INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Algorithms seminar, 1997-1998

Bruno SALVY, éditeur scientifique

N ° 3504
Septembre 1998

THÈME 2

Rapport de recherche

ISSN 0249-6399

Algorithms seminar, 1997-1998

Bruno SALVY, éditeur scientifique

Thème 2 — Génie logiciel
et calcul symbolique
Projet Algo

Rapport de recherche n° 3504 — Septembre 1998 — 180 pages

Abstract: These seminar notes represent the proceedings of a seminar devoted to the analysis of algorithms and related topics. The subjects covered include combinatorics, symbolic computation, asymptotic analysis and average-case analysis of algorithms and data structures.

(Résumé : tsvp)

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
Téléphone : (33) 01 39 63 55 11 – Télécopie : (33) 01 39 63 53 30

Séminaire algorithmes, 1997-1998

Résumé : Ces notes de séminaires représentent les actes, en anglais, d'un séminaire consacré à l'analyse d'algorithmes et aux domaines connexes. Les thèmes abordés comprennent : combinatoire, calcul formel, analyse asymptotique et analyse en moyenne d'algorithmes et de structures de données.

ALGORITHMS SEMINAR
1997–1998

Bruno Salvy[1]
(Editor)

Abstract

These seminar notes represent the proceedings of a seminar devoted to the analysis of algorithms and related topics. The subjects covered include combinatorics, symbolic computation, probabilistic methods and average-case analysis of algorithms and data structures.

This is the seventh of our series of seminar proceedings. The previous ones have appeared as INRIA Research Reports numbers 1779, 2130, 2381, 2669, 2992 and 3267. The content of these proceedings consists of English summaries of the talks, usually written by a reporter from the audience[2].

The primary goal of this seminar is to cover the major methods of the average-case analysis of algorithms and data structures. Neighbouring topics of study are combinatorics, symbolic computation, asymptotic analysis and probabilistic methods.

The study of combinatorial objects—their description, their enumeration according to various parameters—arises naturally in the process of analyzing algorithms that often involve classical combinatorial structures like strings, trees, graphs, and permutations.

Computer algebra plays an increasingly important rôle in this area. It provides a collection of tools that allows one to attack complex models of combinatorics and the analysis of algorithms via *generating functions*; at the same time, it inspires the quest for developing ever more systematic solutions and decision procedures for the analysis of well-characterized classes of problems.

The 40 articles included in this book represent snapshots of current research in these areas. A tentative organization of their contents is given below.

PART I. COMBINATORIAL MODELS

In addition to its own traditions rooted in mathematics, the study of *combinatorial models* arises naturally in the process of analyzing algorithms that often involve classical combinatorial structures like permutations, strings, trees and graphs.

Polyominoes are a classical object of combinatorics, related to statistical physics. A survey of enumeration results in this area is given in [**1**]. Two kinds of permutations are studied in [**2**] and [**3**]: permutations that can be sorted with a bounded stack (a classical problem of Knuth) and permutations with forbidden subsequences. A relation between equations on permutations and combinatorial maps is exhibited in [**4**]. The classical inversion theorem of Lagrange is extended to the multivariate case in [**5**] and applied to algebraic series in [**6**], while [**7**] shows how many power series can be proved to be non-algebraic. Recently, a lot of attention has been paid to so-called "Euler sums" (infinite multi-indexed sums of inverses of integers), this is the subject of [**8**] and [**9**].

[1]This work was supported in part by the Long Term Research Project Alcom-IT (#20244) of the European Union.
[2]The summaries for the past seven years are available on the web at the URL `http://algo.inria.fr/seminars/`.

The talks **[11]** and **[12]** explore links between combinatorics and logic, while **[13]** and **[14]** apply techniques from statistical physics to combinatorial questions.

