Théorèmes limites pour les empilements d'intervalles et de carrés aléatoires.

Stéphane BOUCHERON

(Laboratoire de Recherche en Informatique, LRI, Université Paris-Sud)

Scheinermann a proposé en 1989 le modèle suivant: on tire de manière identique et indépendante $2n$ points sur l'intervalle $[0,1]$: $(X_i)_{i=1\dots 2n}$. Les n paires (X_{2i-1}, X_{2i}) définissent n intervalles. Quelle est le nombre maximal d'intervalles disjoints que l'on peut extraire de cette collection ? Cette quantité suit une loi des grands nombres, elle se concentre autour de $\sqrt{\frac{\pi n}{2}}$ (Justicz et al 1990). Nous montrons en analysant un algorithme glouton que cette quantité suit un théorème central limite et un principe de grandes déviations.

Le problème du calcul du nombre maximal cubes disjoints dans une famille de cubes aléatoires sur $[0,1]^d$ peut être posé en dimension quelconque. Il devient difficile du point de vue algorithmique. Néanmoins, on peut montrer la persistance d'une loi des grands nombres, et vérifier que les inégalités de concentration déduites en observant qu'on a affaire à des "fonctions de configuration" donnent des ordres de grandeur corrects pour les probabilités de queue.

Travail commun avec Wenceslas Fernandez de la Vega.

On the stability number of random interval graphs
http://www.lri.fr/ bouchero/PUB/snrig.ps.gz
Combinatorics, Probability and Computing (à paraître)

On a square packing problem. (soumis)
http://www.lri.fr/ bouchero/PUB/spp.ps.gz

INFORMATION THEORY BY ANALYTIC METHODS

Wojtek SZPANKOWSKI

(Purdue, University)

Recent years have seen a resurgence of interest in redundancy rates of lossless coding. The redundancy rate problem for a class of sources consists in determining by how much the actual code length exceeds the optimal (ideal) code length. In a minimax scenario one finds the maximal redundancy over all sources within a certain class while in the average scenario one computes the average redundancy over all possible source sequences. The redundancy rate problem is typical of a situation where second-order asymptotic play a crucial role (since the leading term of the optimal code length is known to be the entropy of the source). This problem is an ideal candidate for "analytic information theory", which applies analytic tools (i.e., complex analysis) to information theory. In this talk, we survey our recent results on the redundancy rate problem obtained by analytic methods. In particular, we present our findings for the redundancy of Shannon codes, Huffman codes, minimax redundancy for memoryless sources and renewal processes, and Lempel-Ziv codes. We shall briefly discuss some analytic tools used to establish these results, such as Fourier analysis, generating functions, singularity analysis, Mellin transform, the saddle point method, and analytic depoissoinization. To illustrate these techniques in some depth we will present one result in some detail (e.g., redundancy of Shannon and Huffman codes).

Graphes, Polynômes, Cryptographie, et Jeux d'Arthur et Merlin

Jacques PATARIN

(Laboratoire Prism, UVSQ)

Le concept de Cryptographie à clé publique a été publié pour la 1ère fois en 1976. Les premiers algorithmes découverts (et les plus utilisés, encore aujourd'hui) reposaient sur des calculs modulo de grands nombres entiers. Il existe cependant des moyens très différents de faire de la cryptographie à clé publique, comme les algorithmes à base d'Isomorphisme de Graphes ou d'Isomorphisme de Polynômes que nous allons présenter. Ces algorithmes présentent l'avantage d'être très simples à décrire et d'être "Zero-Knowledge" : on parvient à prouver que l'on connaît un secret sans rien révéler de ce secret. De plus en utilisant les jeux dits "d'Arthur-Merlin" (le roi Arthur et Merlin l'enchanteur) on peut les classifier assez bien vis à vis de la théorie de la complexité.