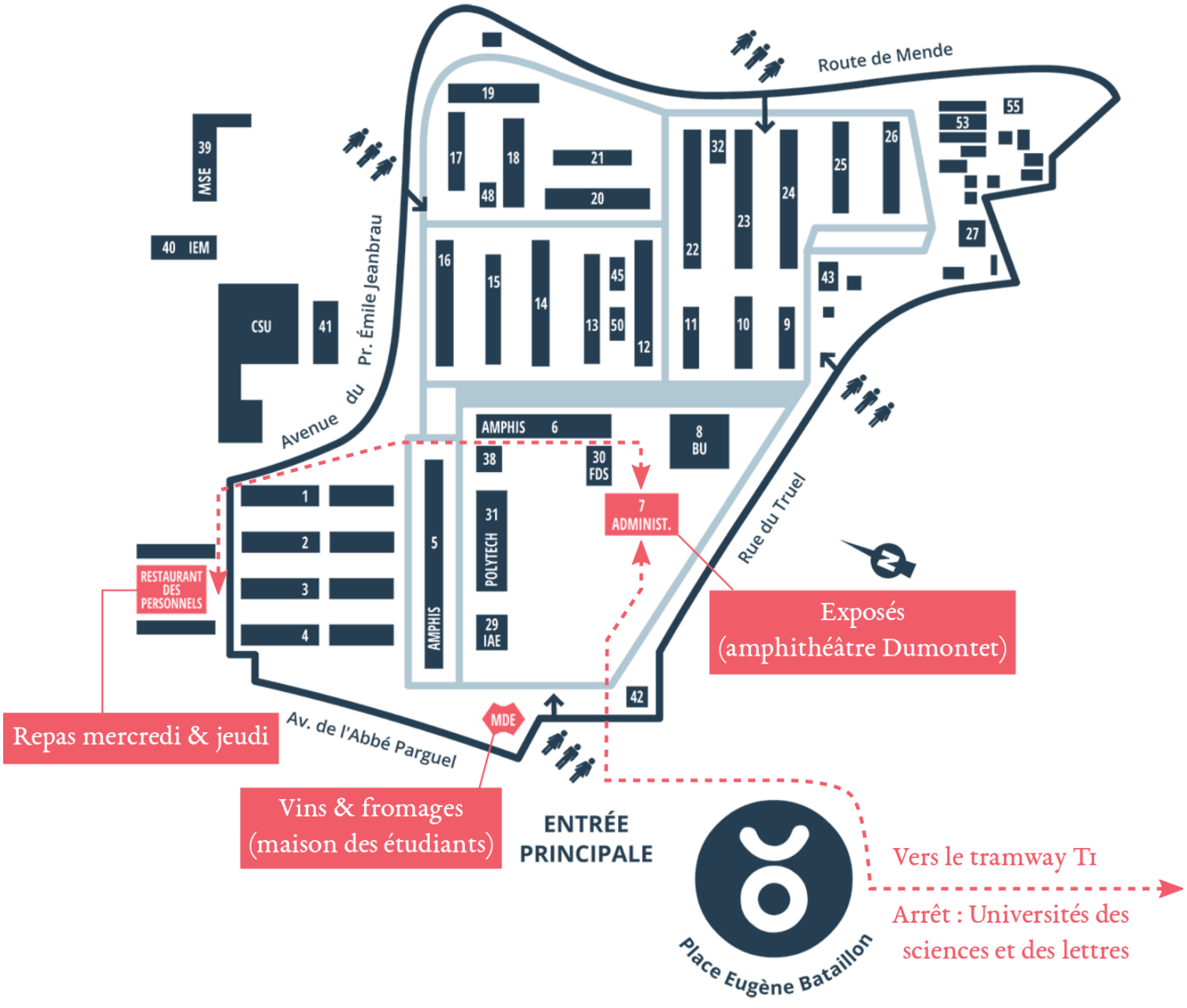
Journées nationales du GDR IM

14 – 16 mars 2017
Université de Montpellier



Mardi 14 mars

13h30	Accueil	
14h	Présentation des journées	
14h30	**Eric Goles** *Réseaux d'automates*	Universidad Adolfo Ibáñez, Santiago, Chili
15h30	Evelyne Hubert *Computing Symmetric cubatures: A moment matrix approach*	INRIA Sophia Antipolis Méditerranée
16h05	Pause	
16h35	Mathieu Liedloff *Algorithmes modérément exponentiels pour un problème d'étiquetage de graphes*	LIFO, U. Orléans
17h10	Amos Korman *From Ants to Query Complexity*	IRIF, CNRS, U. Paris VII
17h45	Posters	
19h	Vin et fromages	Maison des étudiants