[1] Enumeration of Remarkable Families of Polyominoes. *Dominique Gouyou-Beauchamps*
[2] Sorted and/or Sortable Permutations. *Mireille Bousquet-Mélou*
[3] From Motzkin to Catalan Permutations: a "Discrete Continuity". *Renzo Pinzani*
[4] Products of Permutations and Combinatorial Maps. *Gilles Schaeffer*
[5] Multivariate Lagrange Inversion. *Bruce Richmond*
[6] Coefficients of Algebraic Series. *Michèle Soria and Philippe Flajolet*
[7] On the Transcendence of Formal Power Series. *Jean-Paul Allouche*
[8] Multidimensional Polylogarithms. *David M. Bradley*
[9] Monodromy of Polylogarithms. *Minh Hoang Ngoc*
[10] A Combinatorial Approach to Golomb Trees. *Mordecai Golin*
[11] Colouring Rules and Second Order Sentences. *Alan R. Woods*
[12] Fraïssé-Ehrenfeucht Games and Asymptotics. *Alan R. Woods*
[13] Statistical Physics and Random Graphs. *Remi Monasson*
[14] Statistical Physics of the Random K-Satisfiability Problem. *Remi Monasson*

PART II. SYMBOLIC COMPUTATION

Combinatorial identities and their q-analogues are now amenable to an automatic treatment by symbolic computation thanks to Zeilberger's algorithm. This is presented in **[15]**, together with a nice application to obtaining a family of identities. Another connection between combinatorics and symbolic computation arises via generating functions that often satisfy functional or differential equations. Linear q-difference equations possess power series solutions whose divergence is studied by **[16]**. In **[17]**, it is shown that much of the analysis of solutions of systems of linear differential equations can be done automatically. The problems in the non-linear case are of course more difficult, but some theory and packages are already available and presented in **[18]**. The next two summaries are concerned by the resolution of polynomial equations from two very different viewpoints: bivariate Diophantine equations are solved efficiently by a new algorithm in **[19]**, while numerical solutions with arbitrary precision are found by the best known algorithm in **[20]**. Polynomials are also the topic of **[21]** where the problem is whether a given multivariate polynomial can factor over an algebraic extension of $\mathbb{Q}$. Progress in symbolic integration of algebraic function is described in **[22]**. This part concludes with two talks on computational number theory.

[15] q-WZ-Theory and Bailey Chains. *Peter Paule*
[16] Summability of Power Series Solutions of q-Difference equations. *Changgui Zhang*
[17] Computing Invariants of Systems of Ordinary Linear Differential Equations. *Eckhard Pflügel*
[18] Algebra and Algorithms for Differential Systems. *Évelyne Hubert*
[19] Solving Diophantine Equations. *Guillaume Hanrot*
[20] Solution of Polynomial Equations. *Victor Pan*
[21] Absolute Irreducibility of Polynomials with Rational Coefficients. *Jean-François Ragot*
[22] The Lazy Hermite Reduction. *Manuel Bronstein*
[23] ECPP Comes Back. *François Morain*
[24] Cyclotomic Primality. *Preda Mihailescu*

PART III. ANALYSIS OF ALGORITHMS AND DATA STRUCTURES

Linear probing is a classical strategy for the resolution of collision in hashing. The problem of its analysis was first proposed by Knuth in 1962; a solution by analytic combinatorics (an interplay between combinatorics and complex analysis) involving the Airy function is described in **[25]**. Another special function, the Buchstab function is shown in **[26]** to arise quite generally in statistics related to the smallest component in sets of structures. Analytic combinatorics is also applied in **[27]** to analyze an efficient structure for tries. A relation between Pólya urn models and random trees is exploited in **[28]** to analyze various families of random trees, in particular a fringe balancing strategy for binary search trees. An approach based on analytic combinatorics for more precise results on this latter analysis is developed in **[29]**. Binary search trees are present in **[30]** in connection with partitioning processes. Binary trees are used also in **[31]** to model the behaviour of a family of sorting algorithms. Functional analysis is applied in **[32]** to the old problem of analyzing the complexity of the binary Euclidean algorithm. A randomized algorithm in molecular biology is described by **[33]**. The last two summaries concern text searching algorithms.

