

# PREMIERES JOURNEES ANNUELLES DU GDR INFORMATIQUE MATHEMATIQUE (IM)

Les 1er et 2 Février à L'INSTITUT HENRI POINCARÉ  
Amphi Darboux ou Hermite

## Programme

### Jeudi 1er février

**10H: Conférence invitée:** Robin Milner (University of Cambridge)  
"Bigraphs, confluence and the lambda-calculus"

**11H-11H30:** Eric Fusy (Projet ALGO, INRIA Rocquencourt et LIX, Ecole Polytechnique) "Dessin de triangulations: algorithmes, combinatoire, et analyse"

**11H30-12H:** Ioan Todinca (LRI - Paris XI et LIFO - Université d'Orléans)  
"Complétions d'intervalles minimales et largeur linéaire (pathwidth) des graphes"

**12H-12H30:** Lucien Ilie (University of London Ontario et IGM, Marne la Vallée)  
"Repetitions in Strings"

### **12H30 -14H: Déjeuner-buffet à l'IHP**

**14H-14H30 :** Frédéric Jouhet (Institut Camille Jordan, Université de Lyon1)  
" q-analogue d'un problème de divisibilité de Zudilin, via le lemme de Bailey"

**14H30-15H :** Damien Stehlé (CNRS et Ecole Normale Supérieure de Lyon)  
"Arithmétique flottante et algorithmes de réduction de réseaux euclidiens"

**15H-15H30 :** Marie-Pierre Béal (IGM, Marne la Vallée)  
"Conjugaison d'automates"

### **15H30-16H : Pause**

**16H-16H30 :** Delia Kesner (PPS, Université Paris 7)  
"La théorie des substitutions explicites revisitée"

**16H30-17H :** Francis Lazarus (GIPSA-lab, INPG, Grenoble)  
"Homotopie et optimisation de courbes sur les surfaces combinatoires"

**17H-17H30 :** Pascal Schreck (LSIIT, Université de Strasbourg)  
"Modélisation géométrique par contraintes"

## Vendredi 2 février

**9H: Conférence invitée:** Christos Papadimitriou (University of California at Berkeley) "Complexity of Nash equilibria"

**10H-10H30:** Daniel Augot (Projet Codes, INRIA Rocquencourt)  
"Application des algorithmes de décodage par interpolation en cryptanalyse"

**10H30-11H:** Frédéric Magniez (LRI, Paris XI)  
"Marche quantique"

**11H-11H30:** Pascal Koiran (Ecole Normale Supérieure de Lyon)  
"Problèmes de décision et d'évaluation en complexité algébrique"

**11H30 -12H30 : Informations et discussions sur le GDR IM**

**12H30-14H : Dejeuner-buffet à l'IHP**

**14H-14H30 :** Rémy Malgouyres (LLAIC, Université Clermont-Ferrand)  
"Estimateurs discrets de grandeurs différentielles"

**14H30-15H :** Jean Goubault-Larrecq (LSV/ENS Cachan, et INRIA projet SECSI).  
"Capacités, crédibilités, prévisions: quelques modèles élégants de choix probabilistes et non déterministes"

**15H-15H30 :** Wieslaw Zielonka (LIAFA, Université Paris 7)  
"Quand la mémoire est-elle inutile pour jouer optimalement dans les jeux infinis à deux joueurs? "

### Résumés.

**Robin Milner** (Cambridge) "Bigraphs, confluence and the lambda calculus"

The bigraph model is a generic process calculus, aiming to address pervasive computing but also to remain faithful to process calculi that have already proved their value in applications.

I shall introduce bigraphs mainly by example, rather than formally. The main focus of the talk is to treat the notion of confluence, which is well understood in the lambda calculus, in the wider setting where we may be modelling physically distributed systems. It seems that confluence ---i.e. non-interference among possible actions--- is just as important in these physical systems as in a calculus of functions. At the same time, there are more ways in which possible actions can interfere with each other!

Nonetheless, as I shall show, one can find conditions for confluence that are not too stringent; they are certainly satisfied by the lambda calculus.

**Eric Fusy** (Projet ALGO, INRIA Rocquencourt et LIX, Ecole Polytechnique)  
"Dessin de triangulations: algorithmes, combinatoire, et analyse"  
(Proposé par le GT Alea)

L'étude combinatoire de triangulations du plan dites irréductibles (sans triangle séparateur) permet d'obtenir une algorithmique efficace pour le dessin, la génération aléatoire, et le codage de ces triangulations. Par simulation, on observe que la grille utilisée par l'algorithme de dessin a avec grande probabilité une taille asymptotique déterminée par le nombre de sommets. Nous verrons comment ce phénomène s'analyse en combinant des outils de combinatoire bijective et de combinatoire analytique.

