INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Algorithms

Algorithms

Paris - Rocquencourt

THEME SYM

Activity Report

2008

Table of contents

1. Team

Research Scientist

Philippe Flajolet [Research Director (DR) Inria, HdR]
Bruno Salvy [Research Director (DR) Inria]
Alin Bostan [Research Associate (CR) Inria]
Frédéric Chyzak [Research Associate (CR) Inria]

Faculty Member

Philippe Dumas [Professor, Cl. Prép. lycée Jean-Baptiste Say]
Brigitte Chauvin [Professor, University of Versailles, from September]

PhD Student

Alexandre Benoit [starting September]
Shaoshi Chen
Marc Mezzarobba [ENS Paris]

Post-Doctoral Fellow

Nicolas Broutin [McGill University, till September]
Nicolas Le Roux [Professeur en disponibilité, Rectorat de Créteil, till September]
Manuel Kauers [RISC, Linz, till December]

Administrative Assistant

Virginie Collette [(TR) Inria]

2. Overall Objectives

2.1. Overall Objectives

The primal objective of the project is the field of analysis of algorithms. By this is meant a precise quantification of complexity issues associated to the most fundamental algorithms and data structures of computer science. Departing from traditional approaches that, somewhat artificially, place emphasis on worst-case scenarii, the project focuses on average-case and probabilistic analyses, aiming as often as possible at realistic data models. As such, our research is inspired by the pioneering works of Knuth.

The need to analyze, dimension, and finely optimize algorithms requires an in-depth study of random discrete structures, like words, trees, graphs, and permutations, to name a few. Indeed, a vast majority of the most important algorithms in practice either "make bets" on the likely shape of input data or even base themselves of random choices. In this area we are developing a novel approach based on recent theories of combinatorial analysis together with the view that discrete models connect nicely with complex-analytic and asymptotic methods. The resulting theory has been called "Analytic combinatorics". Applications of it have been or are currently being worked out in such diverse areas as communication protocols, multidimensional search, data structures for fast retrieval on external storage, data mining applications, the analysis of genomic sequences, and data compression, for instance.

The analytic-combinatorial approach to the basic processes of computer science is very systematic. It appeared early in the history of the project that its development would greatly benefit from the existence of symbolic manipulation systems and computer algebra. This connection has given rise to an original research programme that we are currently carrying out. Some of the directions pursued include automating the manipulation of combinatorial models (counting, generating function equations, random generation), the development of "automatic asymptotics", and the development of a unified view of the theory of special functions. In particular, the project has developed the Maple library *Algolib*, that addresses several of these issues.

3. Scientific Foundations

3.1. Analysis of Algorithms

Keywords: *analysis of algorithms*, *analytic combinatorics*, *asymptotic enumeration*, *combinatorial analysis*, *hashing methods*, *index tree*, *limit laws*, *random discrete structures*.

While we know the laws of basic physics and while probabilists have been setting up a coherent theory of stochastic processes for about half a century, the "laws of combinatorics", in the sense of the laws governing random structured configurations of large sizes, are much less understood. Accordingly, our knowledge in the latter area is still very much fragmentary. Some of the difficulties arise from the large variety of models that tend to surface in real-life applications—the world of computer scientists and algorithmic designers is really an artificial world, much more "free" than its physical counterpart. Some of us have then engaged in the long haul project of trying to offer a unified perspective in this area. The approach of analytic combinatorics has evolved from there.

Analytic combinatorics leads to discovering randomness phenomena that are "universal" (a term actually borrowed from statistical physics) across seemingly different applications. For instance, it is found that similar laws govern the behaviour of prime factors in integers, of irreducible factors in polynomials, of cycles in permutations, and of components in mappings of a finite set. Once detected, such phenomena can then be exploited by specific algorithms that factor integers (a problem relevant to public-key cryptography), decompose polynomials (this is needed in computer algebra systems), reorganize tables in place (this is of obvious interest in the manipulation of various data sets), and use collisions to estimate the cardinality of massive data ensembles. The underlying technology bases itself on generating functions, which exactly describe discrete models, as well as an interpretation of these generating functions as analytic transformations of the complex plane. Singularities together with the associated perturbative theory then deliver a number of very precise estimates regarding important characteristics of random discrete structures. The process can be largely made formal and accessible to computer algebra (see below) and it may be adapted to the broad area of analysis of algorithms.

3.2. Computer Algebra

Keywords: *Gröbner bases*, *asymptotic scales*, *random generation*, *special functions*.

Computer algebra at large aims at making effective large portions of mathematics, paying due attention to complexity issues. For reasons mentioned above, our project specifically investigates the way mathematical objects originating in complex analysis can be dealt with in an algorithmic way by computer algebra systems. Our main contributions in this area concern the automation of asymptotic analysis and the handling of special functions. The mathematical foundations of our algorithms are deeply rooted in differential algebra (Hardy fields for asymptotic expansions and Ore algebras for special functions).