PART IV. PROBABILISTIC METHODS

This part contains talks of a more probabilistic origin, but not necessarily very different from those of the previous part. For instance, **[36]** explores the connection between birth-death processes and classical combinatorial objects like lattice paths and orthogonal polynomials. Branching processes are related to trees and Dyck paths in **[37]**. Quantitative estimates on convergence of Markov processes are given by **[38]**. Models of network traffic are discussed in **[39]** and **[40]** studies the asymptotic behaviour of a routing strategy.

Acknowledgements. The lectures summarized here emanate from a seminar attended by a community of researchers in the analysis of algorithms, from the Algorithms Project at INRIA (the organizers are Philippe Flajolet and Bruno Salvy) and the greater Paris area—especially University of Paris Sud at Orsay (Dominique Gouyou-Beauchamps) and LIP6 (Michèle Soria). The editor expresses his gratitude to the various persons who actively supported this joint enterprise and offered to write summaries. Thanks are also due to the speakers and to the authors of summaries. Many of them have come from far away to attend one seminar and kindly accepted to write the summary. We are also greatly indebted to Virginie Collette for making all the organization work smoothly.

The Editor
B. SALVY

Part 1

Combinatorics

Enumeration of Remarkable Families of Polyominoes

Dominique Gouyou-Beauchamps
LRI, Université de Paris Sud (Orsay)

Mars 2, 1998

[summary by Cyril Banderier]

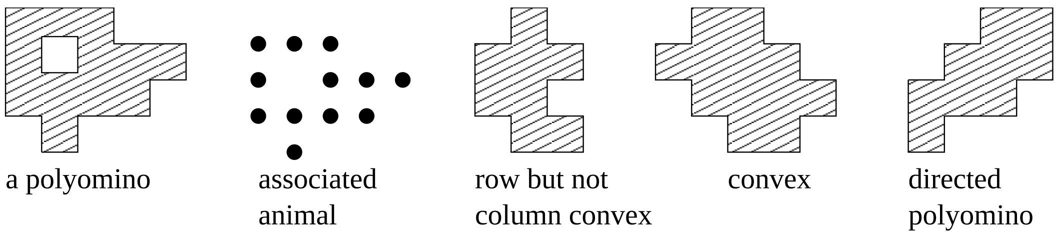
1. Introduction

Polyominoes are objects sprung from recreative mathematics and from different domains in physics (such as Ising's model; its generalisation, Pott's model; directed percolation and branched polymer problems) [14, 20, 21, 25]. Two great classes of problems relative to polyominoes are

- tiling problems;
- enumeration problems.

David Klarner began to study polyomino tilings in 1965. There are still open questions in this field [12, 15, 16, 17], however several (un)decidability results are known [1, 2]. What is more, aperiodic tilings are today a new spring of inspiration in noncommutative geometry [8]. In the remainder, we only consider enumeration problems. Exact asymptotics of polyominoes on a square lattice is still unknown. Accurate results are then limited to special families of polyominoes, for which we know a generative grammar. We are therefore brought back to the study of a functional equation which defines the generating function. Nevertheless, obtaining of a closed form (*i.e.*, an explicit solution) or even any form of solution often remains difficult. We will show several methods to obtain them.

2. Definitions



A polyomino is a connected set on a lattice. A polyomino is said to be convex if it is both column-convex and row-convex. A polyomino is said to be directed if, for each couple of points of the polyomino, there exists a path only made of North and West steps which links this two points.

One can find in previous summaries [4, 13] how to obtain functional equations satisfied by the generating functions (most of the methods are tricky decompositions [5] of polyominoes into very regular smaller pieces, such as "strata" or "wasp-waist" decompositions). For results in dimension greater than 2, see [3, 6].

