EJCIM 2020

Schedule

Horaire de la semaine du 8 juin

Lundi 8 juin

— 10h30 - 10h45 : Ouverture de l'EJCIM 2020
— 10h45 - 11h00 : Exposé de Julien Esnay
— 11h00 - 12h15 : Cours (1/2) de Marthe Bonamy
— 16h00 - 16h15 : Exposé d'Alexandre Clément
— 16h15 - 17h30 : Cours (1/2) de Marni Mishna

Mardi 9 juin

— 9h00 - 9h15 : Exposé d'Andrea Lesavourey
— 9h15 - 10h30 : Cours (1/2) de Jérôme Leroux / Sylvain Schmitz
— 10h30 - 11h00 : Pause (30 minutes)
— 11h00 - 12h00 : Aide à la constitution des dossiers de candidature par Pascal Weil

Mercredi 10 juin

— 9h00 - 9h15 : Exposé de Khaydar Nurligareev
— 9h15 - 10h30 : Cours (1/2) de Fredrik Johansson
— 10h30 - 11h00 : Pause (30 minutes)
— 11h00 - 12h00 : Genre et informatique : les hics et les déclics par Marion Paoletti

Jeudi 11 juin

— 9h00 - 9h15 : Exposé d'Ambre Toulemonde
— 9h15 - 10h30 : Cours (1/2) de Xavier Goaoc
— 10h30 - 11h00 : Pause (30 minutes)
— 11h00 - 12h00 : Carrières dans le monde de l'entreprise par Mohamed Mosbah

Horaire de la semaine du 15 juin

Lundi 15 juin

— 10h45 - 11h00 : Exposé de Jonathan Narboni
— 11h00 - 12h15 : Cours (2/2) de Irena Penev
— 16h00 - 16h15 : Exposé de Florian Galliot
— 16h15 - 17h30 : Cours (2/2) de Marni Mishna

Mardi 16 juin

— 9h00 - 9h15 : Exposé de Pierre Popoli
— 9h15 - 10h30 : Cours (2/2) de Jérôme Leroux / Sylvain Schmitz

Mercredi 17 juin

— 9h00 - 9h15 : Exposé Laurine Bénéteau
— 9h15 - 10h30 : Cours (2/2) de Fredrik Johansson

Jeudi 18 juin

— 9h00 - 10h15 : Cours (2/2) de Xavier Goaoc
— 10h15 - 10h30 Clôture

Cours

Marthe Bonamy[1] et Irena Penev[2]
Université de Bordeaux (LaBRI)[1] et Charles University[2]

Nombre chromatique et sous-graphes induits

Nous nous intéressons ici aux liens entre trois paramètres centraux en théorie des graphes : χ (nombre de couleurs nécessaires pour colorer les sommets de façon à ce que deux sommets adjacents reçoivent des couleurs distinctes), α (taille d'un plus grand stable, c.à.d. un ensemble de sommets deux à deux non-adjacents) et ω (taille d'une plus grande clique, c.à.d. ensemble de sommets deux à deux adjacents), ainsi qu'à l'impact de structures (sous-graphes) interdites sur leur comportement.

Xavier Goaoc
Université de Lorraine (LORIA)

Convexité combinatoire

Ce chapitre introduit à la convexité combinatoire, ses applications algorithmiques et ses prolongements en combinatoire topologique.

Marni Mishna
Simon Fraser University et Université de Bordeaux (LaBRI)

La combinatoire analytique

On apprend les techniques de bases de la combinatoire analytique qui sert à comprendre le comportement des objets combinatoires de grande taille. On suit un chemin qui nous amène vers les séries génératrices multivariées.

Fredrik Johansson
Université de Bordeaux (IMB)

Calculer avec les nombres réels

Le calcul sur machine avec des nombres réels pose des difficultés fondamentales, liées d'une part aux questions de calculabilité elles-mêmes et, d'autre part, aux problèmes pratiques d'efficacité et de suivi de précision. Dans ce chapitre, nous faisons le point sur les problématiques de ce domaine et sur les concepts fondamentaux qui ont été introduits pour les résoudre. Nous présentons également quelques outils (comme les différentes manières de représenter les nombres réels) qui permettent de surmonter en pratique les difficultés qui apparaissent.

