Réunion Boole: Exposés

20-21 juin 2013

Exposés invités

- **Uwe Egly : Questions around quantified boolean formulas.**
- **Bernhard Gittenberger : Infinite dimensional Gaussian limiting distributions in combinatorics.**
  We study random combinatorial structures involving an infinite number of parameters. The random variables are encoded in generating functions satisfying a (possibly infinite) system of functional equations. We prove sufficient conditions under which these random variables tend to an infinite dimensional Gaussian limiting distribution. This is joint work with Michael Drmota and Johannes Morgenbesser.
- **Alfredo Viola : Some ideas to study bent functions.**
  In this informal talk I would like to comment about some empirical evidence I have found in studying bent functions, under a point of view that I have not seen before. In any case, I would like to know the opinion of experts in the area, to see how far we can advance with these ideas in the understanding of the problem. No new results will be present, and it may be the case that the presentation could turn into an interactive discussion, that I hope could be fruitful.

Exposés de membres du projet Boole

- **Nicolas Broutin : Autour des limites d'échelle des graphes aléatoires critiques.**
  Après avoir rappelé quelques généralités sur les graphes aléatoires et introduit les quelques notions topologiques nécessaires, je discuterai de la manière dont on peut généraliser les résultats d'Aldous sur la limite d'échelle d'arbres aléatoires à des graphes. Je survolerai aussi les applications à d'autres problèmes d'optimisation combinatoire / physique statistique, en particulier l'arbre couvrant minimal.
- **Brigitte Chauvin et Nicolas Pouyanne : VLMC et marche aléatoire persistante.**
  Des lettres X_n sont produites avec une source VLMC (Variable Length Markov Chain). On s'intéresse à la marche aléatoire $S_n = X_1 + \ldots + X_n$ qui n'est plus du tout markovienne. Elle est dite persistante. Renormalisée, elle converge vers un processus continu, que l'on identifie, de type processus zigzag.
- **Nadia Creignou et Vlady Ravelomamana : Diverses questions de satisfaisabilité.**
- **Élie de Panafieu : 2Q-Xor-Sat.**
- **Danièle Gardy : Lambda-termes.**
  Les lambda-termes (les termes du lambda-calcul) peuvent être vus comme des arbres enrichis ou coloriés. Nous nous intéressons à leur étude d'un point de vue combinatoire, en abordant des questions telles que tout d'abord leur dénombrement, et différentes propriétés structurelles (répartition des noeuds de différents types, hauteur, proportion de termes en forme normale, ...). Ces résultats portent sur des classes de termes restreints, soit par le nombre de noeuds unaires, au total ou le long d'une branche, soit par le nombre de variables liées par une abstraction.
- **Antoine Genitrini et Cécile Mailler : Overview of quantitative logic.**
  15 years ago, the first probability distribution on Boolean functions induced by random formulas was introduced. It has then been intensively studied and extended. Some key-behaviours have been pointed out by several papers. Analogous results between models based on distinct sets of connectives, but also between models that swap, in some sense, both limits on the size of the formulas and the number of variables they depend. During the talk, we will overview these similar behaviours.
- **Sihem Mesnager : Résultats récents sur des objets rares et optimaux en cryptographie symétrique.**
  La notion de fonction courbe fut introduite par Rothaus et étudiée pour la première fois par Dillon en 1974. Depuis lors, l'étude des fonctions courbes n'a pas cessé car ces fonctions jouent un rôle important non seulement en cryptographie symétrique mais aussi en théorie des codes et dans le domaine des séquences. Une fonction booléenne d'un nombre pair de variables est dite courbe si elle est de nonlinéarité maximale. En cryptographie symétrique, les fonctions courbes sont les fonctions présentant une résistance optimale à l'attaque dite attaque par corrélation rapide. Les fonctions hyper-courbes furent introduites par Youssef et Gong en 2001. Les fonctions hyper-courbes présentent un

intérêt à la fois théorique et pratique. De telles fonctions sont certainement plus rares que les fonctions courbes mais, à ce jour, on connaît très peu de familles de fonctions hyper-courbes. Même si elles sont moins nombreuses que les fonctions courbes, avoir une classification des fonctions hyper-courbes semble illusoire et donc identifier le plus possible de familles de fonctions hyper-courbes est important et permettra certainement de mieux comprendre leur structure. Nous présentons un résumé de nos avancées les plus importantes (obtenues pendant les 4 dernières années dans le cadre de l'ANR Boole) sur les fonctions booléennes courbes et leurs dérivées.

– **Basile Morcrette et Nicolas Pouyanne : Urnes de Pólya, combinatoire analytique, et problème des moments.**
Survol des méthodes et techniques de combinatoire analytique pour l'étude des urnes de Pólya. Pour les fonctions génératrices algébriques : traitement automatique et asymptotique. Pour des extensions aux urnes de Pólya (ajout d'aléa dans les règles de remplacement, urnes non équilibrées) : lien entre série génératrice et équations différentielles.
Brève exposition du problème des moments pour une loi de probabilité. Application au cas des grandes urnes à deux couleurs, où l'on montre que leurs lois limites sont déterminés par leurs moments.