3. Differential Equation Method

Enumeration of convex polyominoes with perimeter $2n$ on the honeycomb (or "hexagonal") lattice can be solved with this method. Let P_n the number of such polyominoes with perimeter $2n+6$, Enting [10] gives the following result. The generating function $P(x) = \sum_{n=0}^{\infty} p_n x^n$ satisfies the differential equation

$$\begin{aligned} &P''(x)(x^2 - 7x^4 - 2x^5 + 12x^6 + 8x^7) + P'(x)(-11x - 4x^2 + 53x^3 + 22x^4 - 40x^5 - 16x^6) \\ &\qquad + P(x)(20 + 22x - 52x^2 - 20x^3 - 16x^4 - 32x^5) = 20 + 22x - 52x^2 + 8x^3 + 4x^4 + 8x^5 \end{aligned}$$

which leads to

$$P(x) = \frac{1 - 2x + x^2 - x^4 - x^2\sqrt{1-4x^2}}{(1+x)^2(1-2x)^2}.$$

Let us mention that the package GFUN in Maple is able to make such translations (recurrences, differential equations, algebraic equations, closed forms), see [23].

4. Temperley's Method

We are going to illustrate Temperley's method [24] with the enumeration of column convex polyominoes (on a square lattice) with respect to perimeter [7]. The generating function

$$G(y) = \sum_{n \geq 2} y^{2n}$$

can be rewritten as

$$G(y) = \sum_{r \geq 1} g_r(y)$$

where the g_r satisfy a recurrence

$$g_{r+4} - 2(1+y^2)g_{r+3} + (1 + 3y^2 + 3y^4 - y^6)g_{r+2} - 2y^2(1+y^2)g_{r+1} + y^4 g_r = 0$$

and g_1, g_2, g_3, g_4, the "initial conditions", are known.

If we "guess" that g_r has the shape λ^r (or is a linear combination of such monomials), we can obtain λ by solving the fourth degree equation associated to the recurrence formula, and we find, as the equation easily splits:

$$(\lambda^2 - \lambda(1 + y + y^2 - y^3) + y^4)(\lambda^2 - \lambda(1 - y + y^2 + y^3) + y^2) = 0.$$

So solving the two second degree equations gives four values (closed forms) $\lambda_1, \lambda_2, \lambda_3, \lambda_4$, two of which are $O(1)$ at 0. We then have to find the A_j such that $g_r = \sum_{j=1}^{4} A_j \lambda_j^r$. But $g_r = O(y^{2r+2})$ at 0, so $A_i = 0$ if $\lambda_i = O(1)$. There are still two coefficients to determine, say A_2 and A_4. They can be found by solving a system involving $g_1, g_2, \lambda_2, \lambda_4, A_2, A_4$ and one finally obtains a closed form

$$G(y) = \frac{A_2 \lambda_2}{1 - \lambda_2} + \frac{A_4 \lambda_4}{1 - \lambda_4}.$$

A very similar method is applied for unidirectional-convex polygons on the honeycomb lattice in [19].

5. **Kernel Method**

In his talk, Dominique Gouyou-Beauchamps has also presented an exploitation of the "kernel method" for the enumeration of parallelogram polyominoes with respect to horizontal and vertical half-perimeter, area and first column height, respectively marked by x, y, q, s.

Remember that the generating function P with respect to horizontal and vertical half-perimeter is easy to obtain: The wasp-waist decomposition directly leads to $P = xy + xP + yP + P^2$ so

$$P(x,y) = \frac{1 - x - y - \sqrt{1 - 2x - 2y + x^2 + y^2 - 2xy}}{2}.$$

The full generating function $P(x, y, q, s)$ satisfies a more intricate equation (obtained by a strata decomposition), namely

$$P(x,y,q,s) = \frac{xysq}{1-ysq} + \frac{xsq}{(1-sq)(1-ysq)} P(x,y,q,1) - \frac{xsq}{(1-sq)(1-ysq)} P(x,y,q,sq).$$

