Informatique mathématique

Journées du GDR IM

2-3 février 2015

◁ ◁ ◇ ▷ ▷

Lundi 2 février

• 9h : accueil

• 9h15-10h15 : **Konstantinos Panagiotou** (Universität München)
Phase transitions in random constraint satisfaction problems

> Since the early 2000's statistical physicists have developed an ingenious but non-rigorous formalism, called the cavity method, that can be used to formulate precise conjectures on several phase transitions in random constraint satisfaction problems (like k-coloring graphs or the k-satisfiability problem). In this talk a survey on these results will be given, and recent progress in the quest for the rigorous localization of the phase transitions will be presented.

• 10h15-10h40, exposés de deux jeunes docteurs :

Aiswarya Cyriac (Uppsala, Suède — GT ALGA/VERIF)
Controllers for the verification of distributed systems

> Distributed systems communicating via FIFO channels are Turing powerful. Hence under-approximations have been considered for their verification. For safety critical systems, it is important to determine in run-time whether an execution has exceeded a verified subclass. A controller is a mechanism to do this. The talk will present this notion and illustrate it on an example.

Julien Bensmail (LIP, ENS Lyon — GT GRAPHES)
Strong edge-colouring of planar and bipartite graphs

> An edge-colouring of a graph G is strong if each of its colour class is an induced matching. The strong chromatic index of G, denoted $\chi'_s(G)$, is the least number of colours in a strong edge-colouring of G. Greedy colouring arguments show that χ'_s is upper-bounded by roughly $2\Delta^2$, where Δ denotes the maximum degree of the graph. But using this many colours is generally not necessary to obtain a strong edge-colouring. For example, the known graphs requiring the most colours have strong chromatic index at most roughly $1.25\Delta^2$. These extremal graphs are obtained by combining a lot of small cycles (C_4's and C_5's).
>
> For graphs with no such small cycles (*i.e.* with length at most 5), the strong chromatic index is expected to be smaller, as confirmed notably by Mahdian (2000) for C_4-free graphs. We confirm this for several new families of planar and bipartite graphs.
>
> [Joint work with A. Harutyunyan, H. Hocquard, A. Lagoutte and P. Valicov]

• 10h40-11h10 : Pause café

• 11h10-11h55 : **Joris van der Hoeven** (LIX, École polytechnique, Palaiseau — GT CF)
Fast integer multiplication

> One fundamental algorithmic problem is the efficient multiplication of two n-bit integers. Let $I(n)$ denote the time complexity for this problem, in the Turing machine

model with a finite number of tapes. Until recently, the best asymptotical bound for $I(n)$ was due to Fürer. He proved that there exists a constant $K > 1$ with

$$I(n) = O(n \log n \, K^{\log^* n}),$$

where $\log^* x$ (for $x \in \mathbb{R}$) stands for the iterator of the logarithm. That is,

$$\log^* x := \min \{k \in \mathbb{N} : \log^{\circ k} x \leq 1\},$$

and $\log^{\circ k}$ denotes the logarithm, iterated k times.

In our recent work, we managed to further improve this bound. Using a new kind of algorithm, we proved that $K = 8$ (and even $K = 4$ under the condition that a certain number theoretic conjecture holds). We also examined optimizations of Fürer's original approach, but it seems that $K = 16$ is the best bound that can be obtained in this way.

[Joint work with David Harvey and Grégoire Lecerf]

• 11h55-12h30, exposés de trois jeunes docteurs :

Chantal Keller (Microsoft research Cambridge, UK — GT LAC)
F^*: a general purpose language for program verification

The goal of program verification is to give developers a way to describe the behavior of their programs using mathematical specifications, together with a formal check of these specifications. In this talk, I will present F^*, a general purpose programming language designed for program verification, relying on an expressive type system. The challenges are to offer the features of modern programming languages such as higher-order aspects, polymorphism or side effects, while being automated and certified.