Jérôme Leroux[1] et Sylvain Schmitz[2]
Université de Bordeaux[1] (LaBRI) et Université de Paris[2] (IRIF)

Accessibilité des systèmes d'addition de vecteurs

Ce chapitre est consacré aux systèmes d'addition de vecteurs, un formalisme équivalent aux réseaux de Petri et employé pour raisonner sur des ressources discrètes : par exemple des processus en calcul parallèle ou distribué, des molécules dans des réactions chimiques, des organismes dans des processus biologiques, etc. De plus, de nombreuses questions algorithmiques en informatique théorique et mathématiques discrètes se ramènent à des questions sur les systèmes d'addition de vecteurs, et en particulier à leur problème d'accessibilité. Celui-ci est décidable, mais avec un coût algorithmique très élevé : il est (au moins) non-élémentaire et (au plus) ackermannien.

Ce chapitre présente les derniers résultats connus à ce jour concernant les bornes de complexité pour le problème d'accessibilité dans les systèmes d'addition de vecteurs. C'est aussi l'occasion de donner un aperçu rapide de plusieurs outils mathématiques utilisés en informatique théorique tels que les systèmes d'équations linéaires ou les ordinaux, et de classes de complexité au-delà des classes habituelles comme `P`, `NP` ou `EXP`.

Exposés

Laurine Bénéteau
Aix-Marseille Université

Médian des graphes médians et leurs complexes cubiques en temps linéaire.

Avec Jérémie Chalopin, Victor Chepoi et Yann Vaxès

Le problème du médian est un des principaux problèmes de localisation dans les graphes. Étant donné un graphe $G = (V, E)$ et un ensemble fini de sommets S, le problème du médian consiste à trouver un sommet de G minimisant la somme des distances vers tous les sommets de S. On se place dans le cas particulier des graphes médians. Un graphe $G = (V, E)$ est dit médian si pour tout triplet de sommets u, v, w de V, il existe un unique sommet qui est à la fois sur un plus court chemin de u à v, de u à w et de v à w. Nous proposons un algorithme qui permet de calculer tous les sommets médians d'un graphe médian en temps linéaire $O(|E|)$. Les arêtes d'un graphe médian sont organisées en classes de parallélisme, appelées Θ-classes. La suppression des arêtes d'une Θ-classe partitionne un graphe médian en deux sous-graphes appelés demi-espaces. On montre qu'on peut calculer les Θ-classes d'un graphe médian en temps linéaire en utilisant un parcours en largeur lexicographique (LexBFS). On utilise également les propriétés des demi-espaces et la *règle de majorité* suivante : un demi-espace H d'un graphe médian G contient au moins un sommet médian si et seulement si H contient au moins la moitié des sommets de S. On en déduit un algorithme optimal qui calcule l'ensemble des sommets médians d'un graphe médian en temps linéaire.

Le ℓ_1-complexe cubique $\mathcal{G}$ d'un graphe médian G est obtenu en remplaçant chaque hypercube de G par un cube unité solide muni de la métrique ℓ_1. Le problème du médian consiste donc à trouver les points minimisant la somme des distances vers un ensemble de points P de $\mathcal{G}$ donné. En utilisant les Θ-classes et en adaptant la règle de majorité, nous obtenons un algorithme linéaire pour calculer l'ensemble médian du ℓ_1-complexe cubique.

Alexandre Clément
LORIA

PBS-calculus : A Graphical Language for Quantum-controlled computations

We introduce the PBS-calculus to represent and reason on quantum computations involving polarising beam splitters (PBS for short). PBS-diagrams can be used to represent various schemes including quantum-controlled computations, which are known to have multiple computational and communication advantages over classically ordered models like quantum circuits.

The PBS-calculus is equipped with an equational theory, which is proved to be sound and complete : two diagrams are representing the same quantum evolution if and only if one can be transformed into the other using the rules of the PBS-calculus. Moreover, we show that the equational theory is minimal. Finally, we show that any PBS-diagram involving only unitary matrices can be transformed into a diagram without feedback loop.

