MARSEILLE - Journées ANR BOOLE

Université de Provence - 17 et 18 janvier 2011

Centre St Charles - Salle 19

Lundi 17 Janvier

11h : Accueil autour d'un café.

11h30-12h15 : A. Genitrini - *Immunité algébrique : approche de combinatoriciens.*

12h45 : Déjeuner.

14h30-15h15 : E. Maneva - *Bounding the threshold of reconstruction on trees using an iterative algorithm.*

15h30 : Pause café

16h00-16h45 : C. Mailler - *La distribution des arbres croissants sur l'espace des fonctions Booléennes.*

17h00-18h45 : V. Rasendrahasina - *Aspects combinatoire et analytique d'un problème d'optimisation : Max-2-XorSat.*

20h : Dîner au restaurant

Mardi 18 Janvier

9h00-9h45 : V. Bapst - *On the spectrum of random regular graphs with random edges weights.*

10h00 : Pause café

10h30-11h15 : J. Vuillemin - *The dimension of a Boolean function.*

11h30-12h15 : D. Gardy - *Lambda-termes de hauteur unaire bornée.*

12h45 : Déjeuner.

14h15-15h00 : F. Delbot - *Comparaison et évaluation en moyenne d'algorithmes d'approximation pour le problème du vertex cover.*

15h15 : Clôture des journées

Liste des participants

Victor Bapst - ENS - bapst@lpt.ens.fr
Claude Carlet - INRIA - claude.carlet@inria.fr
Brigitte Chauvin - UVSQ - Brigitte.Chauvin@math.uvsq.fr
Julien Clément - LIF - julien.clement@info.unicaen.fr
Nadia Creignou - LIF - nadia.creignou@lif.univ-mrs.fr
Hervé Daudé - LATP - daude@cmi.univ-mrs.fr
Francois Delbot - LATP - francois.delbot@ibisc.fr
Jérémie du Boisberranger - PRISM - Jeremie.Du-Boisberranger@prism.uvsq.fr
Philippe Flajolet - INRIA - Philippe.Flajolet@inria.fr
Hervé Fournier - PRISM - herve.c.fournier@gmail.com
Daniele Gardy - PRISM - Daniele.Gardy@prism.uvsq.fr
Antoine Genitrini - LIP6 - Antoine.Genitrini@lip6.fr
Jean-Marie Lebars - GREYC - jean-marie.le_bars@info.unicaen.fr
Loïck Lhote - GREYC - llhote@info.unicaen.fr
Cecile Mailler - PRISM - cecile.mailler@prism.uvsq.fr
Elitza Maneva - Univ. Barcelone - elitza.maneva@gmail.com
Sihem Mesnager - Univ. Paris 8 - mesnager@math.jussieu.fr
Basile Morcrette - INRIA - bmorcret@dptinfo.ens-cachan.fr
Vonjy Rasendrahasina - LIPN - rasendrahasina@gmail.com
Vlady Ravelomanana - LIAFA - vlad@liafa.jussieu.fr
Raphael Rossignol - ORSAY - raphael.rossignol@math.u-psud.fr
Guilhem Semerjian - ENS - guilhem@lpt.ens.fr
Charlotte Truchet - Univ. Nantes - charlotte.truchet@univ-nantes.fr
Jean Vuillemin - ENS - Jean.Vuillemin@ens.fr

Résumés des interventions

V. Bapst - *On the spectrum of random regular graphs with random edges weights.*
The empirical distribution of the eigenvalues of the adjacency matrix of random regular graphs is well-known to converge, in the large size limit, to the Kesten-MacKay measure. If one replaces the non-zero elements of the adjacency matrix by i.i.d. random variables distributed over $[-1, 1]$ (keeping the matrix hermitian), the support of the distribution of eigenvalues remains the same but the behavior of its density around its edge changes qualitatively, exhibiting an essential singularity known as a Lifshitz tail, due to a large deviation phenomenon. We shall present an analysis of this phenomenon based on a combinatorial approach on the limiting tree to which random regular graphs locally converge.

F. Delbot - *Comparaison et évaluation en moyenne d'algorithmes d'approximation pour le problème du vertex cover.*
Dans la littérature, on considère souvent qu'un algorithme d'approximation polynomial est plus performant qu'un autre lorsqu'il possède un meilleur rapport d'approximation en pire cas. Cependant, il faut être conscient que cette mesure, désormais "classique", ne prend pas en compte la réalité de toutes les exécutions possibles d'un algorithme (elle ne considère que les exécutions menant à la plus mauvaise solution).

Dans mes travaux, je me suis focalisé sur le problème du vertex cover et j'ai tenté de mieux "capturer" le comportement des algorithmes d'approximation en montrant que les performances moyennes d'un algorithme peuvent être décorrélées des performances en pire cas, en évaluant les performances moyennes d'un algorithme et en comparant les performances de différents algorithmes (analytiquement et expérimentalement). J'ai également proposé un algorithme de liste et prouvé analytiquement qu'il retourne toujours une meilleure solution que celle construite par un autre algorithme de liste récent [ORL 2006] quand ils traitent la même liste de sommets (dans certains graphes particuliers, la différence de taille peut être arbitrairement grande).