Over the years, in order to automate the average-case analysis of ever larger classes of algorithms, we have developed algorithms and implementations for the following problems: the specification of formally specified combinatorial structures; the corresponding problems of enumeration and random generation; the automatic construction of asymptotic scales which is necessary for extracting the singular behaviour of generating functions; the automatic computation of asymptotic expansions in such scales; the automatic computation of asymptotic expansions satisfied by coefficients of generating series. An *Encyclopedia of Combinatorial Structures*, available on the web, gathers roughly one thousand structures for which generating series, recurrences, and asymptotic behaviour have been determined automatically using our libraries.

An important principle of computer algebra is that it is often easier to operate with equations defining a mathematical object implicitly rather than trying to obtain a "closed-form" expression of it. The class of linear differential and difference equations is particularly important in view of the large variety of functions and sequences they capture. In this area, we have developed the highly successful GFUN package (jointly with P. Zimmermann, from the Spaces project) dealing with the univariate case. In the multivariate case, we have developed the underlying theory based on Gröbner bases in Ore algebra, and an implementation in the MGFUN package. The algorithmic advances of the past few years have made it possible to start the implementation of an *Encyclopedia of Special Functions*, providing various information concerning classical functions (of wide use throughout sciences), including Bessel functions, Airy functions, ... The corresponding information is all automatically generated.

4. Software

4.1. Software

The *Algolib* library is a set of Maple routines that have been developed in the project for more than 10 years. Several parts of it have been incorporated into the standard library of Maple, but the most up-to-date version is always available for free from our web pages. This library provides: tools for combinatorial structures (the *combstruct* package), including enumeration, random or exhaustive generation, generating functions for a large class of attribute grammars; tools for linear difference and differential equations (the *gfun* package), which have received a very positive review in Computing Reviews and have been incorporated in N. Sloane's superseeker at Bell Labs; tools for systems of multivariate linear operators (the *Mgfun* package), including Gröbner bases in Ore algebras, that also treat commutative polynomials and have been the standard way to solve polynomial systems in Maple for a long period (although the user would not notice it); *Mgfun* has also been chosen at Risc (Linz) as the basis for their package Desing.

We also provide access to our work to scientists who are not using Maple or any other computer algebra system in the form of automatically generated encyclopedias available on the web. The Encyclopedia of Combinatorial Structures thus contains more than 1000 combinatorial structures for which generating functions, enumeration sequences, recurrences and asymptotic approximations have been computed automatically. It gets more than 16,000 hits per month. The Encyclopedia of Special Functions gathers around 40 special functions for which identities, power series, asymptotic expansions, graphs,... have been generated automatically, starting from a linear differential equation and its initial conditions. The underlying algorithms and implementations are those of *gfun* and *Mgfun*. All the production process being automated, the difficult and expensive step of checking each formula individually is suppressed. Available on the web (http://algo.inria.fr/esf/), this encyclopedia also plays the role of a showcase for part of the packages developed in our project. It gets 27,000 hits per month. A revision of this encyclopedia with added interactivity is under way in the framework of the DDMF project at the Microsoft Research – Inria Joint Centre. A prototype is available at http://ddmf.msr-inria.inria.fr.

A new package, *MultiSeries* has been developed recently. It implements so-called multi-series, that are series in general asymptotic scales, each of whose coefficient is itself potentially a new series. This makes it possible to handle in a transparent and dynamic way the problems of finding the proper asymptotic scale for an expansion and of dealing with the indefinite cancellation problem. This package is designed in such a way that it can take the place of the existing *series*, *asympt* and *limit* Maple functions, in a totally transparent manner.

5. New Results

5.1. Analysis of algorithms

Participants: Nicolas Broutin, Brigitte Chauvin, Frédéric Chyzak, Philippe Flajolet, Bruno Salvy.

The reference book on analytic combinatorics [21], by Flajolet and Sedgewick, which counts 825 pages, has been completed in the second half of the year 2008; it is now in press (a free web edition is available) and is published by Cambridge University Press. Its aim is to provide a broad and accessible coverage of the interactions between discrete and continuous mathematics, in the perspective of detailed analyses of combinatorial models, as may be present in the applied sciences as well as in analysis of algorithms. The core theory of analytic combinatorics, as presented in [21], is making advances along three major axes: (i) symbolic methods; (ii) complex asymptotics; (iii) random structures and probabilities. Part (i) addresses the issue of setting up equations that automatically translate a given combinatorial-probabilistic model. Part (ii) develops general-purpose methods for extracting asymptotics on coefficients of generating functions, a task best placed within the framework of complex analysis. Part (iii) is evolving in the direction of classifying the most important processes of combinatorics, in a way that often provides an attractive alternative to stochastic theory.

