Résumé des exposés

Ali Akhavi – Speeding-up lattice reduction by random projections

Lattice reduction algorithms such as LLL and its floating-point variants have a very wide range of applications in computational mathematics and in computer science: polynomial factorization, cryptology, integer linear programming, etc. It can occur that the lattice to be reduced has a dimension which is small with respect to the dimension of the space in which it lies. This happens within LLL itself. We describe a randomized algorithm specifically designed for such rectangular matrices. It computes bases satisfying, with very high probability, properties similar to those returned by LLL. It significantly decreases the complexity dependence in the dimension of the embedding space. Our technique mainly consists in randomly projecting the lattice on a lower dimensional space, by using two different distributions of random matrices.

Marie Albenque (Univ. Paris 7) – Animaux dirigés et modèles de gaz markoviens

Un animal dirigé de source S est un ensemble de sommets d'un graphe orienté G qui contient S et tel que tout élément de l'animal puisse être atteint depuis un sommet de S par un chemin orienté dont tous les sommets appartiennent à l'animal. Un modèle de gaz sur G est une fonction qui à chaque sommet de G associe 0 ou 1.

Dhar a montré dans les années 80 qu'il y avait un lien entre la série génératrice des animaux dirigés et la probabilité d'occupation d'un sommet pour un certain modèle de gaz aléatoire. En 1996, Bousquet-Mélou et Conway ont donné la série génératrice des animaux dirigés à une source sur une famille de réseaux, en utilisant un modèle de gaz ad-hoc. J'expliquerai dans cet exposé comment étendre leur résultat à un ensemble plus général de sources en m'appuyant sur un modèle de gaz introduit par Le Borgne et Marckert en 2007. Je montrerai en particulier que le modèle de gaz obtenu est markovien.

Axel Bacher (Univ. Bordeaux 1) – Périmètre de site moyen des animaux dirigés sur les réseaux carrés

Un animal dirigé de source s dans un graphe G est un ensemble fini A de points tel que pour tout sommet v de A, on puisse tracer un chemin de s vers v ne passant que par des points de A. Le périmètre de site d'un animal A est le nombre de points v de G qui ne sont pas dans A mais tels que $A \cup \{v\}$ reste un animal dirigé.

L'énumération des animaux dirigés sur les réseaux carrés a été faite pour la première fois par Dhar. Notre but sera de prouver des conjectures de Conway et Le Borgne, qui donnent le périmètre de site moyen d'un animal à n points dans plusieurs réseaux carrés. La preuve utilise une correspondance entre les animaux et des empilements de pièces, s'inspirant des travaux de Bétréma, Penaud et Viennot.

Cyril Banderier (Univ. Paris 13) – La constante de Duchon... des clubs de Duchon.

Imaginons un club (dit de "Duchon", pour des raisons historiques) dans lequel les clients entrent à 2 et ressortent à 3. Le club ouvre à minuit (vide) et ferme à 5h du mat (vide). Sachant qu'il y a eu n entrées/sorties, quelle a été son occupation moyenne ? (NB: tous les scénarios sont pris équiprobables.) Cette question est bien sûr reliée à l'aire moyenne sous une marche aléatoire (une excursion sur N qui fait des sauts +2 ou -3). L'aire était connue être en $A.n^{3/2}$, pour une mystérieuse constante A. Nous

donnons ici la valeur exacte de cette "constante de Duchon".
Je présenterai ainsi dans cet exposé les progrès faits (avec Bernhard Gittenberger) sur l'asymptotique de l'aire moyenne (dans le cadre assez général des "chemins de Dyck généralisés").
Ceci passe (one more time) par l'étude des racines d'une équation algébrique... (la méthode du noyau frappe encore), et je finirai par une application de cette étude à un problème que j'avais commencé à regarder, avec Philippe Flajolet, durant ma thèse : la hauteur maximale d'une marche aléatoire !

