INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Algorithms

Algorithms

Paris - Rocquencourt

Theme : Algorithms, Certification, and Cryptography

Activity Report

2009

Table of contents

1. Team

Research Scientist
Philippe Flajolet [Team Leader, Research Director, Inria, HdR]
Bruno Salvy [Research Director, Inria]
Alin Bostan [Research Associate, Inria]
Nicolas Broutin [Research Associate, Inria]
Frédéric Chyzak [Research Associate, Inria]

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

PhD Student
Alexandre Benoit [École polytechnique]
Shaoshi Chen [Co-direction with the Chinese Academy of Sciences, China]
Jérémie Lumbroso [Université Paris 6, starting October]
Marc Mezzarobba [ENS Paris]

Post-Doctoral Fellow
Thomas Feierl [starting December]
Stefan Gerhold [Vienna University of Technology, Austria, from February to July]

Visiting Scientist
Manuel Lladser [Grant NSF, University of Colorado, USA, June]
Helmut Prodinger [Stellenbosch University South Africa, from May to June]
Dana Louigi Addario-Berry [University of Montréal, Québec, Canada, from September to October]

Administrative Assistant
Virginie Collette [(AI) Inria]

Other
Pratik Poddar [IIT Bombay, India, from May to July]
Ayla Gafni [Vanderbilt University, USA, Grant NSF, from mid-April to June]
Lucien Pech [ENS Paris, starting September]
Jérémie Lumbroso [Université Paris 6, from March to September]

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

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

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, Jérémie Lumbroso, Bruno Salvy.

Analytic combinatorics serves as a basis for the quantification of properties of a large number of discrete models of computer science and developing its general theory has been an important effort of the ALGORITHMS Project.

The reference book on analytic combinatorics [21], by Flajolet and Sedgewick, which counts 824 pages, has been published by Cambridge University Press in 2009. (By special agreement with the publisher, an entirely free web edition is available from the authors' home pages.) The aim of the book 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.

A combinatorial work [29] by R. Bacher (UJF, Grenoble) and P. Flajolet elucidates the properties of pseudo-factorials and relates them to elliptic functions as well as to a new family of continued fractions and orthogonal polynomials. This could be achieved thanks to ideas coming both from special function theory and from computer algebra (see the next subsection). Another study by P. Flajolet, S. Gerhold (T.U. Vienna, Austria), and B. Salvy [13] provides criteria to help categorize the structural complexity —technically, the (non)holonomic character— of many generating functions of combinatorial interest. Dually, A. Bostan and M. Kauers have developed powerful computer algebra techniques that can be put to use to solve hard conjectures in lattice path enumeration. All these works provide a bridge between combinatorial theory and computer algebra (see also below), which are two pillars of the ALGORITHMS Project. A new postdoctoral fellow, Thomas Feierl (U. of Vienna, Austria), has arrived in December 2009, with a work programme dedicated to related combinatorial questions.

Trees are ubiquitous in computer science, as data structures for fast retrieval of information, as representations of structured objects and models, as substructures in combinatorial optimization problems, and as basic objects of symbolic computation. Understanding the properties of **random trees** serves to analyse and optimize fundamental algorithms in all these contexts.

In the area of random trees, a recent article of Bóna (U. Florida, USA) and Flajolet [31] elucidates many probabilistic properties of isomorphism and symmetries in non-plane binary trees, which arise from classification theory and the study of phylogenetic trees. This, together with earlier results of Broutin and Flajolet (2008) relative to height, confirms that non-plane ("unordered") trees have properties similar to their classical counterparts; for instance, they exhibit the same critical exponents.

Search algorithms are considered by N. Broutin and L. Addario-Berry with the purpose of assessing the performance of simple heuristics for optimization problems in random trees. The authors have quantified the performance of a simple algorithm exploring only subtrees with high potential by giving the moments of the size of the explored portion of the tree (hence, the search time) as well as bounds on the sub-optimal value returned.