Mercredi 15 mars

9h30	**Dimitrios M. Thilikos** LIRMM, CNRS, U. *Montpellier* *Algorithm design for topologically structured graphs*	
10h30	Olivier Bournez *Programmer avec des équations différentielles*	LIX, École Polytechnique
11h05	Pause + Posters	
11h55	Ines Klimann *Des automates au service de la théorie combinatoire des groupes*	IRIF, U. Paris VII
12h30	Arnau Padrol Sureda *On the extension complexity of polytopes*	IMJ, U. Paris VI
13h15	Repas	Restaurant des personnels
14h30	**Mohsen Ghaffari** *On the complexity of Local Distributed Graph Problems*	ETH Zürich, Suisse
15h30	Nathalie Bertrand *Controlling probabilistic systems under Partial Observation*	IRISA, INRIA Rennes Bretagne-Atlantique
16h05	Riccardo Biagioli *La profondeur dans les groupes de Coxeter classiques*	ICJ, U. Claude Bernard Lyon 1
16h40	Pause + Posters	
17h	Assemblée générale du GDR	
18h	Réunion du comité directeur du GDR	

Jeudi 16 mars		
9h30	**Sihem Amer-Yahia** *Why does crowdsourcing need (more) math?*	LIG, CNRS, Grenoble
10h30	Emmanuel Prouff *Securing Finite Field Arithmetic in Embedded Systems*	Safran Identity and Security, Paris
11h05	Pause	
11h30	Stefan Mengel *Knowledge Compilation in Artificial Intelligence and Databases*	CRIL, CNRS, U. Artois
12h05	Gilles Didier *Pattern matching optimal*	IMM, CNRS, U. Aix-Marseille
12h40	Xavier Provençal *Generation of digital planes using generalized continued-fractions algorithms*	LAMA, U. Savoie Mont Blanc
13h15	Repas	Restaurant des personnels

Organisateurs locaux

Christophe Paul
Eleonora Guerrini
Bruno Grenet
Alexandre Pinlou

Comité directeur du GDR IM

Arnaud Durand
Jean-Michel Muller

Guillaume Theyssier
Laurent Imbert
Frédéric Magniez
Natacha Portier
Philippe Langlois
Valérie Berthé
Brigitte Vallée
Julien Clément

Exposés pléniers

Eric Goles (Universidad Adolfo Ibáñez, Santiago, Chili)
Réseaux d'automates

Un réseau d'automates booléen est un système dynamique discret à deux états (0 et 1) sur un graphe fini. Nous allons présenter quelques exemples généraux et des résultats particuliers sur les Automates Cellulaires à une et deux dimensions ainsi que des applications biologiques (réseaux de régulation génétique) et à la modélisation des problèmes sociaux (modèle de Schelling de ségrégation et modèle de champ social de Sakoda).

Dimitrios M. Thilikos (LIRMM, CNRS, U. Montpellier)
Algorithm design for topologically structured graphs

Several techniques in algorithmic graph theory are focusing on graphs with certain topological characteristics. In many cases, structural characteristics such as planarity, surface embeddability, tree-decomposability, or diverse versions of "flatness" can facilitate the design of efficient algorithms and, under certain assumptions, can offer algorithmic meta-theories combining tolls from algorithms, logic, and combinatorics. In this talk, we present some related techniques of algorithmic design in graphs in parameterized computation.

Mohsen Ghaffari (ETH Zürich, Suisse)
On the complexity of Local Distributed Graph Problems

À venir

Sihem Amer-Yahia (LIG, CNRS, Grenoble)
Why does crowdsourcing need (more) math?

Crowdsourcing is the act of posting an open call to hire cheap, immediate, skilled, and easily accessible labor online. Is is also a place where one finds work, possibly with a remuneration. This field has evolved from being industry-driven to becoming a major research field.Researchers have been relying on computational mathematics to solve key questions in crowdsourcing. In particular, mathematical optimization, algorithmic game theory, and graph theory, are heavily used to study task assignment and task completion, worker incentivization schemes, and learning workers' skills.I will describe how task assignment, a key process in crowdsourcing, has been formalized and solved so far and will argue for the need to involve more mathematicians in reaching a better understanding of human workers online.Some of this is joint work with my student Julien Pilourdault and with colleagues Senjuti Basu Roy from the New Jersey Institute of Technology and Dongwon Lee from Penn State University.

Exposés courts

Evelyne Hubert (INRIA Sophia Antipolis Méditerranée)
Computing Symmetric cubatures: A moment matrix approach

A quadrature is an approximation of the definite integral of a function by a weighted sum of function values at specified points, or nodes, within the domain of integration. Gaussian quadratures are constructed to yield exact results for any polynomials of degree 2r-1 or less by a suitable choice of r nodes and weights. These nodes are the roots of the associated orthogonal polynomials. Cubature is a generalization of quadrature in higher dimension. The results there are not as clear cut as in univariate case. We propose an approach based on recent techniques for moment matrices. How to best exploit the symmetry of the standard domains (triangle, simplex, cube) is the main contribution. Using adapted bases of the polynomial ring allows to block diagonalize the moment matrix and thus provides a definite computational advantage.