The article [18] by Flajolet and Huillet applies analytic combinatorics to study a simple model of the stochastic spread of influence in populations. The problem is to determine the stopping time of the process as well as the probability that unanimity of either type is eventually reached, when given a certain initial condition of the population. It belongs to the broad area of quantitative models of social networks, which is of some relevance in the analysis of networks.

In a joint work with Nicolas Pouyanne, a new family of distributions has been found, related to Pólya urns. They appear as martingale's limit distributions in the second term of the asymptotic expansion of a large two colors Pólya urn. The method consists in embedding the discrete urn in continuous time, getting thus a multitype branching process. Writing the dislocation equations for this process gives a system of differential equations on the Fourier transforms, or on the Laplace transforms of the limit distributions. It turns out that the Fourier transforms are explicitly related to Abelian integrals on a Fermat curve. Some properties of these limit distributions are explored: do they have moments of any order? Are they infinitely divisible? Are they stable? Are they determined by their moments? Do they have a density? Are the tails heavy or not? First results are presented in [25].

N. Broutin has worked on characterizing precisely the distances in various probabilistic models for data structures or networks. The distribution of distances in discrete structures crucially influences the performances of algorithms: tree-like data structures perform better when their keys are stored close to the root, graphs are easier to navigate when they have small diameter, and so on.

The behaviour of a random walk usually gives a good idea of the difficulty to navigate in a structure; random walks are also one of the important tools used to devise randomized algorithms. A famous correspondence allows one to reduce the study of random walks to that of electrical networks. In a joint work with L. Addario-Berry (Université de Montréal) and G. Lugosi (Pompeu Fabra, Barcelona), N. Broutin has characterized precisely the effective resistance of random trees [1]. The authors proved in particular that all moments are bounded, and that the effective resistance evolves like a traveling wave. This work is a first step towards dealing with more complex models of networks (graphs) and navigation (first-passage percolation).

Sparse subgraphs of the complete graph are usually a good model for networks. However, for some models that are computationally tractable, the distances between nodes are too large to be of any practical use. It is in this spirit that L. Addario-Berry N. Broutin and B. Reed (McGill University, CNRS) showed that the diameter of the minimum spanning tree of a complete graph is of order $\Theta(n^{1/3})$ [2]. On the other hand, in a weighted complete graph L. Addario-Berry, N. Broutin and G. Lugosi showed that even the longest minimum weight path is about $\alpha \log n$, for some computable constant α [22]. These two situations are the extreme cases of networks based weighted complete graphs, and further investigation is in order.

Uniform binary trees are one of the essential tree families that appear constantly in algorithms. They have mostly been studied when the model of randomness defines the nodes as distinguishable and/or ordered. However, applications to boolean formulae, where operations are commutative, suggest a model in which the nodes are neither ordered nor distinguishable. N. Broutin and P. Flajolet have found the limit distribution of the height of such random binary unlabelled trees [17] and hence confirmed the intuition that such trees behave essentially like uniform plane binary trees.

Radix-rational sequences are defined by recurrences which, in the simplest case of a binary base, relate u_n to u_{2n} and u_{2n+1}. They emerge in various areas of mathematics and computer science: combinatorics of words, numeration system, number theory, divide-and-conquer algorithms. Until now there did not exist a general theorem describing the possible asymptotic behaviours of such sequences and the work of P. Dumas [26] fills the gap.

In the article [9], finite differences of values of the Riemann zeta function at the integers are explored. Such quantities, which occur as coefficients in Newton series representations, have surfaced in earlier investigations surrounding Li's criterion for the Riemann hypothesis. They also arise in connection with the analysis of digital trees (earlier works of Clément, Flajolet, and Vallée), especially in the context of continued fraction representations of real numbers.

An important recent progress in the field of combinatorial random generation was the introduction of Boltzmann samplers by Flajolet *et alii* a few years ago. These samplers open the way to large discrete simulations, provided numerical values of appropriate generating functions can be computed. In [19], C. Pivoteau, B. Salvy and M. Soria showed how these values could be computed efficiently by a Newton iteration with the origin for initial point. The proof relies on a lifting of Newton iteration at the level of systems of combinatorial specifications. The corresponding program solves systems of hundreds of equations in a matter of seconds.

5.2. Computer Algebra

Participants: Alexandre Benoit, Alin Bostan, Frédéric Chyzak, Philippe Flajolet, Manuel Kauers, Nicolas Le Roux, Marc Mezzarobba, Bruno Salvy.

One of our main themes of research is the use of linear differential equations as a data structure for the automatic manipulation of special functions. This concerns various operations, including definite integration. In this vein, J. Borwein, and B. Salvy give a proof [4] of a conjecture on moments of powers of the Bessel function that had attracted the attention of mathematical physicists. Not only is the proof effective, but it gives an efficient derivation of formulas for the computations of these moments.