The connections between search trees and continuous fragmentation processes are currently investigated by N. Broutin, B. Chauvin and J. Berestycki (Paris 6). In particular, they show that the limit distributions appearing in the fragmentation process studied by Janson and Neininger is the same as the one which appears in the asymptotics of the composition vector of m-ary search trees. This correspondence is understood thanks to the additive martingales associated with branching random walks and fragmentations. A key rôle is played by different stopping lines on the underlying tree.

Tree-like objects have also been used in more complex random structures. L. Addario-Berry (McGill, Canada), N. Broutin and C. Goldschmidt (Warwick, UK) have initiated a long term project on the metric properties of networks, including the celebrated example of Erdős–Rényi random graphs. They identified the scaling limit of typical sparse random graphs [28], [27] in terms of certain spanning trees of the graph, which are easily described as modifications of *simply generated trees* and hence relate to previous work of P. Flajolet.

P. Cenac (Dijon), B. Chauvin, F. Paccaut (Amiens) and N. Pouyanne (Versailles) analyse the suffix trie associated with a sequence generated by a Markov chain on left-infinite words and transition depending on an unbounded number of the preceding letters. In other words, a "context tree" gives the chain. The study relies on the analysis of the Markov chain using an associated dynamical system of a non classical type. Necessary and sufficient condition for the existence of a stationary measure are obtained. The time of appearance of patterns —an essential parameter for quantifying depths in the suffix trie— is related to a gambler-type martingale.

B. Chauvin collaborates with N. Pouyanne (Versailles) on asymptotic properties of **Pólya urns**. For a two-color Pólya urn, the limit distribution of the asymptotic composition of the urn is determined, in the non-Gaussian case, i.e. for so called "large" urns. The key method is the embedding into continuous time, which gives a multitype branching process and the related martingales. A differential system is solved, and the Fourier transform of the limit distribution is given by the inverse function of an explicit Abelian integral —this provides a nice probabilistic parallel to combinatorial results obtained earlier within the ALGORITHMS Project. The limit law is shown to admit a density; it is infinitely divisible and self-decomposable. However, the determination by the moments and the exact tails are still open questions [32]. In the case of m-ary search trees, $m \geq 27$, the same method (as for two-color Pólya urns) provides a system of fixed-point equations, but this system cannot be explicitly solved. Nevertheless, the limiting distribution is uniquely determined by a fixed point equation, and its Fourier transform is the unique solution of an integral equation. Once more, the limit law is proved to be infinitely divisible and self-decomposable.

Finally, several of our analytically oriented researches have impact on the **design and optimization of algorithms**.

The general theory of **random generation** as well as the simulation of discrete combinatorial and probabilistic models is a recurrent theme of ALGORITHMS. A study [34] conducted by P. Flajolet in collaboration with M. Soria and M. Pelletier (LIP6, Paris) provides new efficient algorithms for the simulation of Poisson and logarithmic distributions. A perhaps spectacular consequence of this new general theory of "Buffon machines and numbers" is the possibility of devising a Buffon-like experiment that produces a Bernoulli random variable with probability $1/\pi$, using less than six coin-flips on average.

In the area of **analysis of algorithms** *per se*, a collaboration with a team from Hong-Kong (M. Golin *et al.*, HKUST) has led to the solution in [18] of a class of divide-and-conquer recurrences, which reveals some hidden fractal behaviour. Such phenomena are shown to occur in priority-queue data structures (binomial queues) as well as in some problems of computational geometry (extrema finding). Following a trend started by B. Vallée (University of Caen) and J. Fill (Johns Hopkins University, USA), Clément, Fill, Flajolet, and Vallée [20] have recently provided analyses of the highly classical QuickSort and QuickSelect algorithms, under very general and realistic data models ("information sources"), which have the merit of taking into account all elementary operations involved in the management of complex data.

Recent developments in **statistics** have tried to rely on combinatorial ideas in order to improve detection thresholds for signals in the presence of noise. One reduces detection to testing randomly weighted graphs to decide whether all the edges are identically distributed or if some of them, forming a specific structure (path, cycle, clique, etc), have a biased mean. In a collaboration with L. Addario-Berry, L. Devroye (McGill, Canada) and G. Lugosi (Pompeu Fabra, Spain), N. Broutin has studied the detection thresholds for a large class of combinatorial structures and devised general principles to classify the feasibility of detecting procedures [26].

