Project-Team algorithms

Algorithms

Paris - Rocquencourt

Theme: Algorithms, Certification, and Cryptography
# Table of contents

1. **Team** .......................................................... 1
2. **Overall Objectives** ........................................... 1
3. **Scientific Foundations** ...................................... 2
   3.1. Analysis of Algorithms .................................. 2
   3.2. Computer Algebra ....................................... 2
4. **Software** ...................................................... 3
5. **New Results** .................................................. 4
   5.1. Analysis of algorithms ................................... 4
   5.2. Computer Algebra ....................................... 4
6. **Contracts and Grants with Industry** ...................... 4
   6.1. Contracts with Industry .................................. 4
   6.2. National Initiatives ...................................... 4
      6.2.1. Aléa Working Group ................................ 4
      6.2.2. Boole ANR Project ................................ 4
   6.3. International Initiatives ................................. 5
7. **Dissemination** ................................................ 5
   7.1. Animation of the scientific community .................. 5
   7.2. Teaching .................................................. 6
   7.3. Participation in conferences, seminars, invitations .... 6
   7.4. Foreign Visitors .......................................... 7
8. **Bibliography** .................................................. 7
1. Team

Research Scientists
- 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 Members
- Brigitte Chauvin [Professor, University of Versailles, until August]
- Philippe Dumas [Professor, Cl. Prép. lycée Jean-Baptiste Say]

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

Post-Doctoral Fellows
- Thomas Feierl [Until November]
- Cecilia Holmgren [Grant Swedish government, starting September]
- Alexis Darrasse [from April to December]

Administrative Assistant
- Virginie Collette [(AI) Inria]

Others
- Basile Morcrette [ENS Cachan, from February to August]
- Elie De Panafieu [ENS Cachan, from February to December]

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 scenarios, 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 15 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 http://algo.inria.fr/libraries/. 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 Design, tools for expansions in general asymptotic scales, which make it possible to handle in a transparent and automatic way the problems of finding the proper scale for an expansion and of dealing with the indefinite cancellation problem (the MultiSeries package). This year, we have released Algolib versions 13.0 (early 2010) and 14.0 (late 2010). These are compatible with the latest versions of Maple and extend the capabilities of the library by: faster guessing of recurrence/differential equations; faster summation and integration algorithms.

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 at http://algo.inria.fr/ecs/ 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 Dynamic Dictionary of Mathematical Functions (DDMF) at http://ddmf.msr-inria.inria.fr/ gathers several dozens of special functions for which identities, guaranteed high-precision numerical evaluations, power-series and asymptotic expansions, graphs, ...are generated automatically and on the user’s request, starting from a linear differential equation and its initial conditions. The underlying symbolic 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. A nice specificity of this encyclopedia is its interactivity: the approximations values (numbers, series) are not bound to a statically set precision, rather, the user can fill in the precision he wants in a form, before clicking to ask for a refined identity to be generated, then displayed. This interactivity is based on a tool DynaMoW at http://ddmf.msr-inria.inria.fr/DynaMoW/ (for Dynamic Mathematics on the Web) that we develop as well. This is an Ocaml library that simultaneously controls external symbolic calculations and web-page generation at the same time. Being available on the web, the DDMF also plays the role of a showcase for part of the packages developed in our project. It is a successor of our former Encyclopedia of Special Functions at http://algo.inria.fr/esf/.
5. New Results

5.1. Analysis of algorithms

Participants: Nicolas Broutin, Brigitte Chauvin, Frédéric Chyzak, Thomas Feierl, Philippe Flajolet, Jérémie Lumbroso, Basile Morcrette, Bruno Salvy.

The following articles, conference communications and reports summarize new results in analysis of algorithms over the period: [33], [17], [25], [20], [26], [36], [18], [6], [7], [31], [32], [27], [28], [34], [16], [5], [2], [3], [1], [29], [4].

5.2. Computer Algebra

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

The following articles, conference communications and reports summarize new results in computer algebra over the period: [9], [10], [19], [23], [8], [24], [11], [13], [14], [15], [35], [30], [21], [22].

We note that several of the already cited publications are relevant to both analysis of algorithms (analytic combinatorics, discrete models) and computer algebra (special functions, asymptotic analysis): [6], [13], [8], [20], [22].

6. Contracts and Grants with Industry

6.1. Contracts with Industry

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 5 years (2007–2012) by the joint Inria-Microsoft Research Lab. as one of its projects, called “Dynamic Dictionary of Mathematical Functions”.

6.2. National Initiatives

6.2.1. Aléa Working Group

Aléa 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 2010 the yearly meeting (organized by Olivier Bodini Maryse Pelletier and Michèle Soria) has gathered in Luminy over 80 participants from about 20 different research laboratories throughout France.