Mathieu Liedloff (LIFO, U. Orléans)
Algorithmes modérément exponentiels pour un problème d'étiquetage de graphes

Nous nous intéresserons à la construction d'algorithmes exponentiels pour résoudre un problème NP-difficile d'étiquetage L(2,1) dans les graphes. Nous verrons une approche par branchement et une approche par programmation dynamique. Nous illustrerons ainsi la possibilité de concevoir des algorithmes certes exponentiels, mais plus rapides qu'une recherche exhaustive naïve.

Amos Korman (IRIF, CNRS, U. Paris VII)
From Ants to Query Complexity

À venir

Olivier Bournez (LIX, école Polytechnique)
Programmer avec des équations différentielles

Le but sera de te persuader de la chose suivante: si tu sais ce qu'est le nombre 0, le nombre 1, une addition, et une multiplication, et que tu te rappelles de ce qu'est une équation différentielle (ordinaire), alors tu peux définir et programmer plein de choses. Cela inclut présenter/réinventer/redécouvrir la complexité descriptive, la calculabilité et complexité en 35 minutes.

Ines Klimann (IRIF, U. Paris VII)
Des automates au service de la théorie combinatoire des groupes

Depuis les années 1960, les transducteurs apparaissent comme un outil à la fois simple et puissant pour engendrer des groupes. Simple parce que les transducteurs sous-jacents apparaissent comme un levier combinatoire pour l'étude des groupes, puissant de par la très grande variété des groupes engendrés. Ainsi les groupes engendrés par transducteur ont permis de répondre à certaines questions difficiles de théorie des groupes, ou d'apporter de nouvelles réponses plus simples à des problèmes déjà résolus. Dans cet exposé je reviendrai sur des problèmes de nature combinatoire sur lesquels les groupes engendrés par transducteur ont eu une grande influence.

Arnau Padrol Sureda (IMJ, U. Paris VI)
On the extension complexity of polytopes

The extension complexity of a polytope is the minimal number of facets of a polytope that can be linearly projected onto it. This apparently simple problem in combinatorial geometry has been the object of extensive research motivated from applications in linear programming and non-negative factorizations. Yet, many basic questions are still unresolved and there are very few polytopes for which the exact extension complexity is known. I will present some open questions and discuss the extension complexity of polygons and polytopes with few vertices.

Nathalie Bertrand (IRISA, INRIA Rennes Bretagne-Atlantique)
Controlling probabilistic systems under Partial Observation

The verification community has produced a number of interesting decidability and complexity results concerning the control of probabilistic systems under partial observation. These touch upon decision problems in probabilistic automata (over finite or infinite words), optimal strategies for unbounded horizon objectives in POMDP, and more. After presenting some of these existing results, I will list several possible research directions in this area.

Riccardo Biagioli (ICJ, U. Claude Bernard Lyon 1)
La profondeur dans les groupes de Coxeter classiques

Je présenterai une nouvelle statistique, appelée profondeur, définie récemment par Petersen et Tenner pour tout groupe de Coxeter W. La profondeur d'un élément w de W est égale au coût minimal d'un chemin valué partant de l'identité et finissant à w dans le graphe de Bruhat de W, où les arêtes ont un poids donné. Je donnerai des nouveaux résultats sur ce sujet dont des formules explicites pour la profondeur dans les groupes de Coxeter.

Emmanuel Prouff (Safran Identity and Security, Paris)
Securing Finite Field Arithmetic in Embedded Systems

Side Channel Analysis is a class of attacks which exploit leakages of information from a cryptographic implementation during execution. To defeat them, various techniques have been introduced during the two last decades, among which masking (aka implementation sharing) is a common countermeasure. The principle is to randomly split every sensitive intermediate variable occurring in the computation into several shares and the number of shares, called the order, plays the role of a security parameter. The main issue while applying masking to protect cryptographic implementations is to specify efficient schemes to secure the non-linear steps during the processing. Several solutions, applicable for arbitrary orders, have been recently published. Most of them start from the original concept of Private Circuits originally introduced by Ishai, Sahai and Wagner at Crypto 2003. In parallel, and in order to formally prove the security of the proposed masking schemes, the community has also made important efforts to define leakage models that accurately capture the leakage complexity and simultaneously enable to build accurate security arguments. It is worth noting that there is a tight link between masking/sharing techniques, secure Multi Party Computation, Coding Theory and also Threshold Implementations. During this talk, some of the main ideas developped to secure the implementation of finite field arithmetic in embedded devices will be presented, together with models which have been introduced to prove their security.

Stefan Mengel (CRIL, CNRS, U. Artois)
Knowledge Compilation in Artificial Intelligence and Databases

Knowledge compilation is a classic preprocessing technique from artificial intelligence that has recently also been used in the area of database theory. I will introduce knowledge compilation by giving some example applications. Then I will present some recent developments in the field including new strong lower bound techniques, applications in query answering on probabilistic databases and query answer enumeration.