In the past, the ALGORITHMS team has invented several original and high-performance methods for performing **quantitative data-mining** tasks (e.g., works of Durand, Flajolet, Fusy, Giroire, Meunier, relative to the cardinality problem). This year, Jérémie Lumbroso has completed a Master's Thesis, where he analyses precisely what turns out to be an optimal algorithm within the whole category of order-statistics methods. He is currently starting a thesis under the joint responsibility of M. Soria (LIP6) and P. Flajolet.

5.2. Computer Algebra

Participants: Alexandre Benoit, Alin Bostan, Frédéric Chyzak, Philippe Flajolet, Stefan Gerhold, Manuel Kauers, Marc Mezzarobba, Lucien Pech, Pratik Poddar, Bruno Salvy.

The originality of our work in computer algebra lies in the systematic use of linear operators as a data-structure from which various information such as identities for special functions can be extracted. Our work proceeds along three lines: design of fast algorithms either based on using linear operators or giving better complexity for operations on these operators; new algorithmic applications of linear operators; new algorithms extending the class of functions to which our methods apply.

New effectivity results. A very important result this year is in [19], where we extend Zeilberger's approach to special function identities to cases that are not holonomic. The method of creative telescoping is thus applied to definite sums or integrals involving Stirling or Bernoulli numbers, incomplete Gamma function or polylogarithms, which are not covered by the holonomic framework. The basic idea is to take into account the dimension of appropriate ideals in Ore algebras. This unifies several earlier extensions and provides algorithms for summation and integration in classes that had not been accessible to computer algebra before.

The classification of possible asymptotic behaviours of solutions of linear differential equations is classical. Together with a Lindelöf integral representation, this is used in [13] to study various sequences that possess explicit analytic expressions. One of the outcomes of such analyses concerns the non-existence of linear recurrences with polynomial coefficients annihilating these sequences, and, accordingly, the non-existence of linear differential equations with polynomial coefficients annihilating their generating functions. In particular, the corresponding generating functions are transcendental. Asymptotics of certain finite difference sequences come out as a byproduct of our approach.

In [14], we describe an algorithm that takes as input a complex sequence given by a linear recurrence relation with polynomial coefficients along with initial values, and outputs a simple explicit upper bound on its modulus, valid for all values of the index. Generically, the bound is tight, in the sense that its asymptotic behaviour matches that of the bounded sequence. We discuss applications to the evaluation of power series with guaranteed precision.

A Chebyshev expansion is a series in the basis of Chebyshev polynomials of the first kind. When such a series solves a linear differential equation, its coefficients satisfy a linear recurrence equation. In [15], we interpret this equation as the numerator of a fraction of linear recurrence operators. This interpretation lets us give a simple view of previous algorithms, analyze their complexity, and design a faster one for large orders.

Applications. Our two major domains of applications are combinatorics and theoretical physics.

In [16], we propose an experimental mathematics approach leading to the computer-driven discovery of various conjectures about structural properties of generating functions coming from enumeration of 2D and 3D lattice walks.

Gessel walks are lattice walks in the quarter plane $\mathbb{N}^2$ which start at the origin and consist only of steps chosen from the set $\{\longleftarrow, \swarrow, \nearrow, \rightarrow\}$. In [24], we prove that the number of Gessel walks of given length ending at any given point has a trivariate generating series that is an algebraic function. This is a solution to an extension of a famous conjecture due to Gessel.

In [4], we consider the Fuchsian linear differential equation obtained (modulo a prime) for the five-particle contribution to the susceptibility of the square lattice Ising model. We show that one can understand the factorization of the corresponding linear differential operator from calculations using just a single prime. A particular linear combination of the 1-particle and 3-particle contributions can be removed and the resulting series is annihilated by a high order globally nilpotent linear ODE. The corresponding (minimal order) linear differential operator, of order 29, splits into factors of small orders. A fifth order linear differential operator occurs as the left-most factor of the "depleted" differential operator and it is shown to be equivalent to the symmetric fourth power of the linear differential operator corresponding to the elliptic integral. This result generalizes what we have found for the lower order terms of the 3-particle and 4-particle cases. We conjecture that a linear differential operator equivalent to a symmetric power of this operator occurs as a left-most factor in the minimal order linear differential operators for all n-particle cases.