Vincent Vong (LIGM, Marne-la-Vallée — GT COMB-ALG)
Combinatorics, rewriting rules and algebra

The aim of this talk is to present some tools based on computer science and combinatorics which enable to prove algebraic results such as the computation of Hilbert series or the freeness of some algebras. In particular, we apply these methods to the fundamental case of dendriform algebra.

Simon Martiel (I3S, Nice Sophia-Antipolis — GT SDA2)
Causal graph dynamics

Causal graphs dynamics are a generalization of cellular automata to arbitrary, time-varying graphs. In other words, we can formalize, and prove theorems about the intuitive idea of a graph which evolves in time under the natural constraint that information can only ever be transmitted at a bounded speed with respect to the distance given by the graph. After a quick introduction to the model, we will list some of the properties already studied and discuss the future of this model.

Repas salle Badiane, domaine du Haut-Carré

• 14h-14h45 : **Nabil Mustafa** (LIGM, ESIEE Paris — GT GEOALGO)
Separators for combinatorial optimization problems

Separators are by now a widely-used tool for designing efficient algorithms. The planar graph separator theorem of Lipton and Tarjan (1977) has found many uses in the design of exact and approximation algorithms for optimization problems. In this talk I will survey some recent work on new constructions of separators for geometric objects, as well as their use in algorithmic design for combinatorial optimization problems such as the maximum independent set problem, and the set-cover problem.

• 14h45-15h30 : **Guillaume Fertin** (LINA, Nantes — GT COMATEGE)
Sorting permutations by reversals: an algorithmic tour

Let $\pi = \pi_1\ \pi_2 \dots \pi_n$ be a permutation over integers $1, 2, \dots n$, where π_i is the integer that appears at position i in π. An unsigned reversal $\mathcal{R}(\pi; i, j)$ is an operation on π that reverses the order of the elements between positions i and j, both included. For instance, if $\pi = 1\ 3\ 2\ 4\ 8\ 6\ 5\ 9\ 7\ 10$, then after the unsigned reversal $\mathcal{R}(\pi; 3, 6)$ is applied, we obtain the permutation $\pi' = 1\ 3\ \underline{6\ 8\ 4\ 2}\ 5\ 9\ 7\ 10$. The optimization problem Sorting By Reversals asks, given π, for the minimum number of reversals that are needed to obtain the identity permutation $I_n = 1\ 2\ 3 \dots n$, starting from π. Sorting By Reversals has been widely studied in comparative genomics: a genome may be modeled as a permutation, and reversals are one class of observed genome rearrangements that occur during evolution.

Many variants of Sorting By Reversals exist. In particular, the signed variant, in which every π_i is preceded by a +/- sign, and where a reversal not only reverses the order of the affected elements, but also their signs. Another variant is the Sorting By Prefix Reversals problem, a restriction in which the only allowed reversals are the ones that contain π_1.

In this talk, we will review the main algorithmic results that are known about Sorting By Reversals and Sorting By Prefix Reversals, both in their signed and unsigned versions. Essentially, we will discuss polynomiality, NP-completeness and approximation algorithms. This will be done in a lightweight mode, by giving the main ideas without diving too deep into technical arguments. During our tour, we will also see how these problems connect to gastronomy (pancakes and turnips) and famous people (Bill Gates and the Simpsons).

• 15h30-16h : Pause café

• 16h-16h45 : **Nicolas Brisebarre** (CNRS, LIP, ENS Lyon — GT ARIT)
Some tools for evaluating functions on a machine in a certified (yet efficient!) way

We will try to show how algorithmic number theory and computer algebra (or, more precisely, symbolic-numeric computing) can prove useful to the design of routines for the certified and fast evaluation of elementary functions, such as the exponential function for instance, in floating-point arithmetic.