Newton iteration can be put to use in the context of power series of nonlinear differential equations. A. Bostan, F. Morain (project-team Tanc), B. Salvy, and É. Schost apply this idea in [6] to a problem in elliptic curve cryptography. They introduce an algorithm that computes a special rational morphism between two elliptic curves; its complexity is quasi-linear with respect to the degree of the morphism. The new algorithm allows to speed-up a crucial step of the Schoof-Elkies-Atkin algorithm for determining the cardinality of an elliptic curve over a finite field.

Composition of power series is a fundamental operation for which no quasi-optimal algorithm is known except for special cases. The class of special cases has been vastly extended by A. Bostan, B. Salvy, and É. Schost in [16]. They show that right composition with many series can be performed efficiently. This has for consequence a new algorithm for the efficient conversion of polynomials between various bases including the classical orthogonal polynomials. In the case of general formal orthogonal polynomials, different ideas are required and are developed in [24].

A characteristic feature of computer algebra systems is their ability to manipulate arbitrarily large integers by storing them over several machine words. By contrast, efficient computations modulo small prime numbers require skillful implementation combining several residues into one machine word. When considering matrices of such residues, several strategies are possible. These are compared from the theoretical and practical point of view by J.-G. Dumas, L. Fousse (Grenoble), and B. Salvy in [20], [27]. In all cases, the speedup expected in theory, governed by the number of residues that can fit into one word, is reached in practice.

One focus of our project-team is on the complexity analysis of fundamental operations in computer algebra. An operation that had not received sufficient attention is the product of linear differential operators with polynomial coefficients. In [15], A. Bostan, F. Chyzak, and N. Le Roux present an improved algorithm by reducing the number of matrix products involved. They show that matrix multiplication (in size $n \times n$) has essentially the same cost as the product of differential operators (of order n and polynomial coefficient degrees n) when the constants are rational numbers, while the product of operators has an essentially quadratic cost when computations are performed modulo a prime number.

A principal topic of the project-team is the symbolic computation of integrals involving special functions. In this framework, we expect more efficient algorithms provided we focus to more particular classes of inputs. In this spirit, S. Chen has started a PhD thesis in December 2007 under the codirection of F. Chyzak and Z. Li (Chinese Academy of Sciences, Beijing). His work is on the efficiency of the symbolic integration of rational functions, which covers many combinatorial applications.

Structured linear algebra techniques are versatile tools that allow to deal with various types of structured matrices, whether of Toeplitz, Hankel, Vandermonde or Cauchy type. Such linear systems are classically solved by means of a compact representation in $\widetilde{O}(\alpha^2 n)$ operations, where n is the matrix size and α is a measure of the structure that can grow with n. A. Bostan, C.-P. Jeannerod (project-team Arenaire), and É Schost showed in [5] that this cost can be reduced to $\widetilde{O}(\alpha^{\omega-1} n)$, with $\omega < 2.38$. The improvement is based on re-introducing fast dense linear algebra for operations on a compact representation of the given matrix. This makes efficient Hermite-Padé approximation and efficient interpolation of bivariate polynomials possible.

The algorithmic advances on power series manipulation over the last decade (computation of high order expansions, Hermite-Padé approximation, ...) have been used by A. Bostan and M. Kauers in tackling a notorious combinatorial conjecture. Their experimental mathematics approach in [23] led to the computer-aided discovery of structural properties of enumerating functions for walks. They have systematically searched for differential and algebraic equations that the series counting the number of walks in the quarter plane satisfy. They have also made a first step towards classifying walks in the first octant of space by considering all step sets with up to five elements, and performed a systematic search for equations of the corresponding series.

M. Mezzarobba's PhD thesis is about basic algorithms operating on D-finite functions, with a special focus on numerical evaluation. With B. Salvy, he developped algorithms to compute tight bounds on P-recursive sequences and D-finite functions. A preliminary implementation of those algorithms in Maple is available in the NumGfun package available from http://algo.inria.fr/mezzarobba/NumGfun-0.2.tgz.

In his master thesis [28], A. Benoit gave a new algorithm for computing the recurrence of coefficients in a Chebyshev expansion. His algorithm computes the recurrence in a provably and practically more efficient way than previously-known algorithms. He has implemented his algorithm in the computer algebra system Maple.