Olivier Bernardi (Univ. Paris-Sud) – Une bijection entre sous-graphes et orientations basée sur la combinatoire du polynôme de Tutte

Le polynôme de Tutte est un invariant fondamental de la théorie des graphes. Le polynôme de Tutte $T_G(x, y)$ d'un graphe G peut être spécialisé de manière à obtenir de nombreuses informations énumératives sur G, comme par exemple, le nombre d'arbres couvrants, le nombre d'orientations acycliques ou encore le nombre de coloriages de G en q couleurs pour tout q.

Dans cet exposé, nous rappellerons les définitions et propriétés classiques du polynôme de Tutte. Nous donnerons ensuite un caractérisation nouvelle du polynôme de Tutte d'un graphe G qui nécessite de munir G d'un plongement. Une fois le plongement choisi, le polynôme de Tutte s'exprime comme la série génératrice des arbres couvrants comptés selon leurs *activités de plongement*.

Les activités de plongement des arbres couvrants d'un graphe G permettent aussi de définir une bijection entre les sous-graphes couvrants et les orientations de G. Cette bijection possède des propriétés remarquables, comme le fait d'établir une correspondance entre les sous-graphes connexes et les orientations racine-accessibles ou encore les sous-graphes sans cycles (les forets) avec les orientations minimales. On établira, par ce biais, l'interprétation combinatoire de plusieurs spécialisations du polynôme de Tutte en termes d'orientations ou de suite de degrés.

Michel Bauer (IPhT, CEA Saclay et LPT, ENS) – Évolutions de Loewner stochastiques : le regard d'un physicien.

Les courbes aléatoires intéressent depuis longtemps physiciens et mathématiciens. Les premiers sont intéressés par les interfaces séparant deux phases dans certains systèmes physiques à deux dimensions. Les mathématiciens se concentrent souvent sur des objets purement géométriques comme les marches auto-évitantes.

Au tournant du millénaire Oded Schramm a défini de nouveaux processus stochastiques qui décrivent conjecturalement la limite continue de ces courbes aléatoires sous une hypothèse d'invariance conforme. Ces processus de croissance SLE (pour Schramm-Loewner Equation) ont complètement révolutionné notre compréhension des interfaces bidimensionnelles.

Après avoir montré des exemples de systèmes discrets dont la limite continue est décrite par SLE, tant en physique qu'en mathématique, je présenterai l'équation de Schramm-Loewner et je dirai quelques mots de ses applications à des calculs explicites.

Les développements autour de SLE ont aussi mené à la solution élégante de quelques conjectures mathématiques et j'en donnerai un exemple.

Si le temps le permet je présenterai le lien entre l'approche via le calcul stochastique des mathématiciens et l'approche via la théorie des groupes des physiciens.

Je conclurai sur quelques problèmes ouverts.

Nicolas Bonichon (Univ. Bordeaux 1) – Permutations de Baxter et orientations bipolaires planes

(Travail commun avec E. Fusy et M. Bousquet-Mélou) Nous présenterons une bijection directe entre

les permutations de Baxter de taille n et les orientations bipolaires planes à n arêtes. Cette bijection transporte plusieurs paramètres classiques des permutations de Baxter (nombre de montées, nombre de descentes, nombre de saillants supérieurs gauches...) vers des paramètres tout aussi classiques des orientations bipolaires planes (nombre de faces internes, nombre de sommets, degré du puits...). De plus, cette bijection produit des dessins polylines compacts pour les cartes considérées. Nous présenterons également 2 spécialisations de cette bijection.

Mireille Bousquet-Mélou (Univ. Bordeaux 1) – Excursions discrètes

L'énumération des chemins de Dyck est un domaine archi-balisé de la combinatoire énumérative. On sait bien, notamment, que
• la série génératrice de ces chemins satisfait $D = 1 + t^2D^2$,
• la série qui compte les chemins de hauteur au plus k est rationnelle, avec pour expression $F(k)/F(k+1)$, où les $F(k)$ sont les polynômes de Fibonacci, et satisfont $F(k+1) = F(k) - t^2F(k-1)$.