• 16h45-17h30 : **Nicolas Nisse** (INRIA Sophia-Antipolis — GT GRAPHES)
Cops and robber games in graphs

Given a graph G, the seminal cops and robber game involves two players [Nowakowski and Winkler, Quilliot, 1983]. Player 1 first places its cops on some vertices of G, then Player 2 places its robber on one node. Then, turn by turn, Player 1 moves its cops to neighboring nodes and then Player 2 does as well with its robber (cops and robber may stay idle). This is a full information game in the sense that cops and robber are always visible to each other. The cops win if eventually one cop occupies the same node as the robber, and the robber wins otherwise. The cop-number of a graph G is the smallest number of cops that ensures that the robber will eventually be captured in G. In particular, Meyniel conjectured that $O(n^{1/2})$ cops are sufficient to capture a robber in any n-node graph (1985). While still open in general graphs, this conjecture has been proved in many graph classes. In this talk, I will review these results. In particular, I will try to show how cops and robber games provide a nice point of view to study graph structural properties, which has led to new algorithmic and structural results in graphs.

• 17h30-18h15 : informations et discussion sur le GDR, intervention de **Jean Mairesse**, directeur adjoint scientifique à l'INS2I

• 18h30-20h : réunion du comité exécutif du GDR

Mardi 3 février

• 9h-10h : **Joel Ouaknine** (Oxford University)
Decision problems for linear recurrence sequences

Linear recurrence sequences (LRS), such as the Fibonacci numbers, permeate vast areas of mathematics and computer science. In this talk, we consider three natural decision problems for LRS, namely the Skolem Problem (does a given LRS have a zero?), the Positivity Problem (are all terms of a given LRS positive?), and the Ultimate Positivity Problem (are all but finitely many terms of a given LRS positive?). Such problems (and assorted variants) have applications in a wide array of scientific areas, from theoretical biology and software verification to combinatorics and statistical physics.

Perhaps surprisingly, the study of decision problems for LRS involves advanced techniques from a variety of mathematical fields, including analytic and algebraic number theory, Diophantine geometry, and real algebraic geometry.

[Joint work with James Worrell]

• 10h-10h25, exposés de deux jeunes docteurs :

Victor Magron (Imperial College, Londres — GT CF)
New applications of semidefinite programming

Semidefinite programming (SDP) is relevant to a wide range of mathematical fields, including combinatorial optimization, control theory, matrix completion. In 2001, Lasserre introduced a hierarchy of SDP relaxations for approximating polynomial infima. My talk emphasizes new applications of this SDP hierarchy in either computer science or mathematics, investigated during my PhD and postdoc research.

In real algebraic geometry, I describe how to use SDP hierarchies to approximate as closely as desired exact projections of semialgebraic sets. In nonlinear optimization, SDP hierarchies allow us to compute Pareto curves (associated with multicriteria problems) as well as solutions of transcendental problems.

These hierarchies can also be easily interleaved with computer assisted proofs. An appealing motivation is to solve efficiently thousands of nonlinear inequalities occurring in the formal proof of Kepler conjecture by Hales. Finally, SDP can provide precise information to automatically tune reconfigurable hardware (e.g. FPGA) to algorithm specifications.

Adeline Langlois (EPFL, Lausanne — GT C2)
Lattice-based cryptography: security foundations and constructions

I will describe my research in lattice-based cryptography, which is a branch of cryptography exploiting the presumed hardness of some well-known problems on lattices.

• 10h25-10h55 : Pause café

• 10h55-11h40 : **Cristina Sirangelo** (LSV, ENS Cachan — GT ALGA)
Efficiently querying incomplete data

Data is incomplete when it contains missing/unknown information, or more generally when it is only partially available, e.g. because of restrictions on data access.

Incompleteness is receiving a renewed interest as it is naturally generated in data interoperation, a very common framework for today's data-centric applications. In this setting data is decentralized, needs to be integrated from several sources and exchanged between different applications. Incompleteness arises from the semantic and syntactic heterogeneity of different data sources.

Querying incomplete data is usually an expensive task. In this talk we survey on the state of the art and recent developments on the problem of efficiently querying incomplete data, under different possible interpretations of incompleteness.

