a trouvé de nombreux échos en modélisation géométrique, en arithmétique, en combinatoire des mots, en complexité, ...
L'objectif de cet exposé sera de faire un survol subjectif de cette discipline en se focalisant sur certaines activités relatives à l'analyse géométrique d'objets discrets (par exemple analyse volumique et opérateurs différentiels de contours).

Louis Esperet (GScop, Grenoble) *Applications d'une preuve algorithmique du Lemme Local de Lovasz*

Le lemme local de Lovasz est un outil très utilisé permettant de montrer de manière simple l'existence d'objets combinatoires avec certaines propriétés. Il dit que si on a un certain nombre d'événements qui ont tous une probabilité < 1 et que ceux-ci ne sont pas trop interdépendants, la probabilité qu'aucun événement n'arrive est non nulle. Le problème était (jusqu'à une date

récente) que cet outil n'était pas constructif. J'expliquerai les idées (très élégantes et étonnamment simples) qui ont permis à Moser d'obtenir une version algorithmique de ce lemme en 2009. Je donnerai deux exemples :
1) Si on a une suite d'alphabets A_1, A_2, ..., A_n de quatre lettres chacun on peut trouver (efficacement) dans chaque alphabet A_i une lettre a_i telle que le mot a_1 a_2 ... a_n n'a pas de carré.
2) Toute instance de k-SAT dans laquelle chaque clause a des variables en commun avec au plus 2^(k-3) clauses est satisfiable (et on peut trouver une bonne assignation vrai/faux aux variables de manière efficace).

Gregory Kucherov (LIGM, Marne-la-Vallée) *Seed-based sequence search: some theory and some applications*. (Travail commun avec Laurent Noé)

We present a survey of main results on the "spaced seeds" paradigm for sequence search.This technique, invented around 2002, attracted a lot of attention due to its applications in biological sequence analysis. After introducing the context, main ideas and motivations, we focus on two settings: lossless and lossy searches. For each of these two frameworks, we present main developments and results. We briefly mention bioinformatics applications, including applications to new generation sequencing technologies.

Vadim Lyubashevsky (Inria/ENS Ulm) *Lattice Based Crypto: Answering Questions You Don't Understand*

The first construction of a fully-homomorphic encryption scheme in 2009 has arguably been the most exciting result in cryptography of the past decade. Such a scheme allows one to compute any function on encrypted inputs, which is analogous to giving correct answers to questions you don't understand. In this talk, I will present the main ideas that go into constructing this primitive, and will give an almost complete description of one such scheme.

Nicolas Markey (LSV, ENS Cachan) *Logiques temporelles pour les systèmes multi-agents*

Les jeux sur les graphes permettent de modéliser des systèmes en interaction avec leur environnement, dans le cadre de la vérification et de la synthèse de contrôleur. Pour exprimer des propriétés de ces systèmes, la logique ATL a été proposée : elle étend CTL avec la possibilité de quantifier sur les stratégies des joueurs. Dans cet exposé, je présenterai ATL et montrerai qu'elle permet essentiellement d'exprimer des propriétés de jeux à somme nulle (correspondant au contrôle dans un environnement hostile). Je présenterai ensuite une extension récente pour les jeux à somme non-nulle (systèmes multi-agents).

Anca Muscholl (Labri, Bordeaux) *Games and synthesis: going distributed*

Computer-assisted analysis of distributed, asynchronous systems is a notoriously challenging task. Notions like automata, logic and games, which are fundamental when reasoning about sequential systems, become more complex and harder to understand. In this talk we will give an overview of the problem of distributed synthesis of asynchronous systems.

Damien Pous (LIP, ENS Lyon) *Checking NFA equivalence with bisimulations up to congruence*
(Travail commun avec Filipo Bonchi)

We introduce "bisimulation up to congruence" as a technique for proving language equivalence of non-deterministic finite automata. Exploiting this technique, we devise an optimisation of the classical algorithm by Hopcroft and Karp which, as we show, is exploiting a weaker

"bisimulation up to equivalence" technique. The resulting algorithm can be exponentially faster than the recently introduced "antichain algorithms".

Yann Strozecki (PRISM, Versailles) *Problèmes d'énumération, méta-algorithmes et complexité*

Cet exposé traite de la complexité d'énumérations, c'est à dire l'étude d'algorithmes qui listent efficacement et sans répétition toutes les solutions d'un problème. Nous allons montrer comment modéliser des problèmes d'énumérations comme des requêtes sur des structures finies (méthode logique), des polynômes (méthode algébrique) ou des points dans des formes géométriques simples (méthode combinatoire). On peut prouver qu'il existe de bons algorithmes d'énumération quand, par exemple, les formules ou les polynômes sont suffisamment simples. Je conclurai par le lien entre énumération et génération aléatoire de solutions et quelques questions de complexité afférentes.

Laurent Vuillon (LAMA, Université de Savoie) *Pavages, polytopes et polycubes* (Travail commun avec Ian Gambini)

Dans cet exposé, nous allons présenter des techniques pour paver le plan et l'espace par translation d'une tuile. Nous reviendrons sur le théorème de Beauquier-Nivat qui caractérise les polyominos qui pavent le plan par translation. Puis, nous tenterons de généraliser ce théorème en dimension 3. Nous montrerons alors les 5 polytopes convexes de Fedorov qui sont des modèles de pavages de l'espace. Nous nous attarderons sur le plus complexe de ces polytopes qui se révèle être un permutoèdre. Au travers d'exemples provenant de la théorie des pavages mais aussi de la cristallographie et de la métallurgie, nous verrons les différents pavages de l'espace et les réseaux associés. Nous focaliserons ensuite sur le pavage de l'espace avec des pièces non-convexes et des polycubes qui pavent l'espace avec plus de faces que les solides de Fedorov en ont. Et donc qu'il n'y aura certainement pas d'analogue du théorème de Beauquier-Nivat en dimension 3. Puis, nous parlerons des pavages classiques apériodiques du plan et de l'espace (comme ceux de Penrose, Robinson, Wang, Danzer). Enfin, nous étudierons le problème ouvert du pavage apériodique de l'espace par des copies d'une seule tuile.