In [5], we recall various multiple integrals related to the isotropic square Ising model, and corresponding, respectively, to the n-particle contributions of the magnetic susceptibility, to the (lattice) form factors, to the two-point correlation functions and to their lambda-extensions. These integrals are holonomic and even G-functions: they satisfy Fuchsian linear differential equations with polynomial coefficients and have some arithmetic properties. We recall the explicit forms, found in previous work, of these Fuchsian equations. These differential operators are very selected Fuchsian linear differential operators, and their remarkable properties have a deep geometrical origin: they are all globally nilpotent, or, sometimes, even have zero p-curvature. Focusing on the factorised parts of all these operators, we find out that the global nilpotence of the factors corresponds to a set of selected structures of algebraic geometry: elliptic curves, modular curves, and even a remarkable weight-1 modular form emerging in the three-particle contribution of the magnetic susceptibility of the square Ising model. In the case where we do not have G-functions, but Hamburger functions that correspond to the confluence of singularities in the scaling limit, the p-curvature is also found to verify new structures associated with simple deformations of the nilpotent property.

In relations to these studies, we give an example in [24] of an infinite order rational transformation that leaves a linear differential equation covariant. This example can be seen as a non-trivial but still simple illustration of an exact representation of the renormalization group.

Simple proofs of several results and conjectures formulated by Stolarsky and Tran concerning generating functions of some families of Chebyshev-like polynomials are given in [8].

Fast algorithms. An important special class of solutions of linear operators is given by orthogonal polynomials. In [7], we discuss efficient conversion algorithms. We describe a known conversion algorithm from an arbitrary orthogonal basis to the monomial basis, and deduce a new algorithm of the same complexity for the converse operation.

In [17], we address complexity issues for linear differential equations in positive characteristic p: resolution and computation of the p-curvature. For these tasks, our main focus is on algorithms whose complexity behaves well with respect to p. We prove bounds linear in p on the degree of polynomial solutions and propose algorithms for testing the existence of polynomial solutions in sublinear time, and for determining a whole basis of the solution space in quasi-linear time. We show that for equations of arbitrary order, the p-curvature can be computed in subquadratic time, and that this can be improved to logarithmic time for first order equations and to quasi-linear time for classes of second order equations.

The cost of multiplication modulo triangular families of polynomials is studied in [23]. Following previous work by Li, Moreno Maza and Schost, we propose an algorithm that relies on homotopy and fast evaluation-interpolation techniques. We obtain a quasi-linear time complexity for substantial families of examples, for which no such result was known before. Notably, applications are given to addition of algebraic numbers in small characteristic.

A relatively simple algorithm with a low constant factor for exponentials of truncated power series is given in [9].

Specific algorithms for creative telescoping are being developed. For rational functions, this is related to the classical Hermite reduction and was studied in [33], [30].

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 2009, the yearly meeting (organized by Jean Mairesse, Anne Micheli and Dominique Poulalhon) has gathered in Luminy over 80 participants from about 20 different research laboratories throughout France.
For the period 2006–2009, the Algorithms 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).
In September 2009, the Algorithms project has started a new participation in the programme funded by the National Research Agency (ANR) entitled BOOLE for "Quantifying Boolean Frameworks". Four teams are involved: ALGORITHMS from INRIA Paris–Rocquencourt, the Universities of Caen, Versailles (coordinator), and Provence Aix–Marseille 1; the project is for 4 years until August 2013.

8. Dissemination

8.1. Animation

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

Alin Bostan has been on the program committee of the workshop RAIM’09 (ENS Lyon, October 2009), and he is on the program committee for next year’s ISSAC conference, Munich, Germany.