• 11h40-12h05, exposés de deux jeunes docteurs :

Arnaud de Mesmay (IST Austria, Vienne — GT GEOALGO)
Studying surface-embedded graphs with geometric tools

Graphs embedded on surfaces are a natural generalization of planar graphs. In the past decades, a lot of research has been devoted towards understanding their combinatorics and designing efficient algorithms tailored for this class of graphs.

In parallel, the study of the geometric properties of surfaces is an active topic of research in the pure mathematics community, due to their numerous connections with topics such as Riemann surfaces, Riemannian geometry and 3-manifolds.

In this talk, I will illustrate how ideas and theorems coming from the latter community can be applied to improve our understanding of surface-embedded graphs, by focusing on two problems: how to test isotopy of embedded graphs, and how to decompose such a graph into a planar one.

[Based on joint work with Éric Colin de Verdière and Alfredo Hubard]

Dominik Pająk (Cambridge, UK — GT COA)
Algorithms for deterministic parallel graph exploration

A mobile agent is an entity capable of traversing edges of a graph and visiting its vertices. Graph exploration by a team of mobile agents is a problem of visiting each vertex with at least one agent. Our goal is to benefit from having multiple agents thus we are looking for solutions that are faster than the single-agent ones. We will study such algorithms in two scenarios: first in which agents can exchange messages between each other and the second where agents will be allowed to leave some information at the vertices.

Repas salle Badiane, domaine du Haut-Carré

• 13h45-14h30 : **Christine Tasson** (PPS, U. Paris 7 — GT GEOCAL)
Probabilistic coherent spaces, an accurate model of probabilistic programing

The purpose of this talk is to present a semantics of a programing language with probabilistic choice. Probabilistic coherent semantics is a simple denotational model which reflects exactly the operational properties of programs. This strong property allows us to reason on denotations instead of syntax in order to distinguish programs.

[Joint work with Thomas Ehrhard and Michele Pagani]

• 14h30-15h15 : **Stéphan Thomassé** (LIP, ENS Lyon — GT GRAPHES/COA) *Quelques approches de la complexité des stables d'un graphe*

Un des problèmes les plus classiques sur les graphes est le calcul du stable maximum, ou, en version pondérée, celui de poids maximum. Cette question est à l'origine de très nombreuses directions de recherche sous-tendues par le fait que la complexité structurelle d'un graphe peut se voir dans l'ensemble de ses stables. Je donnerai dans cet exposé quelques approches de l'étude des stables d'un graphe en retraçant les résultats récents et les questions encore ouvertes.

En particulier, je parlerai ici des formulations étendues du polytope des stables, de quelques conséquences du lemme de Sperner appliqué au complexe des stables, et des classes de graphes chi-bornée, i.e. dont le nombre chromatique est fonction de la clique de taille maximum.

• 15h15-16h : **Brigitte Vallée** (CNRS, GREYC, U. de Caen — GT ALEA)
An instance of analysis of algorithms: the plain GCD algorithm

The talk describes the probabilistic analysis of an algorithm which computes the gcd of ℓ inputs (with $\ell \geq 2$), with a succession of $\ell - 1$ phases, each of them being the Euclid algorithm on two entries. This algorithm is both basic and natural, and two kinds of inputs are studied: polynomials over the finite field $\mathbb{F}_q$ and integers. The analysis exhibits the precise probabilistic behaviour of the main parameters, namely the number of iterations in each phase and the evolution of the length of the current gcd along the execution. We first provide an average-case analysis. Then we make it even more precise by a distributional analysis. Our results rigorously exhibit two phenomena: (i) there is a strong difference between the first phase, where most of the computations are done and the remaining phases; (ii) there is a strong similarity between the polynomial and integer cases.

In the talk, we focus on the main principles of analytic combinatorics, with its two steps: the construction of generating functions as formal objects; then the study of their analytic properties when they are seen as functions of the complex variable. We also explain the similarities and the differences between the two studies (polynomials and integers), and describe the dynamical point of view which appears in the integer study.

[Joint work with Valérie Berthé (LIAFA) and Loïck Lhote (GREYC)]

- 16h : goûter d'adieu

◁ ◁ ◇ ▷ ▷