**Ioan Todinca** (LRI - Paris XI et LIFO - Université d'Orléans)  
"Complétions d'intervalles minimales et largeur linéaire (pathwidth) des graphes"  
(Proposé par le GT Graphes)

Les graphes étant des objets complexes, on tente souvent de les "simplifier" si possible sans leur apporter beaucoup de modifications. Une technique courante consiste à rajouter des arêtes au graphe en entrée afin d'obtenir un graphe plus simple. Une complétion d'intervalles d'un graphe quelconque  $G$  est un graphe d'intervalles  $H$ , obtenu à partir de  $G$  en lui rajoutant des arêtes. On cherche classiquement à minimiser certains paramètres comme le nombre d'arêtes rajoutées ou la taille de la clique de cardinal maximum de  $H$ . Ces problèmes étant NP-difficiles, nous nous intéressons aux complétions d'intervalles minimales, où l'on demande simplement à ce que l'ensemble d'arêtes ajoutées soit minimal par inclusion. Je montrerai comment calculer une telle complétion et j'évoquerai des applications au calcul de la largeur linéaire pour des graphes particuliers.

**Lucian Ilie** (University of London Ontario et IGM, Marne la Vallée)  
"Repetitions in strings"  
(Proposé par le GT Comatege)

Repetitions in strings constitute one of the most fundamental areas of string combinatorics with very important applications to text algorithms, data compression, or analysis of biological sequences. Squares have been studied already a century ago at the foundations of stringology and runs (maximal repetitions) helped obtaining the first linear-time algorithms for computing all repetitions in a string. I shall discuss a number of recent results and open problems concerning the number of squares and runs in a string.

**Frédéric Jouhet** (Institut Camille Jordan, Université de Lyon 1)  
" $q$ -analogue d'un problème de divisibilité de Zudilin, via le lemme de Bailey"  
(proposé par le GT CombAlg)

Zudilin a publié récemment la résolution d'un problème de divisibilité de sommes de coefficients binomiaux, problème posé à l'origine par Schmidt et résolu partiellement par Strehl. Ces sommes de coefficients binomiaux apparaissent dans le cadre de la preuve par Apéry de l'irrationalité de  $\zeta(3)$ . Dans le même article, Zudilin pose la question de trouver et de résoudre un  $q$ -analogue de ce problème de divisibilité. En utilisant le lemme de Bailey et son extension due à Andrews, nous donnons une réponse à la question de Zudilin, ainsi que d'autres applications généralisant des résultats de divisibilité dus à Calkin.

**Damien Stehlé** (CNRS et Ecole Normale Supérieure de Lyon)

"Arithmétique flottante et algorithmes de réduction de réseaux euclidiens"  
(proposé par le GT Arith)

La réduction des réseaux euclidiens est un outil central dans de nombreux domaines des mathématiques et de l'informatique. On peut entre autres citer la théorie algorithmique des groupes, la cryptographie et le calcul formel. Certaines de ses applications requièrent une algorithmique sous-jacente aussi efficace que possible. Nous verrons en quoi l'utilisation de l'arithmétique flottante plutôt qu'une arithmétique rationnelle ou entière, permet d'améliorer les performances des algorithmes de réduction, en théorie et en pratique. En contrepartie, un effort significatif doit être fourni pour prouver que ces algorithmes demeurent corrects.

Conjugaisons d'automates

**Marie-Pierre Béal** (IGM, Marne la Vallée) "Conjugaison d'automates"

(proposé par le GT SDA2)

Nous présentons deux notions voisines de conjugaison. La première est la notion d'isomorphisme entre deux systèmes dynamiques symboliques. La deuxième, inspirée de la première, désigne une relation entre deux automates finis avec multiplicité. Alors que l'on ignore si la conjugaison entre deux systèmes dynamiques symboliques est décidable, on montrera que deux automates à multiplicité sont reliés par une chaîne de conjugaisons si et seulement si ces automates sont équivalents.

(Travail en collaboration avec Sylvain Lombardy et Jacques Sakarovitch)

**Delia Kesner** (PPS, Université Paris 7)

"La théorie des substitutions explicites revisitée"  
(Proposé par le GT LAC)

Les calculs avec substitutions explicites ont émergé de manière très naturelle dans plusieurs domaines de l'informatique comme la programmation fonctionnelle et/ou logique, la théorie de la démonstration, la concurrence, les langages orientés objets, etc. Des nombreux systèmes complexes avec substitutions explicites ont été développés ces dernières 15 années afin de capturer les bonnes propriétés opérationnelles du système original (avec méta-substitution) qu'ils visaient implémenter.