Gilles Didier (IMM, CNRS, U. Aix-Marseille)

Pattern matching optimal

Le comportement d'un algorithme cherchant un motif donné dans texte peut être simulé par un automate dont les états s'interprètent des combinaisons de ses variables internes. Dans le cas où le motif est cherché dans un texte aléatoire qui suit un modèle Bernoulli (iid), la suite de ces états lors d'une exécution, suit une chaîne de Markov, qu'on sait expliciter et qui permet de déterminer la vitesse asymptotique de l'algorithme. Celle-ci est définie, relativement à un motif et aux fréquences d'un Bernoulli donnés, comme la moyenne limite du nombre de positions dont il avance à chaque caractère lu, en cherchant ce motif dans un texte aléatoire sous le modèle donné. Renversant le problème, on cherche à déterminer un automate (et donc un algorithme), dont la vitesse soit la plus grande possible pour chercher un motif donné dans un texte Bernoulli de fréquences également données. On montre qu'il existe un automate de vitesse maximale, parmi une large classe incluant ceux des algorithmes standards, dont les états sont en bijection avec un sous-ensemble des parties des positions du motif cherché. Un algorithme optimal en termes de vitesse asymptotique, peut ainsi être déterminé par énumération. Lorsque la longueur du motif rend impossible cette énumération, des heuristiques polynomiales qui ne parcourent qu'un sous-ensemble des états possibles, permettent d'obtenir des algorithmes efficaces. Ceux-ci sont plus rapides que les algorithmes standards, non seulement sur des textes aléatoires mais aussi sur de « vrais » textes.

Xavier Provençal (LAMA, U. Savoie Mont Blanc)

Generation of digital planes using generalized continued-fractions algorithms

We investigate a construction scheme for digital planes that is guided by generalized continued fractions algorithms. This process generalizes the recursive construction of digital lines to dimension three. Given a pair of numbers, Euclid's algorithm provides a natural definition of continued fractions. In dimension three and above, there is no such canonical definition. We propose a pair of hybrid continued fractions algorithms and show geometrical properties of the digital planes constructed from them.

Posters

Maxime Audinot (IRISA)
Analyse et Conception formelle d'Arbres d'Attaque

Attack tree is a classic kind of graphical model in security. It is mainly appreciated because it is intuitive and easy to read. But attack tree are constructed manually, which proves to be tedious and error-prone for real, big systems. Our goal in this work is to provide a formal framework for attack trees with respect to a formal model of the system under study. We apply our framework to the automated verification of the correctness of attack trees, and to the automated generation of attack trees. Verification and generation both rely on model-checking.

Tristan Charrier (IRISA)
Planification épistémique pour un système multi-agents

Le but est de faire de la planification épistémique, où l'on considère des agents artificiels pouvant prendre des décisions par rapport à leur environnement, les actions d'autres agents mais également ce qu'ils pensent des capacités de décision des autres agents. Le formalisme utilisé est celui de la logique épistémique dynamique. Les limites de la planification épistémique ainsi que des perspectives sont discutées.

Simon Cruanes (LORIA)
SMBC — SAT Modulo Bounded Checking

We describe a new approach to find models for a computational higher-order logic with datatypes. The goal is to find counter-examples for conjectures stated in proof assistants. The technique builds on narrowing but relies on a tight integration with a SAT solver to analyze conflicts precisely, eliminate sets of choices that lead to failures, and sometimes prove unsatisfiability. The architecture is reminiscent of that of an SMT solver. We present the rules of the calculus, an implementation, and some promising experimental results.

Xavier Ferry (LIFO)
Modeling concurrent behaviors as words

We propose a new word based model, so called Pre-Post-Pomset, making the exploration of pomsets space possible. Our new model stands to be a general model in the sense that some classical models used in specification of concurrent systems (Mazurkiewicz traces, Message sequence charts or Petri nets) can be specified within. Not only our model is general but also offers decidability results on the verification problem with respect to an MSO formula on pomsets.

Vincent Jugé (LSV)
Courcelle's theorem made dynamic

Dynamic complexity is concerned with the complexity of updating a solution to a problem when its input changes. A typical example is as follows: given an directed graph G and two pointed vertices s and t, you wish to know whether there exists a path from s to t in G. After your computation is complete, the graph is modified (e.g. by adding or deleting an edge): how should you proceed to update your answer at the least cost? Computing and storing auxiliary data, such as maintaining a covering forest, might be helpful in that regard. We consider a specific class for dynamic complexity, called DynFO. A dynamic problem belongs to this class if updates can be performed by applying first-order formulas. We show that a dynamic variant of Courcelle's theorem belongs to DynFO (up to a mild precomputation step). This is a joint work with Patricia Bouyer-Decitre and Nicolas Markey.

