L'École de Jeunes Chercheurs en Informatique Mathématique 2021

lundi 7 juin 2021 - jeudi 10 juin 2021

En Ligne

Recueil des résumés

Contents

Quantique / 1

Algorithmes quantiques de base

Auteur correspondant arnault@unilim.fr

Cet exposé vise à présenter les algorithmes quantiques de base, en particulier ceux ayant un impact potentiel en cryptographie. Parmi eux, les algorithmes de type Simon et Grover qui permettent d'accélérer la recherche de valeurs vérifiant une propriété particulière (par exemple une clé cryptographique), et les algorithmes basés sur l'utilisation de
la transformée de Fourier, comme ceux introduits par Shor qui permettent de factoriser des entiers ou de calculer des logarithmes discrets en temps polynomial.

Quantique / 2

Introduction aux codes correcteurs quantiques

Auteur correspondant gilles.zemor@math.u-bordeaux.fr

Un code correcteur quantique peut être vu comme la donnée de deux codes correcteurs classiques. Dans la théorie classique, les codes dits LDPC (Low Density Parity Check) font partie des plus anciens codes connus: ils sont munis d'algorithmes de décodage efficaces et permettent à leurs rendements d'atteindre constructivement la limite de Shannon. Ils ont ainsi peu de rivaux, à la fois en théorie et en pratique.
On s'attend à ce que l'ordinateur quantique utilise des analogues quantiques des codes LDPC. Ces codes sont cependant nettement moins bien compris que leurs versions classiques.
Ils sont beaucoup moins faciles à construire, et les algorithmes
de décodage classiques ne s'adaptent pas naturellement.
Leurs constructions impliquent notamment une structure topologique assez forte.
Nous ferons une introduction au domaine des codes LDPC quantiques, souligneront les similarités et les différences avec la théorie classique, et évoquerons des progrès très récents.

Quantique / 3

Programmation quantique pratique

Auteur correspondant simon.martiel@atos.net

Comme en informatique classique, il y a un fossé entre la description théorique d'un algorithme quantique et son implémentation en terme de séquence d'instructions quantiques. Dans ce cours, nous utiliserons une librairie de description de circuits quantiques (l'extension naturelle
des circuits booléens classique à un modèle quantique) pour implémenter quelques algorithmes. En particulier, nous rappellerons les principes algorithmiques derrière l'algorithme de Grover et implémenterons quelques oracles pour résoudre différents problèmes d'optimisation. Si le temps le permet, nous aborderons d'autres algorithmes de la littérature, comme l'algorithme de Bernstein Vazirani.

Calcul Formel / 4

Computer algebra for lattice path combinatorics

Auteur correspondant alin.bostan@inria.fr

Classifying lattice walks in restricted lattices is an important problem in enumerative combinatorics. Recently, computer algebra has been used to explore and to solve a number of difficult questions related to lattice walks. We give an overview of recent results on structural properties and explicit formulas for generating functions of walks in the quarter plane, with an emphasis on the algorithmic methodology.

Calcul Formel / **5**

Matrices polynomiales : accélérer et exploiter leur algorithmique

Auteur correspondant vincent.neiger@unilim.fr

Les matrices dont les coefficients sont des polynômes à une variable sont un objet mathématique de base, qui se retrouve au coeur d'approches algorithmiques fondamentales du calcul formel : résolution de systèmes linéaires creux ou structurés, calculs d'approximants et d'interpolants, division avec reste pour les polynômes à deux variables, ...
Après une présentation du contexte, nous donnerons une vue d'ensemble des progrès récents concernant les calculs
exacts efficaces avec ce type de matrices. Ensuite, nous verrons comment ces résultats ont été exploités afin d'aboutir à des avancées majeures sur la complexité de problèmes qui n'impliquent pas nécessairement les matrices polynomiales a
priori : la composition modulaire de polynômes, et le calcul du polynôme caractéristique d'une matrice à coefficients dans un corps.

Cryptographie / **6**

Cryptographie post-quantique: alternatives et enjeux

Auteur correspondant gaborit@unilim.fr

Depuis l'apparition de l'algorithme de factorisation de P. Shor
en 1994, on sait que l'existence d'un ordinateur quantique suffisamment puissant peut amener à la cryptanalyse immédiate de tous les systèmes cryptographiques actuels basés sur la théorie des nombres utilisés en pratique comme les algorithmes RSA, les systèmes basés sur le logarithme
discret sur Z/pZ ou encore sur les courbes elliptiques. Dans cet exposé nous ferons le point sur les différentes alternatives pour resister à ce type d'attaques et notamment la cryptographie basée sur les réseaux, les codes correcteurs (en Hamming et en métrique rang) ou encore les signatures basées sur les fonctions de hachages ou encore la cryptographie multivariée. Nous considérerons aussi les enjeux au niveau du concours international lancé par le NIST (institut des standards amériain) sur la crypotgraphie post-quantique.