Julien Esnay
Institut de Mathématiques de Toulouse (IMT) et Laboratoire de l'Informatique et du Parallélisme (LIP)

Decidability of the Domino Problem under Horizontal Constraints

Since the 1960s, when it was popularized by Hao Wang, the Domino Problem has been largely studied. At its core is a simple question : is there a Turing Machine able to take as input any finite tile set and adjacency rules, and say if the space of all configurations using these tiles and respecting these rules – called a subshift – is empty ? The Domino Problem is said to be decidable if such a Turing Machine exists, and undecidable otherwise. This problem has an equivalent formulation in symbolic dynamics : in that setting, a subshift is the space of all colorings of $\mathbb{Z}^n$ by a finite alphabet, which do not contain certain forbidden patterns. The Domino Problem on $\mathbb{Z}$, i.e. trying to tile a discrete line, is decidable ; but the Domino Problem on $\mathbb{Z}^2$ is not.

In view to precise where this difference of behavior resides, we introduce a new two-dimensional Domino Problem where we fix in advance a one-dimensional finite set of forbidden patterns $F(H)$ on a given alphabet. Then, we study if there exists a Turing Machine that takes as input any one-dimensional

set of forbidden patterns $F(V)$ on the same alphabet, and that says if the two-dimensional subshift $X_{H,V}$, which contains no forbidden patterns from $F(H)$ horizontally and from $F(V)$ vertically, contains a valid configuration or not. We prove the undecidability of this new Domino Problem in various cases.

Florian Galliot
Institut Fourier, Université Grenoble Alpes

Un jeu de reconfiguration sur les graphes

Nous étudions le problème de reconfiguration suivant. Un joueur déplace des jetons placés sur les sommets d'un graphe G, suivant la règle dite de 2-adjacence : un mouvement autorisé consiste à déplacer un jeton de son choix vers un sommet non occupé qui possède au moins 2 voisins occupés. On appelle configuration un ensemble de sommets de G représentant les positions occupées par les jetons (maximum un jeton par sommet). Les jetons peuvent ou non être numérotés i.e. distinguables les uns des autres. Etant donné une configuration de départ A et une configuration d'arrivée B, est-il possible de passer de A à B par une suite de mouvements légaux ? Si oui, combien de coups sont nécessaires/suffisants ? Ce problème, dont certaines instances apparaissent dans la littérature dès le milieu du XXe siècle, a été introduit et étudié en 2002 dans sa version générale par E. Demaine, M. Demaine et H. Verrill. Les auteurs résolvent le jeu dans la grille triangulaire, ainsi que certaines instances dans la grille carrée, laissant toutefois à l'exploration les cas les plus difficiles. Nous approfondissons leurs résultats et raffinons leurs algorithmes de résolution. Lors de notre étude structurelle de certaines configurations problématiques sur la grille carrée, apparaissent naturellement des considérations rencontrées dans une célèbre énigme du "virus qui se propage à l'intérieur d'un rectangle", laquelle s'avère être centrale dans notre problème.

Andrea Lesavourey
Université de Wollongong

Retrouver des générateurs courts d'idéaux principaux dans certaines extensions de Kummer réelles

Avec Thomas Plantard et Willy Susilo

The simplest versions of encryption using ideal lattices such as in [4, 9] is as follow. Consider a number field K and $I = g\mathcal{O}_K$ a principal ideal with a short g when I is considered as a lattice i.e. the euclidean norm of g is small compared to the determinant of I. Then K and I are public and g is private. The private key security relies on the hardness of finding g or another short generator. Finding a generator is called the *Principal Ideal Problem* (PIP). Finding a short generator is referred as the *Short Principal Ideal Problem* (SPIP). By default an attack to recover the generator g is done in two steps

1. recover a generator h of I ;
2. find a short generator given h.

The first step corresponds to the PIP which is considered a hard problem in classical computational number theory. However it is shown that it can be efficiently done by using quantum computing as in [2]. The second is a reduction phase which is the kind of tasks that seem difficult even for quantum computers. In order to solve it, one may use the structure of the set of generators of I and the Log-unit lattice. Indeed $\mathrm{Log}(h) = \mathrm{Log}(g) + \mathrm{Log}(u) \in \mathrm{Log}(g) + \mathrm{Log}(\mathcal{O}_K^\times)$ so recovering g can be seen as solving a BDD problem with respect to $\mathrm{Log}(\mathcal{O}_K^\times)$. An analysis over cyclotomic fields has been done in [3] where the authors gave a bound for the norm of the vectors of the dual basis. In [1] the authors studied another family of fields, namely the multiquadratic fields, and were able to recover a short generator of an ideal in classical polynomial time for a wide range of fields.