Alex Bredariol Grilo (IRIF)
Pointer Quantum PCPs and Multi-Prover Games

The quantum PCP (QPCP) conjecture states that all problems in QMA, the quantum analogue of NP, admit quantum verifiers that only act on a constant number of qubits of a polynomial size quantum proof and have a constant gap between completeness and soundness. Despite an impressive body of work trying to prove or disprove the quantum PCP conjecture, it still remains widely open. The above-mentioned proof verification statement has also been shown equivalent to the QMA-completeness of the Local Hamiltonian problem with constant relative gap. Nevertheless, unlike in the classical case, no equivalent formulation in the language of multi-prover games is known. In this work, we propose a new type of quantum proof systems, the Pointer QPCP, where a verifier first accesses a classical proof that he can use as a pointer to which qubits from the quantum part of the proof to access. We define the Pointer QPCP conjecture, that states that all problems in QMA admit quantum verifiers that first access a logarithmic number of bits from the classical part of a polynomial size proof, then act on a constant number of qubits from the quantum part of the proof, and have a constant gap between completeness and soundness. We define a new QMA-complete problem, the Set Local Hamiltonian problem, and a new restricted class of quantum multi-prover games, called CRESP games. We use them to provide two other equivalent statements to the Pointer QPCP conjecture: the Set Local Hamiltonian problem with constant relative gap is QMA-complete; and the approximation of the maximum acceptance probability of CRESP games up to a constant additive factor is as hard as QMA. This is the first equivalence between a quantum PCP statement and the inapproximability of quantum multi-prover games.

Renaud Vilmart (LORIA)
A Real Variant of the ZX-Calculus

The ZX-Calculus is a powerful diagrammatic language dealing with quantum evolutions. It is basically a generalisation of quantum circuits and comes with a set of transformation rules that preserve the represented matrix. The point of using diagrams in this field is the exponential reduction in size of the manipulated object. The matrices usually have complex coefficients, but this is not necessary. There seems to be no downside in using matrices with real coefficients (as long as negative numbers are allowed). The ZX-Calculus is suited for "standard" quantum evolution, and real rotations can only be obtained through composition of complex ones. We have founded the Y-calculus on the same principles as the ZX-Calculus, but so that it only deals with real matrices. We can exhibit links from and to the two languages, allowing us to "transport" some properties (universality, completeness, ...). We show that "standard" quantum evolutions can be efficiently simulated with real transformations, and we show we can use the Y-Calculus to extract the real and imaginary parts of a ZX-diagram.

Mathieu Laurière (NYU Shanghai)
Extended learning graphs for Triangle Finding

à venir

Alexandre Nolin (IRIF)
Robust Bell inequalities from communication complexity

à venir

Julien Destombes (LIRMM)
Pavages à la limite

J'y ferai une présentation des pavages, des résultats principaux, de quelques résultats de l'équipe sur eux et enfin j'exposerai mon travail : comment définir les "bords" d'un pavage, et ainsi considérer des pavages de niveau supérieur où chaque case de $\mathbb{Z}^2$ est constituée d'un pavage classique.

Thomas Leventis (I2M)
An equational description for a probabilistic lambda-calculus

The lambda-calculus is a well-known computation model, and it is quite useful to understand the effect of many primitives used in actual programming languages. Given how useful random algorithms are in practice, it was natural that some lambda-calculus enriched with a probabilistic primitive would appear. But so far terms in such probabilistic calculi were always studied through their execution: the semantics of the probabilistic primitive was described with a probabilistic reduction, and the behaviour of a term was given by all its possible reductions. In this setting it is necessary to fix a reduction strategy, different strategies describing entirely different semantics. We chose to use a different approach and to define a probabilistic calculus with a deterministic and contextual reduction. Then we could extend many standard properties and constructions of the lambda-calculus to the probabilistic case. In particular we proved a correspondence between the largest coherent sensible equational theory, the observational equivalence and some natural notion of Böhm trees.

Alice Pavaux (LIPN)
Inductive Data Types in Ludics

We investigate the representation of data types, and in particular inductive data types, in Ludics. Data types are either the usual base types used in programs, or their combination in order to present information in a structured way, for example: the booleans, the lists of natural numbers, the binary trees labeled by finite words over an alphabet, etc. Among those, the inductive data types can be described as the least fixed point of a certain operator. Ludics is a logical framework whose objects can be seen as an intermediary between formal proofs and programs. In this setting, types are modeled by sets of objects with the same computational behaviour, and there exist such "behaviours" corresponding to the inductive data types, which make Ludics a good environment to study the semantics of those types. Thanks to Kleene fixed point theorem, the internal structure of the representation of inductive data types is made explicit, which allows us to highlight some interesting properties.

Guilhem Gamard (LIRMM)
Coverability in One and Two Dimensions

This work deals with infinite one-dimensional and two-dimensional words, that is functions from $\mathbb{Z}$ and $\mathbb{Z}^2$ to a finite alphabet Σ. A finite word q is said to be a cover of an infinite word w if each position of w belongs to an occurrence of q. An infinite word might have several, or even infinitely many covers; in the latter case, we call it multi-scale coverable. The set of covers of an infinite word contains much information about its structure, and tells in some sense how “regular” it is. This poster sums up known results about coverability: what properties are implied by multi-scale coverability, how to determine the set of quasiperiods of a given word, how very regular families of words (periodic, Sturmian) can be described in terms of quasiperiods, and which of these results generalize to 2D. Connections with related domains, such as combinatoric on words and symbolic dynamics, are emphasized.