On clarifiera dans cet exposé comment ceci s'étend à des chemins de Dyck généralisés (aussi appelés excursions, c'est plus court), prenant leurs pas dans un ensemble fini donné. Des liens pas forcément attendus avec les fonctions de Schur apparaissent dans ce travail.

Guillaume Chapuy (École Polytechnique) – Cartes de genre supérieur, cartes à une face

On parle souvent de cartes planaires, mais les cartes peuvent aussi être dessinées sur d'autres surfaces, comme le tore, ou plus généralement le tore à g trous. Les bijections transformant les cartes planaires en arbres étiquetés marchent encore, à condition de remplacer les arbres par des cartes à une seule face (leur analogue en genre supérieur). Ces bijections sont universelles (i.e. marchent pour de nombreuses familles de cartes, comme les $2k$-angulations ou les constellations), et permettent de faire de l'énumeration asymptotique explicite, en particulier de retrouver l'universalité de l'exposant de comptage $n^{5/2(g-1)}$. Cela demande de bien comprendre comment sont faites les cartes à une face, ce qui reste un problème partiellement ouvert. (une partie du travail est commune avec G.Schaeffer et M.Marcus).

Philippe Chassaing (Université Henri-Poincaré) – Sur quelques statistiques liées aux factorisations des mots

Travail commun avec Elahe Zohoorian-Azad.
Dans les années 1990, Pitman, Diaconis et Mc Grath ont obtenus des résultats sur le nombre de facteurs de longueur 1, 2, 3, etc dans la décomposition de Lyndon d'un mot aléatoire de longueur n, écrit à l'aide d'un alphabet à q lettres équiprobables. Leur approche est d'utiliser une "bijection" entre les mots et les permutations, associant les facteurs du mot aux cycles de la permutation, et de considérer la loi de probabilité sur les permutations induite par cette "bijection".

Alors que Pitman, Diaconis et Mc Grath s'intéressent aux petits facteurs de la décomposition de Lyndon, nous énonçons dans cet exposé des résultats sur la longueurs des facteurs qui sont *à droite* (ou bien à la fin du mot) dans la décomposition de Lyndon. En particulier, les facteurs les plus longs se trouvent être plutôt à la fin. Nos résultats valent pour une distribution de probabilité arbitraire sur alphabet arbitraire, éventuellement infini. La méthode de preuve mêle probabilités et algèbre (des mots), un peu à la manière d'articles récents de Bassino, Clément et Nicaud, ou encore de Marchand et Zohoorian-Azad.

Nadia Creignou (Univ. de la Méditerranée) – Transition de phase et formules booléennes quantifiées

auteurs: Nadia Creignou, Hervé Daudé, Uwe Egly, Raphaël Rossignol

Résumé: Le problème QSAT est la version quantifiée du problème de satisfaisabilité SAT. Nous étudions la transition de phase associée aux instances aléatoires de QSAT. Nous examinons deux problèmes en particulier. L'un est le problème QXOR-SAT, le second peut-être vu comme une variante du problème 2-SAT. Nous proposons une étude de ces problèmes à la fois pratique et théorique, qui permet d'éclairer l'influence des paramètres utilisés pour définir les formules aléatoires.

Alexis Darrasse (Univ. Pierre et Marie-Curie) – Distances dans les structures de réseaux Apolloniens aléatoires

Travail commun: Olivier Bodini, Alexis Darrasse et Michèle Soria

Nous etudions la distribution des distances dans les structures des réseaux apolloniens aléatoires (RANS), une famille de graphes en bijection avec les arbres ternaires planaires. En nous appuyant sur l'utilisation de séries génératrices multivariées pour décrire toute l'information sur les distances, ainsi que sur l'analyse de singularités pour evaluer les coefficients de ces séries, nous décrivons la distribution des distances vers un sommet externe du RANS et montrons que la distance moyenne entre deux sommets quelconques d'un RANS d'ordre n est asymptotiquement $\sqrt{n}$.