Part of the activity of the project-team Algorithms is in the project "Dynamic Dictionary of Mathematical Functions" of the Microsoft Research – INRIA Joint Centre. This aims at a new version of the "Encyclopedia of Special Functions" developed in the past by L. Meunier within the project-team (http://algo.inria.fr/esf), with the goal of added interactivity. For instance, a user on the web will be able to request more terms of an asymptotic expansion, or improved approximation formulas, which requires incremental symbolic computations. To this end, F. Chyzak is developing a system DynaMoW dedicated to the presentation of interactive mathematics on the web. Its essential feature is to control simultaneously the production of displayed documents and symbolic calculations in possibly concurrent computer-algebra sessions. A prototype is available at http://ddmf.msr-inria.inria.fr. In the future, the "Encyclopedia of Combinatorial Structures", also a production of the team, will receive the same kind of extensions.

6. Contracts and Grants with Industry

6.1. Industrial Contracts

The Algorithms Project and Waterloo Maple Inc. (WMI) have collaborated for many years based on reciprocal interests. Thanks to this collaboration, the company WMI considers INRIA as a special partner and grants it a free license for all of its research units.

Our work on automating the derivation of formulæ for special functions is hosted and funded for 3 years (2007–2010) by the joint Inria-Microsoft Research Lab. as one of its projects, called "Dynamic Dictionary of Mathematical Functions".

7. Other Grants and Activities

7.1. National Actions

Alea is a national working group dedicated to the analysis of algorithms and random combinatorial structures. It is a meeting place for mathematicians and computer scientists working in the area of discrete models. It is currently supported by CNRS (GDR A.L.P.) and is globally animated by Philippe Flajolet. In March 2008, the yearly meeting (organized by Philippe Duchon and Jean-François Marckert, Bordeaux) has gathered in Luminy over 80 participants from about 20 different research laboratories throughout France.

From 2005 to 2008, a project called FLUX and involving the RAP project at INRIA as well as the University of Montpellier has been funded by the national action ACI-MD relative to massive data: our objective is to develop high performance algorithms for the quantitative analysis of massive data flows an important problem in the monitoring of high speed computer networks.

For the period 2006–2009, the Algo project participates in a programme funded by the National Research Agency (ANR) entitled GECKO for “A Geometric Approach to Complexity and its Applications". Four teams are involved: ALGO (coordinator) and teams at the École polytechnique, the Universities of Toulouse and Nice. The project concentrates on three classes of objects: (i) univariate and multivariate polynomials (Newton process, factorization, elimination); (ii) structured matrices (whose coefficients can be polynomials); (iii) linear differential operators (noncommutative elimination, integration). The aim is to improve significantly the resolution of systems of algebraic or linear differential equations that appear in models, by taking geometry into account.

The National Research Agency (ANR) is also funding a research project entitled SADA, whose goal is to investigate fundamental properties of random discrete structures and algorithms. The project duration is 3.5 years (Dec. 2005–June 2009). It involves five teams: ALGO/RAP from INRIA Rocquencourt, the Universities of Caen, Versailles, and Bordeaux (coordinator), as well as the Laboratory for Computer Science of the École polytechnique (LIX).

8. Dissemination

8.1. Animation

The ALGO project runs a biweekly seminar devoted to the analysis of algorithms and related topics. Several partner teams in the grand Paris area attend on a regular basis, and also take part in a yearly workshop, Alea.

Brigitte Chauvin has been a co-organizer of the "Colloquium for Philippe Flajolet’s 60th Birthday". This conference brought together approximately 220 participants at ENS Paris in December. She has participated to the Fifth Colloquium on Mathematics and Computer Science, Algorithms, Trees, Combinatorics and Probabilities, on September 22-26, 2008, in Blaubeuren, Germany. She has been a member of the program committee. She has been a member of thesis jurys for Lucas Gerin, PhD, U. Nancy, *"Aspects probabilistes des automates cellulaires"* and Jean-Maxime Labarbe, PhD , U. Versailles *"Marches alatoires, martingales et arbres m-aires de recherche"*.

Frédéric Chyzak has been a co-organizer of the 2008 edition of the French national meeting in computer algebra (JNCF’08), that has gathered some 80 participants in Luminy. He is a member of the recruiting committee of Univ. Limoges, in mathematics.

Philippe Flajolet is an editor of the journal *Random Structures and Algorithms*, an honorary editor of *Theoretical Computer Science*, and an honour member of the French association SPECIF. He also serves as one of the three editors of Cambridge University Press’ prestigious series *Encyclopedia of Mathematics and its Applications*.

He serves as Chair of the Steering Committee of the international series of Conferences and Workshops called *Analysis of Algorithms*. The yearly edition attracts some 80 specialists of the area. He serves in a similar capacity as founder and chair of the French Working Group Alea supported by the GDR-IM [mathematical informatics] of CNRS: the yearly meetings are held at Luminy near Marseilles, and the participation nears 80 every year.