6.2.2. Boole ANR Project

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. The INRIA Team also includes researchers at the École Normale Supérieure (ENS Ulm): Guilhem Semerjian and Jean Vuillemin.
6.3. International Initiatives

6.3.1. Procope

Nicolas Broutin has obtained two years funding from Egide to support a collaboration on geometric data structures with Ralph Neininger from the University of Frankfurt.

7. Dissemination

7.1. Animation of the scientific community

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.

A. Bostan was a PC member of the 23rd International Symposium on Symbolic and Algebraic Computation (ISSAC’10), Munich, Germany, 2010.

Nicolas Broutin has organized (together with L. Addario-Berry, L. Devroye and C. McDiarmid) the workshop on Branching Random Walks and Searching in Trees at the Banff International Research Station (BIRS), in Canada. He has given invited tutorials at the Young European Probabilist (YEP) Workshop on random trees and algorithms at Eurorandom in Eindhoven and at the mini-school that took place before the Conference on Analysis of Algorithms in Vienna. He also gave talks at the workshop organized by the ANR A3 and at the University of Frankfurt.

Brigitte Chauvin has been a referee for the thesis of Bruno Jaffuel, PhD, U. Paris 6, “Marches aléatoires avec branchement et absorption” and for the thesis of Xingang Liang, PhD, U. de Bretagne Sud, “Propriétés asymptotiques des martingales de Mandelbrot et des marches aléatoires branchantes”. She has been a member of thesis jurys for Chunmiao Huang, PhD, U. de Bretagne Sud, “Théorèmes limites et vitesses de convergence pour certains processus de branchement et des marches aléatoires branchantes”, for Bénédicte Haas, Habilitation, U. Paris 9, “Arbres aléatoires et fragmentations” and for Julien Berestycki, Habilitation, U. Paris 6, “Structures aléatoires de branchement et applications en génétique des populations”. 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 is member of the editorial board of Computer Science Reviews (published by Elsevier). 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 ALÉA 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 2010 as Programme Committee (co)Chair of SIAM’s Conference ANALCO (San Francisco, January 2011) and member of the Programme Committee of ICALP (Bordeaux, July 2010).

Philippe Flajolet has served in several thesis committees: Alexis Darrasse (PhD, algorithms, LIP6, Paris); Patrick Truong (PhD, networks, LIP6, Paris; external referee); Nicolas Schabanel (Habilitation, complex systems, LIAFA, Paris, external referee); Frédéric Jouhet (Habilitation, mathematics, Lyon); Kilian Raschel (PhD, probability, Paris, external referee); Olivier Bodini (Habilitation, random generation, LIP6, Paris; external referee); Cyril Nicaud (Habilitation, automata, Marne la Vallée, Paris; external referee).
Bruno Salvy was a member of the program committee of the International Congress of Mathematical Software (Kobe, Japan), where he organized a session on “Computation with Special Functions”. 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 dissertation of L. Chaussade (Rennes) and the habilitation of M. Safey el Din (Paris 6). He has also been a member of the committees hiring researchers at Inria (CR, DR).

7.2. Teaching

Alin Bostan gave mini-courses on "Fast algorithms for polynomials and matrices" (3h) at the JNCF 2010 at Luminy, and on "Counting Walks using Computer Algebra" (4h) at the "Hypergeometric Days" meeting at Grenoble in April.

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 six hours on Analysis of Algorithms at the Parisian Master of Research in Computer Science (MPRI). Since september 2010, he is supervising (with T. Duquesne) the doctoral research of M. Wang from Paris 6.

Brigitte Chauvin has given a mini-course on “Martingales and random trees” at Monastir (Tunisia) on October.

Frédéric Chyzak gave a lecture (4h and a half) on symbolic algorithms for special functions during the the workshop “Algorithmique et programmation 2010” at Luminy.

Philippe Flajolet has taught a Master level–2 course (MPRI, Paris) on analysis of algorithms, as part (about one third) of a 48 hour course, of which he is responsible, jointly with Michèle Soria (LIP6). He has directed the Master–2 memoir of Basile Morcrette (ENS Cachan, defended in September 2010). He has taught a two week doctoral course at the Technische Universität Berlin (November 2010, comprised of 15 hours of lectures and 8 hours of exercises). He has taught at the “École Jeunes Chercheurs” (a doctoral course, at Chambéry in March 2010: three hours with Brigitte Vallée), at the XVI Incontro Italiano di Combinatoria Algebraica (Bologna, June 2010: three hours) and “Journées de Probabilité” (mini-doctoral course, Monastir, Tunisia, October 2010: two and a half hours).

7.3. Participation in conferences, seminars, invitations

Alin Bostan gave mini-courses on “Fast algorithms for polynomials and matrices” (3h) at the French national meeting in computer algebra (JNCF'10, CIRM, Luminy, May 3-7), and on "Counting Walks using Computer Algebra" (4h) at the "Hypergeometric Days" meeting (Institut Fourier, Grenoble, April 27-29).