We first generalised the approach of [1] to multicubic fields in [5] then to real Kummer extensions of $\mathbb{Q}$ with a prime exponent i.e of the form $\mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ where $m_i \in \mathbb{Q}$. The lattice of subfields and the set of complex field morphisms of these fields have a structure similar to the ones of multiquadratic fields. Thus the algorithms to compute the unit group and a generator of a principal ideal can be adapted. Moreover, in order to break the structure a little, we also considered the combination of two Kummer extensions with distinct exponents i.e. of the form $\mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r}, \sqrt[q]{n_1}, \ldots, \sqrt[q]{n_s})$. Again the structure of such fields allows to design algorithms more efficient than the standard ones. From the experimental data that we computed, general Kummer extension of $\mathbb{Q}$ with only one exponent seem to show the same properties than multiquadratic and multicubic fields i.e. high probabilities to retrieve

the private key. This probability seems to be smaller over Kummer extensions with two exponents. However the fact that relatively fast classical computations (when compared to standard algorithms) can be done over the number fields in this work seems to indicate that one should be careful with very structured fields.

In order to obtain practical results, improvements on classical number theoretical computations are needed. Further work can also consist on studying other tasks of computational number theory over these fields such as computing the class group and S-units. It could be possible to implement and have practical examples of the attack to solve the *Ideal Shortest Vector Problem* (ISVP) presented in [7]. Another direction would be to study number fields with more complicated structures in order to look whether we can again find a good basis for the Log-unit lattice or not.

Jonathan Narboni
Université de Bordeaux

On the 4-color theorem for signed graphs

There are several ways to generalize graph coloring to signed graphs. Máčajová, Raspaud and Škoviera adopted the Zaslavsky's definition of coloring [11] to introduce the chromatic number of a signed graph [6].

If (G, σ) is a signed graph, a k-coloring of (G, σ) is a mapping :

$$c : V(G) \to \{-k/2, \dots, -1, 1, \dots, k/2\} \quad \text{if } k \equiv 0 \pmod 2, \text{ or}$$
$$c : V(G) \to \{-(k-1)/2, \dots, -1, 0, 1, \dots, (k-1)/2\} \text{ otherwise,}$$

such that : $\forall uv \in E(G)$, $c(u) \neq \sigma(uv) \cdot c(v)$.
$\chi(G)$ denotes the signed chromatic number of G, and is defined as the minimum k such that (G, σ) has a k-coloring.

Máčajová, Raspaud and Škoviera also conjectured that the Four Color Theorem holds for the signed planar graphs as well, generalizing thereby The Four Color Theorem :

Conjecture : Let G be a simple signed planar graph. Then $\chi(G) \leq 4$.

We first translate the problem of vertex coloring of a signed planar graph to a problem of edge labeling of its dual. We generalize in this way the translation from a 4-coloring of a triangulation to a 3-edge-coloring of the dual, used in the proof of the four-color theorem (see [8]). We then prove that the Conjecture is false by building a signed triangulation which is not 4-colorable.

Khaydar Nurligareev
Université Paris 13

Asymptotics for the probability of labeled objects to be connected

Let f_n be the counting sequence of a labeled combinatorial class and g_n be the number of connected objects of size n in the same class, so that their exponential generating series satisfies $F(z) = \log(G(z))$. We are interested in the asymptotic behavior of the probability $p_n = g_n/f_n$. It turns out that if f_n is growing sufficiently fast, then p_n converges to 1 and we can describe the coefficients h_i involved in the asymptotic expansion of p_n explicitly. In some cases, we can indicate other combinatorial objects that these coefficients count. Moreover, the asymptotic expansion of h_n/f_n can also be described.

Pierre Popoli
Université de Lorraine, IECL

Complexité d'ordre maximal des suites de Thue–Morse et de Rudin–Shapiro le long des polynômes

Certaines suites automatiques, comme celle de Thue–Morse ou de Rudin–Shapiro, ne sont pas de bonnes suites pseudo-aléatoires en dépit d'une large complexité d'ordre maximal car leur complexité

d'expansion est bornée. En 2019, Sun et Winterhof montrent que ces deux suites le long des carrés gardent une complexité d'ordre maximal assez grande et il est connu que ces suites ne sont plus automatiques. Alors d'après le théorème de Christol, la complexité d'expansion de chaque suite n'est plus bornée. Ainsi la suite de Thue–Morse et la suite de Rudin–Shapiro le long des carrés pourraient être de bons candidats pour être des suites pseudo-aléatoires. Dans cet exposé, en répondant à une question des deux auteurs, je présenterai la généralisation du résultat de Sun et Winterhof [10] à tout polynôme à valeurs entières. Ce résultat a été montré à l'aide d'outils combinatoires et d'études de propagation de retenues. Je présenterai également des problèmes encore ouverts à ce sujet.