Philippe Flajolet is also an external member of the Recruiting Committee for computer science at the École polytechnique. He is a member of the board of experts for the Canada Research Chairs. In 2008, he has been a member of several jurys: Joris van der Hoeven (Hab., U. Paris Sud; computer algebra); Roland Bacher (referee, Hab., U. Grenoble; discrete mathematics); Philippe Duchon (referee; Hab., U. Bordeaux; combinatorics); Vlady Ravelomanana (referee; Hab.; U. Paris Nord; analysis of algorithms); Carine Pivoteau (PhD; U. Paris 6; random generation); Jose Ramon Sanchez (referee; PhD; U of Madrid; data structures). He has also served as chair of the evaluation committee of the LIPN and L2Ti Laboratories (University Paris Nord).

Bruno Salvy has been on the program committee of the conference "Formal Power Series and Algebraic Combinatorics", Valparaiso, Chile, 2008 and he is on the program committee for next year's ISSAC, Seoul, Korea. He is organizing the working group Computer Algebra of the CNRS GDR IM ("Mathematical Informatics"). He is a member of the editorial board of the Journal of Symbolic Computation and of the Journal of Algebra (section Computational Algebra).

This year, he was a co-organizer of the Gecko-Tera'08 week in École polytechnique and of the 2-day long Colloquium for Philippe Flajolet's 60th birthday at École normale supérieure. He has also been a referee for the PhD dissertation of Cl. Durvye (U. Versailles), and a member of the PhD committee of C. Pivoteau (U. Paris 6).

8.2. Teaching

Alin Bostan, *Frédéric Chyzak*, and *Bruno Salvy* have set up and taught a 48h course in computer algebra together with Marc Giusti (from École polytechnique). This course is part of the *Master Parisien de Recherche en Informatique* (MPRI).

Alin Bostan and *Bruno Salvy* have also set up and taught a 48h course at the *École Normale Supérieure* on computer algebra oriented towards experimental mathematics.

Frédéric Chyzak teaches a course in computer algebra as a *chargé d'enseignement à temps incomplet* at École polytechnique.

Philippe Flajolet has given a 12 hour course at the Parisian Master of Research in Computer Science (MPRI), on the analysis of algorithms.

Bruno Salvy has also given an introduction to asymptotic analysis for the analysis of algorithms as a mini-course at the conference AofA'08 (Analysis of Algorithms, Maresias, Brasil).

8.3. Participation in conferences, seminars, invitations

Alin Bostan, has been invited for two weeks (April 2008) at the Symbolic Computation Laboratory in the Computer Science Department at the University of Western Ontario, where he collaborated with Éric Schost on differential equations in positive characteristic.

Frédéric Chyzak has presented his joint work [15] with Alin Bostan and Nicolas Le Roux at the conference ISSAC'08 (Hagenberg, Austria), July 2008. Alin Bostan and Bruno Salvy's joint work with Éric Schost [16] has also been presented there.

Alin Bostan gave a talk entitled "The full counting function of Gessel walks is algebraic", in November 2008 in Palaiseau, for the yearly workshop of the Gecko project of the ANR.

Nicolas Broutin has presented the results of [17] at the fifth colloquium on mathematics and computer science that took place in Blaubeuren in September. He was invited to participate to the workshop on probabilistic combinatoris in Bellairs institute, Barbados. He gave a talk at the conference in Bordeaux organized on the occasion of D. Knuth's honorary degree. He has also given invited lectures in the universities of Caen, Nancy, Paris 6 and 7, Frankfurt and Oxford and at École Polytechnique. He is currently organizing with L. Addario-Berry, L. Devroye and B. Reed the workshop on probabilistic combinatorics that will be held in Bellairs institute next march. He also organizes a week long workshop on "branching random walks and searching in trees" with L. Addario-Berry, L. Devroye and C. McDiarmid; the workshop will take place at the BIRS in Banff, Canada in February 2010.

Brigitte Chauvin has given a talk "What kind of laws come from urns?", joint work with N. Pouyanne, at the Colloquium for Philippe Flajolet's 60th birthday.

Frédéric Chyzak has presented preliminary work joint with A. Bostan and B. Salvy (of the project-team), and Z. Li (Academy of Mathematics and System Sciences, Beijing) at the University of Rennes and at the team's seminar. Expected results are fast algorithms for the computation of least common multiples of linear differential and difference operators. He has presented the work [15] joint with A. Bostan and N. Le Roux at the international conference ISSAC'08 (Linz, Austria) and at the yearly workshop of the Gecko project of the ANR. He presented the prototype of the Dynamic Dictionary of Mathematical Functions on several occasions at the joint Microsoft Research – INRIA Centre.