Nous passerons en revue les travaux dans le domaine en pointant les motivations et défis qui ont guidés le développement de tous ces systèmes. Nous utiliserons ensuite une technologie très simple pour établir une théorie générale des substitutions explicites pour le lambda-calcul vérifiant des bonnes propriétés comme la simulation d'un pas de beta-réduction, la confluence sur les méta-termes, la préservation de la normalisation forte, la normalisation forte pour les termes typés et la composition forte. Nous établirons aussi un lien entre notre théorie et les réseaux de démonstration de la logique linéaire.

**Francis Lazarus** : GIPSA-lab, INPG-CNRS UMR 5216

"Homotopie et optimisation de courbes sur les surfaces combinatoires"

(Proposé par le GT GeoAlgo)

On assiste depuis une quinzaine d'années au sein de la communauté de géométrie algorithmique à un intérêt croissant pour des questions de topologie. J'illustrerai ce constat par un bref tour d'horizon sur des questions relatives à l'homotopie des courbes sur les surfaces combinatoires, en insistant sur les techniques utilisées pour y répondre.

**Pascal Schreck** (LSIIT, Université de Strasbourg)

"Modélisation géométrique par contraintes"

(Proposé par le GT Modélisation géométrique)

Pour l'utilisateur d'un logiciel de modélisation géométrique, modéliser un objet, ou une scène géométrique, signifie souvent le construire avec les outils fournis par le logiciel en vue de le manipuler (c'est-à-dire le visualiser, en explorer les propriétés, naviguer à l'intérieur, etc.). Malgré la puissance de description qui a été autorisée par les progrès dans ces domaines (par exemple en modélisation à base topologique ou en courbes et surfaces), l'utilisateur peu expérimenté se trouve souvent démuné lorsqu'il veut mettre ces outils en pratique. Depuis quelques années, des chercheurs venus d'horizon différents ont développé indépendamment des méthodes pour franchir ce cap et aider l'utilisateur dans sa description des objets. On retrouve là une évolution générale en informatique, mais plus particulièrement dans le domaine des langages de programmation partis de langages où les questions du matériel influent fortement sur la manière de programmer, jusqu'à avoir un point de vue de haut niveau sur les problèmes à résoudre. Une action spécifique du CNRS sur le sujet (l'AS contraintes géométriques) a permis de faire une synthèse sur le sujet : parmi les différents thèmes qui ont été présentés, on trouve la modélisation par contraintes géométriques en CAO. Je me propose de broser rapidement le paysage des problématiques posées par cette AS, d'approfondir un peu plus le domaine de la résolution de contraintes géométriques que j'illustrerai par un travail récent concernant la résolution de contraintes en dimension 3.

**Christos Papadimitriou** (University of California at Berkeley) "Complexity of Nash equilibria" (exposé invité)

In 1951, Nash proved that every game has a Nash equilibrium. The proof is non-constructive, reducing the existence of Nash equilibria to that of Brouwer fixpoints. Whether Nash equilibria can be computed efficiently had remained open. I shall outline our recent proof (with Daskalakis and Goldberg) that the problem is intractable (technical term: PPAD-complete). The proof is by a reduction from Brouwer, establishing a close computational link between two important existence theorems of the 20th century.

**Daniel Augot** (Projet Codes, INRIA Rocquencourt) "Application des algorithmes de décodage par interpolation en cryptanalyse"  
(Proposé par le GT C2)

Je présenterai l'algorithme de Sudan, de décodage des codes de Reed-Solomon, après avoir d'abord présenté ceux-ci comme des codes d'interpolation. Cet algorithme, ainsi que son amélioration due à Guruswami-Sudan, permet de corriger un grand nombre d'erreurs. Cette propriété peut-être utilisée pour cryptanalyser le système de chiffrement à clé secrète de Knudsen et Nyberg, qui est cependant un système d'école. Ensuite, je montrerai un algorithme analogue pour décoder les codes de Reed-Muller, qui sont une généralisation multivariée des codes de Reed-Solomon, mais qui correspondent à une vision plus réaliste des systèmes de chiffrement. Ce dernier algorithme de décodage permet d'obtenir de bonnes approximations de certaines versions réduites de l'algorithme de chiffrement DES, approximations qui peuvent être utilisées en cryptanalyse.