Alain Denise (Univ. Paris-Sud) – Génération aléatoire appliquée au test statistique et au model checking

Je présenterai des travaux en cours depuis quelques années au LRI pour appliquer des techniques de génération aléatoire de chemins au test de logiciel, et plus généralement de tout modèle représentable par des graphes. Je parlerai des travaux que nous effectuons
- pour le test statistique de logiciel, où l'un des problèmes consiste à savoir biaiser la distribution des chemins engendrés de façon à respecter un "critère de couverture" du programme que l'on teste ;
- pour le "model checking", où il est nécessaire de tirer des chemins uniformément dans de très grands "modèles", en tirant profit de la décomposition de ces modèles en modèles bien plus petits.

Références :

Alain Denise, Marie-Claude Gaudel, and Sandrine-Dominique Gouraud. A generic method for statistical testing. In Proc. of 15th IEEE International Symposium on Software Reliability Engineering (ISSRE 2004), 2004. http://www.lri.fr/Rapports-internes/2004/RR1386.pdf

Alain Denise, Marie-Claude Gaudel, Sandrine-Dominique Gouraud, Richard Lassaigne, and Sylvain Peyronnet. Uniform random sampling of traces in very large models. Proceedings of the First International Workshop on Random Testing (RT 2006). http://www.lri.fr/Rapports-internes/2006/RR1445.pdf

---

Philippe Flajolet (INRIA -Rocquencourt) – Mellin vu du ciel

La transformation de Mellin fait partie de l'arsenal classique des transformations intégrales, tant en analyse qu'en théorie analytique des nombres. L'objectif de cet expoé est d'en brosser les principales propriétés utiles en analyse asymptotique et en analyse d'algorithmes. On visera, sans trop se soucier de détail, à en organiser l'utilisation selon quelques principes simples incluant les correspondances singularités–asymptotique et la factorisation des sommes harmoniques. Les liens avec l'estimation des sommes dyadiques, liées aux arbres digitaux, à leurs variantes, ainsi qu'à à l'analyse dynamique seront discutés. L'exposé sert ainsi de complément introductif au cours de Julien Clément à ALEA-2008.

Danièle Gardy (Univ. Versailles-Saint Quentin) – Fonctions génératrices pour la satisfiabilité

Dans les dernières années, un certain nombre de travaux ont porté sur les expressions booléennes aléatoires, et les lois de probabilité en arbre qu'elles conduisent à définir sur les fonctions booléennes.

Nous étudions ici ce que cette approche peut apporter aux problèmes de satisfiabilité. Nous considérerons en particulier le cas de 2XOR-SAT.

Antoine Genitrini (Univ. Versailles-Saint Quentin) – Probabilité et complexité des fonctions Booléennes dans le système de l'Implication

Travail commun avec H. Fournier, D. Gardy, B. Gittenberger

Mon exposé considère des expressions Booléennes construites à l'aide d'un unique connecteur, l'Implication et de k variables. Nous définissons une suite de mesures de probabilités dépendant de k puis étudions sa limite lorsque k croît. Ce travail établit un lien entre la probabilité et la complexité des fonctions Booléennes : $Proba(f) = C_f/(4^k.k^{L(f)+1})$, où $L(f)$ est la complexité de f. Afin d'obtenir C_f nous introduisons des règles d'expansions et d'élagages sur les expressions (représentées par des arbres). Le nombre C_f correspond au nombre d'expansions valides des arbres minimaux de f. De plus, nous pouvons donner des bornes sur C_f ce qui nous donne des bornes sur la probabilité de f.

Lucas Gerin (Université Henri-Poincaré) – Convergences lente et rapide de particules sur une grille.

Le but de cet exposé est de décrire certains systèmes de particules très simples sur une grille finie : il s'agit d'une classe particulière d'Automates Cellulaires $2D$. La plupart de ces systèmes convergent vers un état stable, je vais essayer d'expliquer pourquoi la convergence est parfois rapide (polynomiale en le nombre de cellules) ou lente (exponentielle). (Travail en cours avec Nazim Fatès, LORIA)

Thierry Klein (Univ. Paul Sabatier) – Grandes déviations conditionnées: Application à la combinatoire