Silvère Gangloff (IMT)
Computability of the entropy of block gluing subshifts of finite type

à venir

Benjamin Bergougnoux (LIMOS)
Algorithme simple exponentiel paramétré par la largeur de clique

La largeur de clique est un paramètre plus général que la fameuse largeur arborescente, dans le sens où celle-ci est bornée dans plus de graphe notamment dans certaine classe de graphe dense. Nous présentons un algorithme FPT simple exponentiel pour feedback vertex set et/ou un algorithme XP simple exponentiel pour Hamiltonian Path paramétré par la largeur de clique rejoignant les bornes inférieurs sous ETH.

Florian Bridoux (LIF)
On The Cost Of Simulating A Parallel Boolean Automata Networks By A Sequential One

In this presentation, we study Boolean automata networks (BANs). A given BAN can be associated with several dynamics, depending on the schedule (i.e. the order) we choose to update its automata. In this presentation, we consider all block-sequential update schedules: we group automata into blocks, and we update all automata of a block at once, and iterate the blocks sequentially. For the last 15 years, people have studied the influence of the update schedules on the dynamics of a BAN. Here, we do the opposite. We want to determine the minimum number K of additional automata that a BAN associated with a given block-sequential update schedule needs to simulate a given BAN with a parallel update schedule. To solve this problem, we introduce a graph that we call confusion graph built from the BAN and the update schedule. We show the relation between K and the chromatic number of the confusion graph. Thanks to this confusion graph, we bound K in the worst case between $n/2$ and $2n/3 + 2$ (n being the size of the BAN simulated) and we conjecture that this number equals $n/2$. We support this conjecture with two results: the clique number of a confusion graph is always less than or equal to $n/2$ and, for the subclass of bijective BANs, K is always less than or equal to $n/2$.

Émilie Allart (Cristal)
Elementary modes refine abstract interpretation of reaction networks with partial kinetic information

Genetic engineering is nowadays widely used to change the genome of cells in order to modify their behaviour, for example to overproduce some metabolite of interest. Gene knockout is one common genetic engineering technique which consists in removing one or more genes from the genome. Given the combinatorial number of possible genetic changes and the consequent impossibility of testing all of them by wet lab experiments, in silico prediction of the most interesting genetic modifications is often desirable. However, the necessary information for the in silico modelling of the organism of interest is usually lacking. This is the case for example for the bacterium B. Subtilis: its genetic engineering for the overproduction of surfactin (a well-known antibiotic) is of high interest in agriculture among other fields, but the lack of information about the biochemical functioning of this organism prevented us from modeling it with the existing methods. In order to overcome this problem, we developed a modeling language to represent reaction networks with partial kinetic information, and a method based on abstract interpretation that allows us to analyse models written in this language even in the absence of quantitative information: from the steady state semantics of the reaction network, we transform arithmetic constraints into abstract constraints over a finite domain where unknowns have been abstracted away. The qualitative behaviour of the system can therefore be evaluated in silico by means of a constraint solver, which gives us the set of all solutions (corresponding to combinations of feeding changes and gene knockouts) that lead to the desired behaviour. However, abstract interpretation usually over-approximates the solution space. As an example, while a finite system of linear equations implies all the equations that can be expressed as a linear combination, this implication no longer holds once the equations have been translated into abstract constraints. My current work consists in optimally generating new arithmetic constraints from the existing in order to minimize the solution space. Here I will discuss in particular our interest in elementary flux modes and how to adapt classical elementary mode analysis to the generation of abstract constraints to improve the qualitative analysis of reaction networks with partial kinetic information.

Laurent Thevenoux (LIP)
More accurate complex floating-point multiplication in gcc

This poster focuses on the software support of complex multiplication using the floating-point hardware instructions of 64-bit ARMv8 architecture. Given two complex floating-point numbers $x = a + ib$ and $y = c + id$, actual implementations compute the product xy as $(ac-bd) + i(ad+bc)$. With this implementation, it is well known that either the real part or imaginary part can be completely wrong. It is also well known that the FMA operation can be used to improve this method using the so-called compensation approach. We study here how more accurate complex multiplication algorithms, derived from highly accurate algorithms for $ab + cd$, behave in practice by implementing them into GCC. As we shall see, the overhead introduced by these new multiplication implementations turns out to be smaller than what the arithmetic costs suggest.

Svyatoslav Covanov (LORIA)

Exhaustive search of optimal formulae for bilinear maps

In 2012, Barbulescu, Detrey, Estibals and Zimmermann proposed a new framework to exhaustively search for optimal formulae for evaluating bilinear maps, such as Strassen or Karatsuba formulae. The main contribution of this work is a new criterion, based on rank metric, to ag- gressively prune useless branches in the exhaustive search, thus leading to the computation of new optimal formulae, in particular for the short product modulo X 5 and the circulant product modulo (X5 − 1). Moreover, we are able to prove that there is essentially only one optimal decomposition of the product of 3 × 2 by 2 × 3 matrices up to the action of some group of automorphisms.