When $q = 1$, this can be rewritten

$$(1 - (1 - x - y)s + y^2)P(x, y, 1, s) = xsP(x, y, 1, 1) + xys(1 - s).$$

It is typically the type of equation on which the kernel method applies. This method belongs to mathematical folklore (see [18], exercise 2.2.1.4 for an early example). It works as follows: If one cancels the kernel $(1 - (1 - x - y)s + y^2)$, *i.e.*, one finds s_0 such that $(1 - (1 - x - y)s_0 + y^2) = 0$, then one gets $0 = xs_0P(x, y, 1, 1) + xys_0(1 - s_0)$, from which follows a closed form for $P(x, y, 1, 1)$ and finally one obtains a closed form for $P(x, y, 1, s)$, *viz.,*

$$P(x,y,1,s) = \frac{xs\left(\frac{1-x-y-\sqrt{1-2x-2y-2xy+x^2+y^2}}{2}\right) + xys(1-s)}{1-(1-x-y)s+y^2}.$$

6. **Physicists' Guesses**

We have already mentioned that polyominoes are present in physical problems and in fact the first people who found interesting results on this subject where physicists. They sometimes base their works on empirical results. For example, in [9], the authors are doing as if

$$N_r^s = N_{r-1}^{s-1} + N_r^{s-1} + N_{r+1}^{s-1}$$

(N_r^s is the number of directed animals of size s with a "compact source" of size r) was a recurrence formula satisfied by the N_r^s although it is only empirically verified for the first values. Nevertheless, they go on and find that

$$N_r^s = \frac{1}{2\pi} \int_0^{2\pi} (1 + e^{it})e^{-irt}(1 + 2\cos t)^{s-1} dt \quad \text{and in particular} \quad N_1^s = (s-1)! \sum_{q=0}^{\lfloor s/2 \rfloor} \frac{s-q}{q!^2(s-2q)!}.$$

Another example of a typical physicist's method is [14] (enumeration of directed animals on a strip of width k); they consider a transfer matrix as an operator acting on a spin space and are drawing their inspiration from standard techniques on integrable systems.

When k tends to infinity, they obtain:

$$a_n = \sum_{0 \le i \le n} \binom{n-1}{i} \binom{i}{\lfloor i/2 \rfloor} \quad \text{and thus} \quad \sum_{n \ge o} a_n t^n = \frac{1}{2}\left(\sqrt{\frac{1+t}{1-3t}} - 1\right).$$

Analysis of singularities gives

$$a_n \sim 3^n n^{-1/2}.$$

7. Matricial and Continued Fraction Method

We will show on a simple example (Dyck paths) how this method works. Let

$$d_h(x) = \sum_{l \geq 0} a_{h,l} x^l$$

the ordinary generating function of Dyck paths which end at height h.

A path of length n which ends at height h is either a path of length $n-1$ which ends at height $h-1$ followed by a NE step, or a path of length $n-1$ which ends at height $h+1$ followed by a SE step. Thus one obtains the following infinite system

$$\begin{cases} d_0(x) = 1 + x d_1(x) \\ d_1(x) = x d_0(x) + x d_2(x) \\ d_2(x) = x d_1(x) + x d_3(x) \\ \qquad \vdots \\ d_h(x) = x d_{h-1}(x) + x d_{h+1}(x) \\ \qquad \vdots \end{cases}$$

which can be written as

$$\begin{pmatrix} -1 & x & 0 & 0 & \dots \\ x & -1 & x & 0 & \dots \\ 0 & x & -1 & x & \dots \\ 0 & 0 & x & -1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} d_0(x) \\ d_1(x) \\ d_2(x) \\ d_3(x) \\ \vdots \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ \vdots \end{pmatrix}.$$