Soit $(X^{(n)}, Y^{(n)}) \in \mathbb{N} \times \mathbb{R}$ un vecteur aléatoire. Pour chaque n on se donne des copies indépendantes $(X_1^{(n)}, Y_1^{(n)}), (X_2^{(n)}, Y_2^{(n)}) \dots$ de $(X^{(n)}, Y^{(n)})$. Posons , pour $n \in \mathbb{N}^*$ et $q_n \in \mathbb{N}^*$, $S_n = X_1^{(n)} + \cdots + X_{nq_n}^{(n)}$ et $T_n = Y_1^{(n)} + \cdots + Y_{nq_n}^{(n)}$.
Dans cet exposé nous commencerons par montrer à partir de deux exemples classiques de quelle manière la loi de T_n conditionnée par l'événement $\{S_n = np_n\}$ apparaît naturellement dans de nombreux problèmes combinatoires. Puis nous étudierons le comportement asymptotique de cette loi en regardant ces propriétés de grandes déviations.
Nous rappelons qu'une suite de mesure de probabilité (R_n) vérifie un principe de grandes déviations de fonction de taux I à la vitesse a_n si:
i) I est s.c.i. à valeur dans $\mathbb{R}^+ \cup \{+\infty\}$.
ii) Pour tout ensemble mesurable A:

$$-I(\text{int } A) \leq \liminf_{n\to\infty} a_n \log R_n(A) \leq \limsup_{n\to\infty} a_n \log R_n(A) \leq -I(\text{clo } A),$$

où $I(A) = \inf_{\xi\in A} I(\xi)$ et $\text{int } A$ (resp. $\text{clo } A$) est l'intérieur (resp. l'adhérence) de A.

Guy Louchard (Univ. Libre de Bruxelles). – Tail estimates for the Brownian excursion area and other Brownian areas (Joint work with S.Janson)

Several Brownian areas are considered in this work: the Brownian excursion area, the Brownian bridge area, the Brownian motion area, the Brownian meander area, the Brownian double meander area, the positive part of Brownian bridge area, the positive part of Brownian motion area. We are interested in the asymptotics of the right tail of their density function. Inverting a double Laplace transform, we

can derive, in a mechanical way, all terms of an asymptotic expansion. We illustrate our technique with the computation of the first four terms. We also obtain asymptotics for the right tail of the distribution function and for the moments. Our main tool is the two-dimensional saddle point method.

Grégory Miermont (Univ. Paris-Sud) – Quelques propriétés métriques des cartes continues

On s'intéresse aux espaces métriques obtenus comme limites d'échelle des grandes quadrangulations aléatoires, en genre quelconque. En utilisant une variante multi-pointée de la bijection de Schaeffer, on montre, entre autres, une propriété d'unicité du chemin géodésique entre deux points typiques.

Pierre Nicodème (École Polytechnique) – Clump analysis

Travail commun: Frederique Bassino, Julien Clement, Julien Fayolle, Pierre Nicodeme

We analyse by formal language manipulations and translation to generating functions several statistics associated to clump counts of a "pattern" in random texts. Texts are generated by a Bernoulli model and we consider as "pattern" a finite reduced set of words (no word is factor of another word in the set). Considering all the occurrences of words from this set in a text, a clump is either (a) an isolated occurrence, or (b) a maximal set of occurrences such that each occurrence overlaps at least another occurrence of the set (i.e. of the clump). We typically consider the number of clumps, the number of occurrences in clumps and the total size of the text covered by clumps.

Carine Pivoteau (Univ. Pierre et Marie-Curie) – Itération de Newton combinatoire pour le calcul de l'oracle de Boltzmann

La génération aléatoire sous le modèle de Boltzmann repose sur les valeurs des séries génératrices en des points intérieurs à leur disque de convergence. Le calcul de ces valeurs est traditionnellement relégué à un "oracle". Nous produisons un tel oracle pour une grande classe de structures spécifiées par des systèmes combinatoires. Cet oracle repose sur une itération de Newton au niveau des structures combinatoires elles-mêmes, généralisant des travaux de Bergeron, Décoste, Labelle et Leroux. Il en découle aussi un algorithme quasi-optimal pour le calcul des séries génératrices d'énumération.