Brigitte Chauvin has been a co-organizer of the "Colloquium for Alain Rouault’s 60th Birthday". This conference brought together approximately 80 participants at IHP Paris in April 2009. She has been a member of the program committee of the Conference Aofa 2009. Brigitte Chauvin has been a member of thesis jurys for Arno Siri-Jegousse, PhD, U. Paris 5, *“Étude des généalogies dans des modèles de génétique des populations”* and Florian Simatos, PhD , École polytechnique, *“Étude de modèles probabilistes de réseaux pair-à-pair et de réseaux avec mobilité”* and Rafik Aguech, Habilitation, U. Monastir (Tunisia). She is an associate editor of the Journal "Annals of Applied Probability”.

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 counts as one of the five 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 (co)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 has served in 2009 as member of the advisory council to the director general of CNRS, whose mission was to select candidates for the direction of the newly formed national institute in computer science (INSIS). He has also been a member of the special committee meant to determine, at a national level, the strategic directions for the years to come in the area of computing sciences ("sciences du numérique"). At INRIA, he has served as president of the jury that recruits researchers at the entry level (CR2/CR1). He has been also a member of the recruiting committee for computer science professors at LIP6 (University of Paris). As a follow up to his former presidency of the Mathematics Committee of the French National Research Agency (ANR) in 2005–2006, he has also served as president of a day session relative to mathematial sciences at the National Science Colloquium held at La Villette in February 2009. This year, he has been a member of the following thesis and habilitation jurys: Guillaume Chapuy at École Polytechnique (PhD, combinatorics of maps, June 2009), J. R. Sanchez-Couso at Universidad Complutense de Madrid (PhD, analysis of algorithms), Andrea Roeck at École polytechnique (PhD, cryptography, May 2009), Antonio Vera at the University of Caen (PhD, computational number theory, July 2009), Yousra Chabchoub at LIP6 (PhD, network management, December 2009).

Bruno Salvy has been on the program committee of the conference ISSAC'09, Seoul, Korea. He is organizing the working group Computer Algebra of the CNRS GDR IM. 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 has been a referee for the PhD dissertations of S. Chevillard (ENS Lyon) and T. Feierl (U. Vienna, Austria). He has also been a member of the selection committee hiring computer science professors in Bordeaux and of the committees hiring researchers at Inria (jurys d'admissibilité et d'admission CR).

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.

Nicolas Broutin has taught 9 hours on Analysis of Algorithms at the Parisian Master of Research in Computer Science (MPRI).

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

Philippe Flajolet has given an 18 hour master's course at the Parisian Master of Research in Computer Science (MPRI, 2nd year master level), on the analysis of algorithms. He has also taught a 6-hour postdoctoral research course at Luchon in January 2009 on analytic combinatorics and random discrete structures. He has also given a special 16 hours postdoctoral course at the Institut Henri Poincaré. within the framework of a special trimester dedicated to statistical physics and combinatorics.

8.3. Participation in conferences, seminars, invitations

Alin Bostan has been invited for two weeks (June 2009) at the Symbolic Computation Laboratory in the Computer Science Department at the University of Western Ontario, where he colaborated with Éric Schost on differential equations in positive characteristic.

Alin Bostan has presented his joint work [17] with Éric Schost at the conference ISSAC'09 (Seoul, Korea, July 2009). On several occasions, he gave talks on his joint works [16] and [24] with Manuel Kauers, at the workshop “Calcul algébrique et équations différentielles" (Limoges, March 24–25), and at the internal seminars of several research teams: “Calcul formel et complexité" (Rennes, January 30), “OCAD" (Paris 13, March 2), “SALSA" (Paris 6, May 29), “Algorithms" (Rocquencourt, June 8).