Philippe Flajolet has been an invited plenary speaker at the *Foundations of Computational Mathematics* conference (FoCM'08, Hong Kong). He has been invited to give the Fields Lecture at Carleton University Ottawa (February 2008). He has given a seminar on Algorithmics and Quantitative Data Mining within Pr. G. Berry's Chair (Technological Innovation) at Collège de France. He has given talks at the International Workshop on Analysis of Algorithms (Maresias, Brazil), the ALÉA Metting (CIRM, Marseilles), the Mathematics and Computer Science Colloquium (Blaubeuren, Germany), the Algorithms Day (Warwick, U.K.). He has been invited for one week of research on combinatorial models of statistical physics at the Mathematisches Forschungsinstitut Oberwolfach (within the framework of the Leibniz Fellowship Programme). He has given colloquium talks at the mathematics department of the University of Toulouse, the Institut de Physique Théorique (IPhT), Saclay, and the FREMIT (mathematics and computer science) meeting in Toulouse. He has finally given an invited talk at the Combinatorics Day at The Queen Mary University, London, U.K.

M. Mezzarobba visited Éric Schost (University of Western Ontario, London, Ontario, Canada) for one month. There, he collaborated on the automatic computation of the bilinear complexity of common operations. On several occasions, he gave talks on the work he has conducted during and since his master's internship on the high-precision numerical evaluation of D-finite functions and on the computation of tight bounds for P-recursive sequences: at the workshops "Algorithmes pour les équations différentielles et aux différences" (Limoges) and RAIM 2008 (Lille), and at the internal seminars of several research teams (UWO, London, ON; Cacao, Nancy; Arénaire, Lyon).

Bruno Salvy has given a talk on D-finiteness at the workshop on "Combinatorics and Statistical Physics" of the Schrödinger Institute (Vienna, Austria), a talk on [16] and [24] at the Algorithms Seminar, talks on [19] at the Gecko/Tera08 conference and at the Colloquium for Philippe Flajolet's 60th birthday.

8.4. Foreign Visitors

A large number of our visitors have given talks at the seminar of the project. This year, we received: Mihyun Kang, Humboldt-Universität zu Berlin, Institut für Informatik, Germany; P. Blasiak, Institute of Nuclear Physics, Polish Academy of Sciences, Krakow, Poland; Peter Paule, RISC, Johanes Kepler University, Linz, Austria; Marni Mishna, Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada; Wojciech Szpankowski, Department of Computer Science, Purdue University, West Lafayette, Indiana, USA; François Bergeron, Quebec University, Montreal, Canada; Stefan Gerhold, Financial and Actuarial Mathematics, Vienna University of Technology, Vienna, Austria; Christoph Koutschan, RISC, Johanes Kepler University, Linz, Austria; Sergei Abramov, Dorodnicyn Computing Centre of the Russian Academy of Sciences, Moscow, Russia.

9. Bibliography

Year Publications

Articles in International Peer-Reviewed Journal

[1] L. ADDARIO-BERRY, N. BROUTIN, G. LUGOSI. *Effective resistance of random trees*, in "The Annals of Applied Probability", To appear, 2008.

[2] L. ADDARIO-BERRY, N. BROUTIN, B. REED. *Critical random graphs and the structure of a minimum spanning tree*, in "Random Structures Algorithms", To appear, 2008.

[3] G. BOLDINA, A. IVASHCHENKO, M. RÉGNIER. *Using Profiles Based on Nucleotide Hydrophobicity to Define Essential Regions for Splicing*, in "International Journal of Biological Sciences", vol. 5, n^{o} 1, 2009, 13â19, http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2597731.

[4] J. M. BORWEIN, B. SALVY. *A proof of a recursion for Bessel moments*, in "Experimental Mathematics", arXiv:0706.1409, vol. 17, n^{o} 2, 2008, p. 223–230.

[5] A. BOSTAN, C.-P. JEANNEROD, É. SCHOST. *Solving structured linear systems with large displacement rank*, in "Theoretical Computer Science", vol. 407, n^{o} 1-3, 2008, p. 155–181.

[6] A. BOSTAN, F. MORAIN, B. SALVY, É. SCHOST. *Fast algorithms for computing isogenies between elliptic curves*, in "Mathematics of Computation", arXiv:0609020, vol. 77, n^{o} 263, July 2008, p. 1755–1778.

[7] G. CHAPUY, É. FUSY, M. KANG, B. SHOILEKOVA. *A Complete Grammar for Decomposing a Family of Graphs into 3-connected Components*, in "Electronic journal of combinatorics", vol. 15, n^{o} 1, December 2008, R148, http://www.combinatorics.org/Volume_15/PDF/v15i1r148.pdf.

[8] F. CHYZAK, M. DRMOTA, T. KLAUSNER, G. KOK. *The distribution of patterns in random trees*, in "Combinatorics, Probability & Computing", vol. 17, 2008, p. 21–59.

[9] P. FLAJOLET, L. VEPSTAS. *On Differences of Zeta Values*, in "Journal of Computational and Applied Mathematics", vol. 220, n^{o} 1–2, 2008, p. 58–73.