Cyril Hugounenq (LMV)

Arithmétique Rapide appliqué à la Géométrie et à la Cryptologie: Calcul de r-isogénies à l'aide de la ℓ-torsion.

Le travail présenté a consisté à généraliser l'algorithme de Couveignes sur les tours ℓ-adiques permettant ainsi une utilisation de celui-ci sur des corps de caractéristique de taille arbitrairement grande tout en conservant le temps quadratique obtenu lors de ses améliorations par DeFeo'10. Plus précisément soient deux courbes elliptiques ordinaires E,E' en entrée que l'on sait r-isogènes alors on veut calculer la r-isogénie qui les relie. L'idée originale de l'algorithme de Couveignes est de se servir du fait que la r-isogénie envoie la p-torsion de E sur la p-torsion de E' ainsi on a une correspondance, que l'on doit deviner, entre deux groupes cycliques qui par interpolation va à précision suffisante nous donner assez d'informations pour calculer la r-isogénie. L'idée sur laquelle j'ai travaillé a été de remplacer la p-torsion par la ℓ-torsion afin de se débarasser de la dépendance exponentielle en la caractéristique p de l'algorithme original de Couveignes. Le fait de travailler avec la ℓ-torsion fait que au lieu de mettre en correspondance deux groupes cycliques on met en correspondance deux produits de deux groupes cycliques, dès lors il est crucial de restreindre les candidats. L'étude de l'action du Frobenius a donc été cruciale pour déterminer ces sous-groupes invariants sous l'action de la r-isogénie. Une utilisation de construction d'extensions de corps efficaces (en utilisant les travaux de Schost-Doliskani 2015, DeFeo-Schost-Doliskani 2013) ajouté à cette étude de l'action du Frobenius a permis d'atteindre un temps quasi-quadratique.

Vincent Despré (LABRI)

A routing algorithm for Delaunay triangulations

We give an algorithm with a stretch of at most 4.08. It improves the previous best stretch of 5.90. In addition, our algorithm is fairly easy to implement.

Jocelyn Meyron (LJK, Orsay)

An algorithm for optimal transport between a simplex soup and a point cloud

We are interested in solving an optimal transport problem between a measure supported on a simplex soup and a measure supported on a finite point set for the quadratic cost in Rd. This problem can be recast as finding a Power diagram supported on the finite point set such that the Power cells intersected with the simplex soup have a prescribed measure. We show the convergence with linear speed of a damped Newton algorithm to solve this non-linear problem. We then apply our algorithm in 3D to compute optimal transport plans between a measure supported on a triangulated surface and a discrete measure.

Aldo Gonzales-Lorenzo (LSIS)

Discrete world problems : comment ouvrir les trous d'un objet

Un objet discret est un ensemble de pixels, voxels ou leur analogue en dimension supérieure. Un objet discret 3D peut contenir des trous : composantes connexes, tunnels, anses ou cavités. Ouvrir les trous d'un objet discret consiste à éliminer tous ses trous en enlevant certains de ses points. Une façon de le faire est de prendre un point dans l'objet et de le dilater en restant contractile : les points restants sont ceux qui doivent être enlevés. Nous avons développé deux algorithmes pour ouvrir les trous d'un objet discret en dimension quelconque. Les deux algorithmes s'appuient sur la transformée de distances de l'objet, mais ils diffèrent sur la manière dont la dilatation est faite.

Florian Barbero (LIRMM)

Exploring the complexity of layout parameters in tournaments and semi-complete digraphs

In graph theory, a directed graph consists of a set of vertices connected by arcs, where the arcs have a direction associated with them. We say that a directed graph is semi-complete if it is simple (it has no self-loop nor multiple arcs) and for any two of its vertices u and v, at least one of the arcs (u,v) and (v,u) is present. We study the complexity of computing two layout parameters of semi-complete digraphs: cutwidth and optimal linear arrangement (OLA). We prove that (1) both parameters are NP-hard to compute, and the known exact and parameterized algorithms for them have essentially optimal running times, assuming the Exponential Time Hypothesis, and (2) the cutwidth parameter admits a quadratic Turing kernel, whereas it does not admit any polynomial kernel unless NP $\subseteq$ coNP/poly; by contrast, OLA admits a linear kernel. Our techniques can be also used to analyze the sizes of minimal obstructions for having small cutwidth under the induced subdigraph relation.

Fangan-Yssouf Dosso (IMath, Toulon)

Elliptic curve cryptography and Euclidiean addition chains (EAC) : Another (efficient) algorithm of multiplication

Random Euclidean addition chain generation has proven to be an efficient low memory and SPA secure alternative to standard ECC scalar multiplication methods in the context of fixed base point. In this work, we show how to generalize this method to random point scalar multiplica- tion on elliptic curves with an efficiently computable endomorphism. We also propose a software implementation of our method on various platforms/languages. We compare this method (and its implementations) to GLV and its SPA-secure version (GLV-SAC), also implemented on the same platforms/languages. With this, we show that the proposed method can be an interesting alternative to GLV/GLV-SAC in many situations because it is (relatively) easy to implement and provides better performances in many cases.