On constate dans ces études que les algorithmes 2-approchés étudiés sont ceux qui obtiennent les plus mauvaises performances en moyenne et que ceux qui ont les meilleurs comportements moyens ont de mauvais rapports d'approximation.

D. Gardy - *Lambda-termes de hauteur unaire bornée.*
We aim at the asymptotic enumeration of lambda-terms of a given size where the order of nesting of abstractions is bounded whereas the size is tending to infinity. This is done by means of a generating function approach and singularity analysis. The generating functions appear to be composed of nested square roots which exhibit unexpected phenomena. We derive the asymptotic number of

such lambda-terms and it turns out that the order depends on the bound of the height. Furthermore, we present some observations when generating such lambda randomly and explain why powerful tools for random generation as Boltzmann samplers face serious difficulties in generating lambda-terms.

A. Genitrini - *Immunité algébrique : approche de combinatoriciens.*
La génération de suites de nombres aléatoires est une question centrale en cryptographie. Une méthode consiste à combiner des registres à décalages avec une fonction booléenne, bien choisie. En effet, afin de résister à certaines attaques, elle doit posséder plusieurs propriétés : un degré algébrique élevé, le fait d'être équilibrée, ou encore une immunité algébrique élevée... Les spécialistes du domaine s'évertuent donc à construire des classes de fonctions satisfaisant ces contraintes. Pour notre part, nous souhaitons dans un premier temps énumérer les fonctions booléennes d'immunité algébrique maximale (relativement au nombre de variables) et éventuellement exhiber la distribution du nombre de fonctions booléennes suivant l'immunité algébrique. Nous souhaitons développer une énumération récursive afin, dans un second temps, de pouvoir générer aléatoirement les fonctions d'immunité algébrique maximale. Ces travaux sont en cours, et je vais donc vous présenter nos résultats préliminaires.

C. Mailler - *La distribution des arbres croissants sur l'espace des fonctions Booléennes.*
On définit une nouvelle loi de probabilité sur l'ensemble des fonctions Booléennes à k variables, et ce via leur représentation sous forme d'arbres binaires étiquetés. Cette nouvelle loi, que l'on nomme *loi des arbres croissants*, est inspirée du modèle de croissance des arbres binaires de recherche. On l'étudie dans différents systèmes logiques et on la compare à des distributions déjà étudiées : celle des arbres de Catalan, celle des arbres de Galton-Watson, et celle des arbres équilibrés.

E. Maneva - *Bounding the threshold of reconstruction on trees using an iterative algorithm.*
The concept of reconstruction on trees is best illustrated through the model of graph-coloring. Consider a uniformly random coloring of the vertices of a regular tree (or a Galton-Watson tree) of growing depth n using q colors, such that neighbouring vertices are of different colors. The probability that the colour of the root can be reconstructed by observing only the colors of the leafs is bounded away from 1/q (the success probability of a random guess) as long as the (expected) degree of the tree is large enough. How large the degree needs to be for this to hold is precisely the problem of identifying the threshold of reconstruction. This threshold in statistical physics corresponds to the replica symmetry breaking glass transition which is associated with the phenomenon of "clustering" of the set of colorings

of a random graph with the same degree distribution. In physics its location is estimated using a heuristic algorithm known as population dynamics.

I will present an alternative iterative algorithm which provides rigorous upper bounds on the probability of reconstruction. It is based on a method for approximating a recursive sequence of distributions with growing support by another recursive sequence of distributions with small support.

V. Rasendrahasina - *Aspects combinatoire et analytique d'un problème d'optimisation : Max-2-XorSat.*
Nous présentons une approche analytique du problème d'optimisation Max-2-XorSat basée sur la combinatoire analytique et énumérative. Dans cet exposé, nous étudions les séries génératrices liées aux configurations optimales de Max-2-XorSat. En combinant ces outils avec ceux d'analyse complexe, nous quantifions le nombre maximum de clauses satisfaisables des instances aléatoires de Max-2-XorSat.

J. Vuillemin - *The dimension of a Boolean function.*
The dimension of a Boolean function is the rank of the linear space generated over F2 by its BDD sub-functions. It is invariant under input - reversal, although the effect on BDD may be exponential. It is invariant under the Binary Mobius Transform, where the effect on BDD may again be exponential. It follows that the dimension $\dim(f) \leq |DD(f)|$ is a lower bound on the size of a great number of proposed decision diagrams DDs, deterministic and not.

The worst and average dimension of f with $2i$ inputs is 2^i while the gate complexity of f is $O(d^2/i)$.

A Boolean function f of dimension $d = \dim(f)$ is uniquely represented by its minimal ordered multi ?linear circuit $mlc(f)$. The MLC circuit has d AND gates for base ; $O(d^2/i)$ XOR combine base elements. Circuit operations are incremental. The logical ones take $O(d^2)$ word operations, hence $O(d^3)$ bit operations.

More than other DDs, the MLC is interesting for circuit synthesis. With proper input ordering, the MLC for each ALU arithmetic operation yields a (nearly) minimal circuit. In the worst and average case, the MLC circuit is within a factor two of Shannon's optimal circuit. Twisting the compromise between and/xor gates yields a circuit which meets Shannon's bound, and is simpler to describe than Lupanov's original one.