Nicolas Broutin has given talks at the ALEA meeting (CIRM, Marseille), the CRM workshop on Combinatorics Randomization, Algorithms and Probability (Montreal), the algorithms seminar at the Université Libre in Brussels and the probability seminar at Université Paul Sabatier in Toulouse. With L. Addario-Berry and B. Reed, he has organized the workshop on probabilistic aspects of combinatorics that was held in Bellairs Institute in march. He has also organized a week long workshop with L. Addario-Berry, L. Devroye and C. McDiarmid on the theme “branching random walks and searching in trees” that will be held in Banff next February. He has spent research periods with L. Addario-Berry, L. Devroye and B. Reed at the University of Montréal and McGill, P. Bose and S. Langermann at Université Libre in Brussels, C. Goldschmidt and C. McDiarmid at Oxford University, R. Neininger at W. Goethe University in Frankfurt, and C. Bordenave in Toulouse. He has participated to the weekly workgroup on random matrices and stochastic processes at LPMA, Paris VI and VII and to in the semester on Combinatorics, Probability and Statistical Physics at IHP. He also participated to the Combinatorics Days in Bordeaux and to the International Conference on Analysis of Algorithms.

Brigitte Chauvin has participated to the Workshop “Random trees” at Oberwolfach, Germany, on January; to the Workshop “Quantum and combinatorics”, at Zakopane (Poland), on November, to the conference AofA (Analysis of Algorithms) at Fréjus on June. She has given a seminar at Orsay in April and at Lyon, ENS in November.

Shaoshi Chen presented two posters on his research on fast algorithms for the definite integration of rational functions with Alin Bostan and Frédéric Chyzak (of the project-team) and Ziming Li (Academy of Mathematics and System Sciences, Beijing): at the conference ICMM'09 (Beijing, China), May 2009 [33] and at the conference ISSAC'09 (Seoul, South Korea), July 2009 [30]. He also gave a talk on the topic during an invited visit in RISC (Linz, Austria).

Frédéric Chyzak presented his joint work [19] on symbolic summation and integration of a larger class of special functions, obtained with Bruno Salvy (of the project-team) and Manuel Kauers (RISC, Linz, Austria)), at the conference ISSAC'09 (Seoul, South Korea), July 2009. He gave several talks on the Dynamic Dictionary of Mathematical Functions developped at the Microsoft Research – INRIA Joint Centre at the Groupe de Travail Programmation (Université Paris 6) and on several other occasions.

Philippe Flajolet has been an invited plenary speaker at the Conference *Orthogonal Polynomials, Special Functions and Applications*, held at the Katholieke Universiteit Leuven, Belgium, in July 2009. He has been invited as member of a delegation of about ten senior mathematicians and members of the Academy to address the *Franco-Thai Seminar in Pure and Applied Mathematics* (October 2009). He has been keynote speaker at the *International Teletraffic Conference* (ITC 2009). He has been invited in February 2009 to give the *William Benter Distinguished Lecture* at the Centre for Mathematical Sciences of the City University of Hong Kong. He has been invited to give the opening lecture at the *Quantum and Combinatorics* Conference (Zakopane, Poland, November 2009). He has otherwise participated and (co)authored presentations in ICALP'09 (Greece, July 2009) and AofA'09 (Fréjus, June 2009).

Bruno Salvy has been an invited speaker at FPSAC'09. He has given talks on automatic proofs of identities at the "Journées combinatoires de Bordeaux" and at the seminar of the LIP (ENS Lyon). He has given a presentation of the DDMF during the Forum2009 of the joint Inria-Microsoft research lab.

8.4. Foreign Visitors

A large number of our visitors have given talks at the seminar of the project. This year, we received Manuel Kauers, RISC, Johannes Kepler University, Linz, Austria; Christoph Koutschan, RISC, Johannes Kepler University, Linz, Austria; Stefan Gerhold, Financial and Actuarial Mathematics, Vienna University of Technology, Vienna, Austria; Cecilia Holmgren, Uppsala universitet, Sweden; Christina Goldschmidt, Department of Statistics at the University of Warwick, UK; Ayla Gafni, Vanderbilt University, USA; Helmut Prodinger, Department of Mathematics, University of Stellenbosch, South Africa; Manuel Lladser, University of Colorado, USA; Cecilia Holmgren, Uppsala universitet, Sweden; Christina Goldschmidt, Department of Statistics at the University of Warwick, UK; Dana Louigi Addario-Berry, University of Montréal, Québec, Canada.

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", vol. 19, 2009, p. 1092–1107.