With an analog of Cramer's formula for infinite matrices, one has

$$d_0(x) = \frac{\det \begin{pmatrix} -1 & x & 0 & 0 & \dots \\ 0 & -1 & x & 0 & \dots \\ 0 & x & -1 & x & \dots \\ 0 & 0 & x & -1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}}{\det \begin{pmatrix} -1 & x & 0 & 0 & \dots \\ x & -1 & x & 0 & \dots \\ 0 & x & -1 & x & \dots \\ 0 & 0 & x & -1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}} = \lim_{k \to \infty} \frac{\det \left(\ \right)_{k \times k}}{\det \left(\ \right)_{k \times k}} = \lim_{k \to \infty} \frac{P_k(x)}{Q_k(x)}$$

where $\left(\ \right)_{k \times k}$ stands for the $k \times k$ truncated associated matrices. The special structure of these matrices gives the recurrence

$$\begin{cases} P_k(x) = -Q_{k-1}(x) = -P_{k-1}(x) - x^2 P_{k-2}(x) & \text{with } P_1(x) = -1, \\ Q_k(x) = -Q_{k-1}(x) - x^2 Q_{k-2}(x) & \text{with } Q_1(x) = -1 \text{ and } Q_2(x) = 1 - x^2. \end{cases}$$

from which follows

$$\frac{P_k(x)}{Q_k(x)} = \frac{-Q_{k-1}(x)}{Q_k(x)} = \frac{-Q_{k-1}(x)}{-Q_{k-1}(x) - x^2 Q_{k-2}(x)} = \frac{1}{1 - x^2 \frac{Q_{k-2}(x)}{-Q_{k-1}(x)}} = \frac{1}{1 - x^2 \frac{P_{k-1}(x)}{Q_{k-1}(x)}}$$

and then

$$d_0(x) = \lim_{k\to\infty} \frac{P_k(x)}{Q_k(x)} = \cfrac{1}{1 - \cfrac{x^2}{1 - \cfrac{x^2}{\ddots}}}$$

hence

$$d_0(x) = \frac{1}{1 - x^2 d_0(x)} \quad i.e., \quad d_0(x) = \frac{1 - \sqrt{1 - 4x^2}}{2x^2}.$$

In fact the continued fraction is a special case of a much more general result that we will express in the next section.

8. Multicontinued Fractions Theorem

We will need the following notations. Let $(\lambda_{l,k})_{0\le k\le l}$ be a family of elements of a commutative field and let $(P_k)_{k\ge 0}$ be a family of monic polynomials which satisfy a recurrence relation:

$$P_{k+1}(x) = xP_k(x) - \sum_{i=0}^{k} \lambda_{k,k-i} P_{k-i}(x).$$

One then defines a multicontinued fraction by

$$L(\lambda, t) = \cfrac{1}{1 - \lambda_{0,0}t - \sum_{p=1}^{\infty} \lambda_{p,0} t^{p+1} \prod_{i=1}^{p} \cfrac{1}{1 - \lambda_{i,i}t - \sum_{q=1}^{\infty} \lambda_{q+i,0} t^{q+1} \prod_{i=1}^{q} \cfrac{1}{\ddots}}}.$$

Let δ be the operator defined by $\delta(\lambda_{k,l}) = \lambda_{k+1,l+1}$. We note P^* the reciprocal polynomial of P:

$$P^*(x) := x^{\deg(P)} P(\frac{1}{x}).$$

Theorem 1 (Roblet, Viennot). *If one sets $\lambda_{i,j} := 0$ in $L(\lambda, t)$ for $i \ge k+1$ and $j \le i$, one gets a rational fraction $L_k(t)$, it is the k-th convergent of the multicontinued fraction $L(\lambda, t)$ and we have*

$$L_k(t) = \frac{\delta P_k^*(t)}{P_{k+1}^*(t)}$$

and the following approximation near $t = 0$ holds

$$L(\lambda, t) = L_k(t) + O(t^{k+1}).$$

For a deeper understanding of links between continued fractions and combinatorics, see [11, 22]. The multicontinued fraction method allows to find the generating functions of diagonally convex directed, diagonally convex, parallelogram, vertically convex directed, vertically convex polyominoes and remains to be exploited to obtain generating functions of other classes of polyominoes or directed animals.

You are now ready to try the different kinds of methods presented here on your favourite class of polyominoes or even on other classes of combinatorial objects!