**Frédéric Magniez** (LRI, Université Paris XI) "Marche quantique"  
(Proposé par le GT IQ)

Nous proposons une nouvelle méthode pour construire des algorithmes quantiques pour trouver un élément "marqué" dans l'espace des états d'une chaîne de Markov classique. Cet algorithme est basé sur une marche quantique définie à partir de la chaîne de Markov. La nouvelle idée principale est d'utiliser l'estimation quantique de phase, l'ingrédient clé de l'algorithme quantique de factorisation de Shor. Ainsi nous généralisons les champs d'applications des précédentes approches d'Ambainis et Szegedy, tout en étant conceptuellement plus simple. Le résultat est une méthode générique intégrant la partie quantique et pouvant être appliquée sans connaissance a priori. Nous illustrerons notre méthode en réécrivant simplement et en améliorant plusieurs algorithmes quantiques.

**Pascal Koiran** (Ecole Normale Supérieure de Lyon)  
"Problèmes de décision et d'évaluation en complexité algébrique"  
(Proposé par le GT CMF)

Deux catégories principales de problèmes sont étudiés en complexité algébrique :

les problèmes de décision et les problème d'évaluation. L'évaluation du permanent ou du déterminant d'une matrice sont des exemples typiques de problèmes d'évaluation. De tels problèmes peuvent être étudiés dans le cadre du modèle de calcul algébrique proposé par Valiant. Décider si un polynôme en plusieurs variables a une racine réelle est un exemple typique de problème de décision. Ce problème est NP-complet dans le modèle de Blum-Shub-Smale de calcul sur les nombres réels.

Dans cet exposé je présenterai les modèles de Valiant et de Blum-Shub-Smale, et si le temps le permet je présenterai un théorème de transfert obtenu avec Sylvain Périfel (à paraître dans STACS 2007) qui établit des liens entre problèmes de décision et problèmes d'évaluation : nous avons montré que si certains problèmes d'évaluation sont faciles alors d'autres problèmes de décision (dont le problème NP-complet mentionné ci-dessus) sont faciles également.

**Rémy Malgouyres** (LLAIC, Université de Clermont-Ferrand)

"Estimateurs discrets de grandeurs différentielles"

(proposé par le GT GeoDis)

Dans cet exposé, nous présenterons une méthode de calcul des dérivées, à différents ordres, pour des courbes dans le plan discret  $Z^2$ . La méthode repose sur l'utilisation itérée de convolutions élémentaires. Cette approche s'inspire du cadre «scale space», avec des masques de convolutions bien particuliers. Nous allons montrer que moyennant quelques hypothèses sur la courbe continue et étant donnée une borne d'erreur à respecter, un pas de discrétisation suffisamment petit et un masque adéquat permettent d'obtenir de bons estimateurs pour les tangentes et la courbure en chaque «point» de la courbe discrète. A la fin de l'exposé, nous présenterons l'extension de cette méthode au cas des surfaces discrètes.

**Jean Goubault-Larrecq** (LSV/ENS Cachan, et INRIA projet SECSI).

"Capacités, crédibilités, prévisions: quelques modèles élégants de choix probabilistes et non déterministes" (proposé par le GT GeoCal)

J'aime bien faire du neuf avec du vieux. Je montrerai que certains concepts inventés par des économistes dès les années 1950 et par des statisticiens dans les années 1960 peuvent être remis au goût du jour pour fournir des modèles de systèmes de transition mêlant choix probabiliste et choix non déterministes (démoniaque, angélique, chaotique,... au choix), et ce même dans des espaces à états continus. L'accent sera sur les capacités, l'intégration de Choquet, la notion de crédibilité. La notion de prévision, dérivée des précédentes par un théorème de représentation à la Riesz, permet, elle de donner des modèles sémantiques simples de langages de programmation mêlant les mêmes séries de choix, notamment via des monades de choix combinés, probabilistes et non déterministes (de nouveau, au choix, démoniaque, angélique, chaotique).

**Wieslaw Zielonka** (LIAFA, Université Paris 7)

"Quand la mémoire est-elle inutile pour jouer optimalement dans les jeux infinis à deux joueurs?" (proposé par le GT Jeux)

Given a stochastic or a deterministic game, when there exists optimal pure memoryless strategies? Usually it is simpler to answer this question for one player games. It turns out however that, if a given payoff mappings admits optimal pure memoryless strategies for one player games, then it admits optimal pure memoryless strategies for two player perfect information games.