[2] L. ADDARIO-BERRY, N. BROUTIN, G. LUGOSI. *The longest minimum weight path in a complete graph*, in "Combinatorics, Probability and Computing", vol. 19, 2010, p. 1–19.

[3] L. ADDARIO-BERRY, N. BROUTIN, B. REED. *Critical random graphs and the structure of a minimum spanning tree*, in "Random Structures Algorithms", vol. 35, 2009, p. 323–347.

[4] A. BOSTAN, S. BOUKRAA, A. J. GUTTMANN, S. HASSANI, I. JENSEN, J.-M. MAILLARD, N. ZENINE. *High order Fuchsian equations for the square lattice Ising model: $\widetilde{\chi}^{(5)}$*, in "J. Phys. A: Math. Theor.", vol. 42, n^{o} 27, 2009, 32pp.

[5] A. BOSTAN, S. BOUKRAA, S. HASSANI, J.-M. MAILLARD, J.-A. WEIL, N. ZENINE. *Globally nilpotent differential operators and the square Ising model*, in "J. Phys. A: Math. Theor.", vol. 42, n^{o} 12, 2009, 50pp.

[6] A. BOSTAN, P. DUMAS. *Wronskians and linear independence*, in "American Mathematical Monthly", 2010.

[7] A. BOSTAN, B. SALVY, É. SCHOST. *Fast conversion algorithms for orthogonal polynomials*, in "Linear Algebra and its Applications", vol. 432, n^{o} 1, January 2010, p. 249–258.

[8] A. BOSTAN, B. SALVY, K. TRAN. *Generating functions of Chebyshev-like polynomials*, in "International Journal of Number Theory", 2010.

[9] A. BOSTAN, É. SCHOST. *A simple and fast algorithm for computing exponentials of power series*, in "Information Processing Letters", vol. 109, n^{o} 13, 2009, p. 754–756.

[10] N. BROUTIN, L. DEVROYE, E. MCLEISH. *Note on the structure of Kruskal's algorithm*, in "Algorithmica", 2010.

[11] P. CLOTE, E. KRANAKIS, D. KRIZANC, B. SALVY. *Asymptotics of Canonical and Saturated RNA Secondary Structures*, in "Journal of Bioinformatics and Computational Biology", vol. 7, n^{o} 5, October 2009, p. 869–893, http://www.worldscinet.com/jbcb/07/0705/S0219720009004333.html.

[12] P. CÉNAC, B. CHAUVIN, S. GINOUILLAC, N. POUYANNE. *Digital Search Trees and Chaos Game Representation*, in "ESAIM, P-S", vol. 13, 2009, p. 15-37.

[13] P. FLAJOLET, S. GERHOLD, B. SALVY. *Lindelöf Representations and (Non-)Holonomic Sequences*, in "Electronic Journal of Combinatorics", 2010.

[14] M. MEZZAROBBA, B. SALVY. *Effective Bounds for P-Recursive Sequences*, in "Journal of Symbolic Computation", 2010.

International Peer-Reviewed Conference/Proceedings

[15] A. BENOIT, B. SALVY. *Chebyshev Expansions for Solutions of Linear Differential Equations*, in "ISSAC '09: Proceedings of the twenty-second international symposium on Symbolic and algebraic computation", J. MAY (editor), 2009, p. 23–30.

[16] A. BOSTAN, M. KAUERS. *Automatic classification of restricted lattice walks*, in "DMTCS Proceedings of the 21st International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC'09), Hagenberg, Austria", 2009, p. 203–217.

[17] A. BOSTAN, É. SCHOST. *Fast algorithms for differential equations in positive characteristic*, in "ISSAC'09", J. MAY (editor), 2009, p. 47–54.

[18] Y. K. CHEUNG, P. FLAJOLET, M. GOLIN, C. Y. J. LEE. *Multidimensional Divide-and-Conquer and Weighted Digital Sums (Extended Abstract)*, in "Proceedings of the Fifth Workshop on Analytic Algorithmics and Combinatorics (ANALCO)", SIAM Press, 2009, p. 58–65.