Alina Mayorova (LIX)

Generating series formulas for the structure constants of Solomon's descent algebra

Introduced by Solomon in his 1976 paper, the descent algebra of a finite Coxeter group received significant attention over the past decades. As proved by Gessel, in the case of the symmetric group its structure con- stants give the comultiplication table for the fundamental basis of qua-sisymmetric functions. We show that this property actually implies several well known relations linked to the Robinson-Schensted-Knuth correspondence and some of its generalisations. We further use the theory of type B quasisymmetric functions introduced by Chow to provide analogue results when the Coxeter group is the hyperoctahedral group.

Gabriel Scherer (Northeastern University, Boston)

Deciding program equivalence with sums and the empty type

The simply-typed lambda-calculus is a simplified, formal programming language that captures the notion of function – without polymorphism or recursion. It can be enriched with more datatypes relevant to programming: pairs (product type) and disjoint unions (sum types), as well as the one-element type (unit) and the empty type. With only functions, pairs, and the unit type, it is easy to decide whether two simply-typed lambda-terms are equivalent; it is more difficult with sums, where equivalence was first proved decidable in 1995; finally, equivalence in presence of the empty type was an open problem. n the presented work, we extend the proof-theoretic technique of 'focusing' to give a canonical representation of simply-typed lambda-terms, that allows to decide equivalence of simply-typed terms even in presence of the empty type. This new attack to programming-language problems opens new challenges and could have other applications, such as formal verification of refactoring changes, or improvements in program synthesis.

Pablo Rotondo (IRIF, GREYC, Montevideo)
The recurrence function of a random Sturmian word

This poster presents a probabilistic analysis of the recurrence of a random Sturmian word. This parameter, which can be viewed as a waiting time to discover all the factors of length n in an infinite word, is central to combinatorics of words. Previous studies concentrate on the behaviour of almost every Sturmian word rather than probabilistic behaviour. We present Sturmian words and a probabilistic model for what a random Sturmian word is, and conclude by presenting some of the results we have obtained regarding the limit distribution of their recurrence.

Dimitri Darthenay (GREYC)
The number of symbol comparisons in the dichotomic selection algorithm

à venir

Bérénice Oger (CIMI)
Opérade et algèbre combinatoire

La notion d'opérade est apparue dans les années 1960 en topologie algébrique. Après un temps d'hibernation, la théorie des opérades a connu une renaissance dans les années 1990 dans un autre domaine : l'algèbre. Depuis, de nombreux exemples d'apports réciproques entre opérades, combinatoire et algèbre ont vu le jour. Nous en présentons ici quelques applications reliées à la combinatoire du treillis de Tamari et aux nombres de Catalan.

Alexandre Wallet (LIP)
Calculs d'indice dans les variétés Jacobiennes de courbes hyperelliptiques

Calculer des logarithmes discrets dans le groupe des points rationnels d'une variété abélienne est un problème réputé difficile en général. Par exemple, lorsque la variété est de dimension 1, c'est une courbe elliptique et le problème est utilisé en cryptographie comme garantie de sécurité pour certains protocoles. Les méthodes de calcul de logarithmes discrets se partagent principalement en deux catégories. D'un côté, les algorithmes génériques pour les groupes abéliens s'exécutent au mieux en temps exponentiel en la taille des éléments du groupe. De l'autre, les algorithmes de type calcul d'indice sont rapidement meilleurs asymptotiquement, mais il est nécessaire d'estimer précisément ce gain tant asymptotiquement que pratiquement. Le poster présentera de manière générale le calcul d'indice et ses problématiques. Il décrira aussi une variante adaptée aux variétés Jacobiennes de courbes hyperelliptiques définies sur des extensions de corps finis dont le degré admet un petit facteur. Dans cette situation, la difficulté principale est de comprendre la complexité de résolution de systèmes polynomiaux dont la structure est connue à l'avance: le poster décrira une analyse mélangeant une nouvelle notion de polynômes de sommation hyperelliptiques et des techniques de bases de Gröbner.

Laurent Feuilloley (IRIF)
A hierarchy of local decision

An analogue of the theory of complexity has recently been developed for distributed computing on networks. The poster describes this field of research, and in particular the analogue of the polynomial hierarchy.

Giacomo Kahn (LIMOS)
Génération incrémentale des éléments d'un 3-treillis

De nombreux problèmes de fouille de données se rapportent à la manipulation de boîtes n-dimensionnelles de 1 dans une matrice binaire n-dimensionnelle. Nous proposons un nouvel algorithme incrémental pour recalculer ces boites lorsqu'une nouvelle couche est ajoutée à la matrice dans le cas n=3. Notre approche peut être généralisée à un n quelconque.