Cryptographie / **7**

Preuves Implicites

Auteur correspondant olivier.blazy@unilim.fr

Les Smooth Projective Hash Functions ont été introduites en 2002 par Cramer et Shoup pour permettre de faire du chiffrement CC2.
Nous allons montrer comment les classifier, comment en construire et comment étendre le champ des langages pouvant être générés.
Pour celà, nous les étudions tout d'abord sous l'angle classique des courbes elliptiques mais également des réseaux euclidiens, ou même de la cryptographie à base de codes. Ensuite nous proposons de nouvelles méthodologies pour construire et prouver des protocoles d'échanges de clé authentifiés (que nous regroupons derrière le concept de LAKE : Language Based Authenticated Key Exchange, Echange de clé authentifié par un langage), et des protocoles asymétriques (regroupés sous le concept d'OLBE : Oblivious Language-Based Envelope, Enveloppe Inconsciente basée sur un langage). A chaque fois, nous regarderons les
fonctionnalités idéales, des instantiations génériques et montrons comment instantier les diverses briques pour générer des protocoles sûrs et le plus efficaces possibles. Bien que développées de façon générique, nous remarquons que nos instantiations conduisent à des protocoles extrêmement efficaces même en cas de corruptions adaptatives, et que ces constructions se transposent presque naturellement aux hypothèses post-quantiques.

Verification Formelle / 8

Analyse symbolique de protocoles cryptographiques, modélisation logique, et algorithme de vérification

Auteurs correspondants: vincent.cheval@inria.fr, lucca.hirschi@inria.fr

Présentations Doctorants / 9

Algorithme de dénombrement de points fixes

Auteur correspondant balthazar.charles@gmail.com

Présentations Doctorants / 10

On the Besicovitch-Stability of Noisy Random Tilings

Auteur correspondant lgayral@math.univ-toulouse.fr

we introduce a noisy framework for SFTs, allowing some amount of forbidden patterns to appear. Using the Besicovitch distance, which permits a global comparison of configurations, we then study the closeness of noisy measures to non-noisy ones as the amount of noise goes to 0. Our first main result is the full classification of the (in)stability in the one-dimensional case. Our second main result is a stability property under Bernoulli noise for higher-dimensional periodic SFTs, which we finally extend to an aperiodic example through a variant of the Robinson tiling.

Présentations Doctorants / 11

Asymptotic probability of connected labeled objects and virtual species

Auteur correspondant nurligareev@lipn.univ-paris13.fr

There are a number of combinatorial structures that admit a notion of connectivity, including graphs as the most commonly used example. We are interested in the probability that a random labeled object
is connected, as its size tends to innity. We will show that the asymptotics for these probabilities can be obtained in a common manner and that asymptotic coecients have a combinatorial meaning in terms
of virtual species. Moreover, we will show how to get the asymptotic probability that a random labeled
object has a given number of connected components, and we will indicate the combinatorial meaning of the
coecients involved in the asymptotic expansions.
This is ongoing work joint with Thierry Monteil.

Présentations Doctorants / **12**

Construction de coloriages de produits de groupes en dynamique symbolique

Auteur correspondant sachahuriot@gmail.com

Présentations Doctorants / **13**

Aperiodic Subshifts of Finite Type on Baumslag-Solitar Groups

Auteur correspondant julien.esnay@ens-lyon.fr

The Cayley graph of a group is a way to visualize its structure as a graph. A Subshift of Finite Type (SFT) on a group is the set of all the colorings of the Cayley graph that use a given finite number of colors and respect a given finite number of adjacency rules between colored vertices. Initially studied on $\mathbb{Z}$ as tilings of the biinfinite line with dominoes, the notion was extended to $\mathbb{Z}^2$ using square tiles with colored edges called Wang tiles, then to any $\mathbb{Z}^d, d > 2$; and more recently to any group of finite type.

On $\mathbb{Z}$, any SFT must contain a periodic coloring – but this becomes false with $\mathbb{Z}^2$, on which there are some SFTs with only non-periodic colorings. On $\mathbb{Z}^d, d > 2$, two distinct and finer notions of aperiodicity arise. This talk will detail these results, then proceed to prove, using notably substitutions on biinfinite words, that these finer notions of aperiodicity are also present for SFTs on some Baumslag-Solitar groups, that are two-generator one-relator groups that resemble $\mathbb{Z}^2$.

This is a joint work with E. Moutot.

Présentations Doctorants / **14**

Augmented Broadcast Encryption with constant size ciphertext, from standard assumption

Auteur correspondant anais.barthoulot@orange.com

Présentations Doctorants / 15

Algorithmes de fractions continues multidimensionnelle

Auteur correspondant melodie.andrieu-estevez@univ-amu.fr

Syndrome de l'imposture / 16

Atelier sur le syndrome d'imposture

Auteur correspondant natacha.portier@ens-lyon.fr

Avez-vous déjà entendu parler du syndrome d'imposture ?
Dans cet atelier interactif, nous verrons ce que c'est, d'où ça vient et ce qu'on peut y faire.

Vous pourrez participer de manière anonyme dans un navigateur ou avec votre téléphone (j'utilise l'outil wooclap).