Vlady Ravelomanana (Univ. Paris 13) – Formules 2-XORSAT aléatoires dans la fenêtre critique

Nous considérons le problème de satisfaisabilité des formules 2-XOR. Ces formules sont des conjonctions d'équations booléennes de la forme $x \oplus y = 0$ (ou $x \oplus y = 1$). Une formule aléatoire de taille m sur n variables est générée en choisissant uniformément m équations parmi les $\binom{n(n-1)}{m}$ possibles. La probabilité $p(n, m)$ qu'une telle formule soit satisfaisable décroît en fonction de la taille m de la formule. Lorsque n tend vers l'infini, la transition de phase de la satisfaisabilité à l'insatisfaisabilité s'effectue pour les valeurs $0 < c < 1/2$ du paramètre d'ordre $c = m/n$. Nous proposons une étude fine de la probabilité $p(n, m)$ lorsque m varie dans la fenêtre critique du seuil de satisfaisabilité : $m = n/2(1 + \mu n^{-1/3})$. En exploitant des résultats d'énumération exacte de familles de graphes contraints, nous montrons que $p(n, n/2(1 + \mu n^{-1/3})) = \Theta(n^{-1/12})$. Pour le problème de satisfaction de contraintes 2 XORSAT, ce résultat valide l'exposant critique, $(-1/12)$, inféré par les physiciens. Nous explicitons la fonction f, définie par $f(\mu) = \lim_{n \to +\infty} n^{1/12} p(n, n/2 + \mu n^{2/3})$, à l'aide de la fonction d'Airy.

Charlotte Truchet (Univ. Nantes) – Un modèle markovien pour Walk-SAT

Les algorithmes de résolution de SAT les plus efficaces en général sont incomplets et assez forte-

ment aléatoires. Expérimentalement, leur comportement est assez bien connu, cependant il existe peu de résultats théoriques sur le sujet. On s'intéressera ici à GSAT et WalkSAT, proposés par Selman en 92 et 94. Les observations expérimentales font notamment apparaître une forte dépendance du temps de calcul à certains paramètres de l'algorithme - en pratique, le réglage de ces paramètres est fait à la main. On propose un modèle de Markov naturel pour les algorithmes GSAT et WalkSAT. Ce modèle permet de donner deux majorations du temps de calcul en fonction des valeurs propres de la matrice de transition, qui dépend elle-même de l'instance de SAT et du paramétrage de l'algorithme. Nous montrons expérimentalement sur de petites instances que cette borne permet de retrouver le paramétrage optimal observé dans la littérature. Ceci fournit une piste pour déterminer automatiquement le paramétrage optimal. Cependant, le calcul de la borne est d'une complexité rédhibitoire. Des pistes de recherche pour l'approximer seront présentées.

Brigitte Vallee et Antonio Vera (Univ. Caen) – Analyse probabiliste de l'algorithme de reduction des reseaux de Gauss

(I) Analyse de la configuration de sortie
(II) Analyse de l'execution de l'algorithme

L'algorithme de réduction des réseaux dû à Gauss, construit, à partir d'une base d'un réseau de dimension 2, et en temps polynomial, une base "minimale" du réseau. Cet algorithme est central, car il est à la base du célèbre algorithme LLL de réduction de réseaux, qui résout le même genre de problème pour une dimension quelconque: l'algoritthme LLL construit, à partir d'une base d'un réseau de dimension n quelconque, et en temps polynomial, une base du réseau, formée de vecteurs assez courts et assez orthogonaux. L'algorithme LLL est très utilisé, mais son comportement probabiliste est très mal compris.

Le projet ANR LAREDA cherche à élucider ce comportement probabiliste de l'algorithme LLL. Il faut commencer par la dimension 2, et cet exposé décrira des premiers résultats qui décrivent à la fois l'exécution de l'algorithme et sa configuration de sortie. Nous expliquerons aussi comment ces résultats constituent une première étape pour décrire le comportement de l'algorithme LLL.