[19] F. CHYZAK, M. KAUERS, B. SALVY. *A Non-Holonomic Systems Approach to Special Function Identities*, in "ISSAC '09: Proceedings of the twenty-second international symposium on Symbolic and algebraic computation", J. MAY (editor), 2009, p. 111–118.

[20] B. VALLÉE, J. CLÉMENT, J. A. FILL, P. FLAJOLET. *The Number of Symbol Comparisons in QuickSort and QuickSelect*, in "ICALP 2009, Part I", S. ALBERS (editor), Lecture Notes in Computer Science, vol. 5555, Springer-Verlag, 2009, p. 750–763, Proceedings of the 36th International Colloquium on Automata, Languages and Programming.

Scientific Books (or Scientific Book chapters)

[21] P. FLAJOLET, R. SEDGEWICK. *Analytic Combinatorics*, Cambridge University Press, 2009, http://algo.inria.fr/flajolet, 824 pages (ISBN-13: 9780521898065); also available electronically from the authors' home pages..

Research Reports

[22] A. BOSTAN, S. BOUKRAA, S. HASSANI, J.-M. MAILLARD, J.-A. WEIL, N. ZENINE, N. ABARENKOVA. *Renormalization, isogenies and rational symmetries of differential equations*, n^{o} 0911.5466, arXiv, 2009, Technical report.

[23] A. BOSTAN, M. CHOWDHURY, J. VAN DER HOEVEN, É. SCHOST. *Homotopy methods for multiplication modulo triangular sets*, arXiv, 2009, Technical report.

[24] A. BOSTAN, M. KAUERS. *The complete generating function for Gessel walks is algebraic*, n^{o} 0909.1965, arXiv, 2009, Technical report.

Other Publications

[25] L. ADDARIO-BERRY, N. BROUTIN. *Total progeny in killed branching random walk*, 2009, arXiv:0908.1083 [math.PR].

[26] L. ADDARIO-BERRY, N. BROUTIN, L. DEVROYE, G. LUGOSI. *On combinatorial testing problems*, 2009, arXiv:0908.3437 [math.PR].

[27] L. ADDARIO-BERRY, N. BROUTIN, C. GOLDSCHMIDT. *Critical random graphs: limiting constructions and distributional properties*, 2009, arXiv:0908.3629 [math.PR].

[28] L. ADDARIO-BERRY, N. BROUTIN, C. GOLDSCHMIDT. *The continuum limit of critical random graphs*, 2009, arXiv:0903.4730 [math.PR].

[29] R. BACHER, P. FLAJOLET. *Pseudo-factorials, elliptic functions, and continued fractions*, 2009, arXiv:0901.1379v2, 24 pages. Accepted for publication in The Ramanujan Journal.

[30] A. BOSTAN, F. CHYZAK, S. CHEN, Z. LI. *Rational-functions telescopers: Blending creative telescoping with Hermite reduction*, 2009, http://issac2009.kias.re.kr/program_page.html#posters, Poster at the conference ISSAC'09 (Seoul, South Korea).

[31] M. BÓNA, P. FLAJOLET. *Isomorphism and Symmetries in Random Phylogenetic Trees*, 2009, arXiv:0901.0696, 14 pages. To appear in the Journal of Applied Probability..

[32] B. CHAUVIN, N. POUYANNE. *Limit distributions for large Pólya urns*, 2009, arXiv:0907.1477 [math.PR].

[33] S. CHEN, Z. LI. *A speed-up of the Hermite reduction for rational functions*, 2009, http://mmrc.iss.ac.cn/wu90/, Poster at the conference ICMM'09 (Beijing, China).

[34] P. FLAJOLET, M. PELLETIER, M. SORIA. *On Buffon Machines and Numbers (Extended Abstract)*, June 2009, Preprint, 14 pages. Available as arXiv:0906.5560..

[35] L. PECH. *Algorithmes pour la sommation et l'intégration symboliques*, École Normale Supérieure, novembre 2009, http://algo.inria.fr/papers/pdf/Pech-2009-ASI.pdf, 22 pages, Masters thesis.