Ambre Toulemonde
Université de Versailles-Saint-Quentin-En-Yvelines et Thales DIS

Consensus protocols from Byzantine Generals problem to Blockchain

Reaching an agreement on a value in distributed manner, *i.e.* reaching a consensus in a group without a central authority, is one of the challenges in distributed systems. This issue, *a.k.a* the *Byzantine Generals problem* (BGP), was introduced by Lamport *et al.* in 1982. For decades, BGP has been widely studied to provide solutions called *consensus protocols*. The *Practical Byzantine Fault Tolerant* (PBFT) solution released in 1999 became the reference to construct consensus protocols. PBFT has been designed for small sets of identified participants, generally called *nodes*, while considering that some of them may be *Byzantine*, *i.e.* malfunction or maliciously behave.

Since the release by Nakamoto in 2008 of the Bitcoin paper based on a *blockchain*, an increased interest in the consensus protocols has emerged. The blockchain is an immutable distributed ledger where a new *block* of data can only be appended after reaching a consensus. Nakamoto proposes a consensus protocol, called *Proof-of-Work* (PoW), to address BGP taking into account new criteria, *e.g. scalability* and *incentive*, brought by his Bitcoin blockchain which is a *public* blockchain, *i.e.* anyone at any time can take part in the protocol. In PoW, the nodes have to resolve a hash puzzle which can only be solved through brute-force, thus requiring intensive energy resources. In addition to this energy waste problem, it seems that the design of PoW protocol has some other issues, *e.g.* pools centralization or rational strategies such as *Selfish mining*. The lessons learned from the works on BGP and public blockchain need for new consensus protocols for blockchain.

PhD research focus on consensus protocols for *private* blockchain where only a group of authenticated nodes can read and write data into the ledger, *e.g.* a consortium of banks which wants to share data only between them. There exists consensus protocols with random leader election using a *Verifiable Random Function* (VRF) that seems as promising approaches to avoid the issues of both public blockchain and PBFT. In this presentation, we provide an overview of consensus protocols, from the first results for BGP to those for blockchain, and the ongoing PhD research on consensus protocols using VRF.

Bibliographie

[1] Jens Bauch, Daniel J. Bernstein, Henry de Valence, Tanja Lange, and Christine van Vredendaal. Short generators without quantum computers : The case of multiquadratics. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, pages 27–59, Cham, 2017. Springer International Publishing.

[2] J.-F. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 893–902, 2016.

[3] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 559–585, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[4] Craig Gentry. *A Fully Homomorphic Encryption Scheme*. PhD thesis, Stanford, CA, USA, 2009. AAI3382729.

[5] Andrea Lesavourey, Thomas Plantard, and Willy Susilo. On ideal lattices in multicubic fields. `http://nutmic2019.imj-prg.fr/confpapers/MultiCubic.pdf`, 2019.

[6] Edita Máčajová, André Raspaud, and Martin Škoviera. The chromatic number of a signed graph. *The Electronic Journal of Combinatorics*, 23(1), January 2016.

[7] Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé. Approx-svp in ideal lattices with pre-processing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 685–716, Cham, 2019. Springer International Publishing.

[8] Neil Robertson, Daniel Sanders, Paul Seymour, and Robin Thomas. The four-colour theorem. *Journal of Combinatorial Theory, Series B*, 70(1) :2–44, May 1997.

[9] N. P. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography – PKC 2010*, pages 420–443, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[10] Zhimin Sun and Arne Winterhof. On the maximum order complexity of subsequences of the Thue–Morse and Rudin–Shapiro sequence along squares. *International Journal of Computer Mathematics : Computer Systems Theory*, 4(1) :30–36, 2019.

[11] Thomas Zaslavsky. Signed graph coloring. *Discrete Mathematics*, 39(2) :215–228, 1982.