On several occasions, Alin Bostan gave talks on his recent works at the internal seminars of several research teams: "Émil Picard", Institut de Mathématiques de Toulouse (Jan. 27-28), "Arénaire", LIP, ENS Lyon (Feb. 11), "Théorie des Nombres et Combinatoire", Univ. Lyon 1 (Dec. 7).

Nicolas Broutin has obtained two years funding from Egide to support a collaboration on geometric data structures with Ralph Neininger from the University of Frankfurt. He has spent twice two weeks at the university of Frankfurt to work with Ralph Neininger. He also spent two weeks invited by the LaBRI to work with J.-F. Marckert. He also spent shorter research periods at McGill University in Montreal (Addario-Berry, Devroye, Reed) and the Free university of Brussels (Langerman).
Brigitte Chauvin has given a talk on “Variable length Markov chains” at the “Journées de Probabilité” at Dijon on June, she has participated to the “Journées ALÉA” on March at Marseille and to the conference AofA (Analysis of Algorithms) at Vienna (Austria) on June. She has been a member of the program committee. She has given a talk in the honour of Jacques Neveu on August at Bordeaux, at the conference of the group Mas of Smai, and at Bath (England) on September for the workshop Paris-Bath on branching random walks. She has given a seminar at U. Paris 6 in January, at Grenoble in November.

Shaoshi Chen presented the 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 workshop FELIM’10 (Limoge, France), March 2010; in a seminar at the École polytechnique (Palaiseau, France), March 2010; at the conference ISSAC’10 (Munich, Germany), July 2010 [24]; at the Algorithms seminar (Rocquencourt, France), October 2010. He also presented his work with Ziming Li on the structure of hyperexponential-hypergeometric functions at the conference The Renaissance of Combinatorics — Advances, Algorithms, Applications (Tianjin, China), August 2010 and as a poster at the conference DART-IV (Beijing, China), October 2010.

Frédéric Chyzak gave a lecture on symbolic algorithms for special functions during the workshop “Algorithmique et programmation 2010”, CIRM, Luminy, May 10. He gave invited presentations on the team’s DDMF project during the Sage Days 24 (Linz, Austria), July 2010 and the Working Knowledge workshop (Trento, Italy), December 2010. He was also invited speaker at the conference The Renaissance of Combinatorics — Advances, Algorithms, Applications (Tianjin, China), August 2010, where he presented joint work with Alin Bostan (of the project-team) and Mark van Hoeij (Florida State University, Tallahassee, USA) on explicit formula for the generating series of diagonal 3D rook paths.

Thomas Feierl gave a talk on Asymptotics for reflectable lattice walks in a Weyl chamber of type B at the “Séminaire Lotharingien de Combinatoire 64” in March 28 - 31, Lyon; and to AofA 2010, June 28 - July 2 2010, Wien, Austria, he gave a talk on Asymptotics for Walks in a Weyl chamber of Type B. He has been at the 7th international conference on lattice path combinatorics and applications, July 4-7 2010, Siena, Italy where he gave the talk on Asymptotics for walks in a Weyl chamber.

Philippe Flajolet has given invited talks at the following places: University of Paris South at Orsay (Statistical Physics Seminar, January 2010); University of Bordeaux (Combinatorics Days, January 2010); Academia Sinica, National Taipei University, and National Tsing Hua University (Taiwan); University of Paris South at Orsay (Combinatorics Day in the honour of D. Gouyou-Beauchamps, May 2010); University of Paris North (Combinatorics Day, May 2010); University of Bordeaux (“Journées SMAI/MAS et Jacques Neveu, August 2010); Institut Henri Poincaré (Combinatorics Seminar, October 2010); University of Caen (Algorithms Seminar and Working Group, November 2010). He has been invited for three weeks at the Institute of Nuclear Physics (Crakow, Poland) in February, July, and October 2010 and for a two week visit at Purdue University (USA).

Bruno Salvy has been an invited speaker at ANALCO’10 (Austin, Texas), where he gave a talk on “Newton iteration: From numerics to combinatorics, and back”; and at AISC’10, where he gave the talk on the Dynamic Dictionary of Special Functions. He presented the DDMF or talks on proofs of special function identities at the International Congress of Mathematical Software (Kobe, Japan), at a seminar in the Institute of Mathematics and System Sciences of the Chinese Academy of Sciences (Beijing, China), at the Joint Institutes Workshop of the Microsoft research - Inria joint centre (Orsay), at a seminar of the University of Marne-la-Vallée.

7.4. Foreign Visitors

The following visitors have spent research periods in the group and participated in seminars: Kilian Raschel, Bielefeld University, Germany; Henning Sulzbach, Universität Frankfurt, Germany; Mark Daniel Ward, Purdue University, USA;

8. Bibliography
Publications of the year

Articles in International Peer-Reviewed Journal


International Peer-Reviewed Conference/Proceedings


Research Reports