[10] É. FUSY. *Uniform random sampling of planar graphs in linear time*, in "Random Structures & Algorithms", To appear.

[11] É. FUSY. *Transversal structures on triangulations: combinatorial study and straight-line drawing*, in "Discrete Mathematics", In press. Available online March 2008., 2008, http://www.sciencedirect.com/science.

[12] É. FUSY, D. POULALHON, G. SCHAEFFER. *Dissections, orientations, and trees, with applications to optimal mesh encoding and to random sampling*, in "Transactions on Algorithms", vol. 4, n^{o} 2, April 2008.

[13] F. MEUNIER. *A combinatorial proof of a theorem of Freund*, in "Journal of Combinatorial Theory, Series A", vol. 115, n^{o} 2, 2008, p. 317–325.

Articles in National Peer-Reviewed Journal

[14] C. GOMEZ, B. SALVY. *Calcul Formel*, in "Les Techniques de l'Ingénieur", vol. Dossier AF1460, 2008, p. 1–20.

International Peer-Reviewed Conference/Proceedings

[15] A. BOSTAN, F. CHYZAK, N. LE ROUX. *Products of Ordinary Differential Operators by Evaluation and Interpolation*, in "ISSAC'08 (July 20-23, 2008, Hagenberg, Austria)", Conference proceedings. Available as arXiv:0804.2181, ACM, 2008, p. 23–30.

[16] A. BOSTAN, B. SALVY, É. SCHOST. *Power Series Composition and Change of Basis*, in "ISSAC'08: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation", D. J. JEFFREY (editor), ACM Press, 2008, p. 269–276.

[17] N. BROUTIN, P. FLAJOLET. *The height of random binary unlabelled trees*, in "Fifth Colloquium on Mathematics and Computer Science", DMTCS Proceedings, vol. AI, 2008, p. 121–134.

[18] P. FLAJOLET, T. HUILLET. *Analytic Combinatorics of the Mabinogion Urn*, in "Proceedings of Fifth Colloquium on Mathematics and Computer Science: Algorithms, Trees, Combinatorics and Probabilities", U. RÖSLER (editor), Discrete Mathematics and Theoretical Computer Science Proceedings, vol. AI, 2008, p. 549–572.

[19] C. PIVOTEAU, B. SALVY, M. SORIA. *Boltzmann Oracle for Combinatorial Systems*, in "Algorithms, Trees, Combinatorics and Probabilities", Proceedings of the Fifth Colloquium on Mathematics and Computer Science. Blaubeuren, Germany. September 22-26, 2008, Discrete Mathematics and Theoretical Computer Science, 2008, p. 475–488.

Workshops without Proceedings

[20] J.-G. DUMAS, L. FOUSSE, B. SALVY. *Compressed Modular Matrix Multiplication*, in "Milestones in Computer Algebra (MICA 2008)", M. MORENO MAZA, S. M. WATT (editors), Proceedings of a conference in honour of Keith Geddes' 60th birthday. Stonehaven Bay, Trinidad and Tobago, 1-3 May 2008. Available as arXiv:0803.1975, May 2008.

Scientific Books (or Scientific Book chapters)

[21] P. FLAJOLET, R. SEDGEWICK. *Analytic Combinatorics*, In press; 825 pages (ISBN-13: 9780521898065); also available electronically from the authors' home pages., Cambridge University Press, 2008.

Research Reports

[22] L. ADDARIO-BERRY, N. BROUTIN, G. LUGOSI. *The longest minimum weight path in a complete graph*, Technical report, arXiv:0809.0275 [math.PR], submitted, 2008.

[23] A. BOSTAN, M. KAUERS. *Automatic classification of restricted lattice walks*, Technical report, arXiv:0811.2899, 2008.

[24] A. BOSTAN, B. SALVY, É. SCHOST. *Fast conversion algorithms for orthogonal polynomials*, Technical report, also available as arXiv:0804.2373, 2008.

[25] B. CHAUVIN, N. POUYANNE. *What kind of laws come from urns?*, Technical report, University of Versailles, 2008, http://www.math.uvsq.fr/~chauvin/compactpolyapf60.pdf.

[26] P. DUMAS. *Mean asymptotic behaviour of radix-rational sequences and dilation equations (Extended version)*, Technical report, arXiv:0807.1523, 2008.

[27] J.-G. DUMAS, L. FOUSSE, B. SALVY. *Simultaneous Modular Reduction and Kronecker Substitution for Small Finite Fields*, Technical report, arXiv:0809.0063, 2008.

Other Publications

[28] A. BENOIT. *Développements de fonctions D-finies sur des polynômes de Tchebychev*, Masters thesis, Université Paris VI-MPRI (Mastère 2), September 2008, http://www.msr-inria.inria.fr/~benoit/rapport.pdf.