Bibliography

[1] Beauquier (Danièle), Nivat (Maurice), Remila (Éric), and Robson (Mike). – Tiling figures of the plane with two bars. *Computational Geometry. Theory and Applications*, vol. 5, n° 1, 1995, pp. 1–25.

[2] Berger (Robert). – The undecidability of the domino problem. *Memoirs of the American Mathematical Society*, vol. 66, 1966, p. 72.

[3] Bousquet-Mélou (M.) and Guttmann (A. J.). – Three-dimensional self-avoiding convex polygons. *Physical Review E. Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics. Third Series*, vol. 55, n° 6, part A, 1997, pp. R6323–R6326.

[4] Bousquet-Mélou (Mireille). – Counting convex polyominoes according to their area. In *Algorithms seminar 1995-1996*. – INRIA, 1996. Available at *http://pauillac.inria.fr/algo/seminars/sem95-96/bousquet1.ps*.

[5] Bousquet-Mélou (Mireille). – A method for the enumeration of various classes of column-convex polygons. *Discrete Mathematics*, vol. 154, n° 1-3, 1996, pp. 1–25.

[6] Bousquet-Mélou (Mireille) and Guttmann (Anthony J.). – Enumeration of three-dimensional convex polygons. *Annals of Combinatorics*, vol. 1, n° 1, 1997, pp. 27–53.

[7] Brak (R.), Guttmann (A. J.), and Enting (I. G.). – Exact solution of the row-convex polygon perimeter generating function. *Journal of Physics. A. Mathematical and General*, vol. 23, n° 12, 1990, pp. 2319–2326.

[8] Connes (Alain). – *Noncommutative geometry*. – Academic Press Inc., San Diego, CA, 1994, xiv+661p.

[9] Dhar (Deepak), Phani (Mohan K.), and Barma (Mustansir). – Enumeration of directed site animals on two-dimensional lattices. *Journal of Physics. A. Mathematical and General*, vol. 15, n° 6, 1982, pp. L279–L284.

[10] Enting (I. G.) and Guttmann (A. J.). – Polygons on the honeycomb lattice. *Journal of Physics. A. Mathematical and General*, vol. 22, n° 9, 1989, pp. 1371–1384.

[11] Flajolet (P.). – Combinatorial aspects of continued fractions. *Discrete Mathematics*, n° 2, 1980, pp. 125–161.

[12] Grünbaum (Branko) and Shephard (G. C.). – *Tilings and patterns*. – W. H. Freeman and Company, New York, 1989, *A Series of Books in the Mathematical Sciences*, xii+446p. An introduction.

[13] Guttmann (Tony). – Staircase polygons, elliptic integrals and Heun functions. In *Algorithms seminar 1996-1997*. – 1997. Available at *http://pauillac.inria.fr/algo/seminars/sem96-97/guttmann.ps*.

[14] Hakim (V.) and Nadal (J. P.). – Exact results for 2D directed animals on a strip of finite width. *Journal of Physics. A. Mathematical and General*, vol. 16, n° 7, 1983, pp. L213–L218.

[15] Klarner (D.). – My life among the polyominoes. *Nieuw Archief voor Wiskunde. Derde Serie*, vol. 29, n° 2, 1981, pp. 156–177.

[16] Klarner (David A.). – Some results concerning polyominoes. *The Fibonacci Quarterly*, vol. 3, 1965, pp. 9–20.

[17] Klarner (David A.). – Packing a rectangle with congruent n-ominoes. *Journal of Combinatorial Theory*, vol. 7, 1969, pp. 107–115.

[18] Knuth (Donald E.). – *The art of computer programming*. – Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1973, second edition, xxii+634p. Volume 1: Fundamental algorithms, Addison-Wesley Series in Computer Science and Information Processing.

[19] Lin (K. Y.) and Wu (F. Y.). – Unidirectional-convex polygons on the honeycomb lattice. *Journal of Physics. A. Mathematical and General*, vol. 23, n° 21, 1990, pp. 5003–5010.

[20] Privman (V.) and Švrakić (N. M.). – Difference equations in statistical mechanics. I. Cluster statistics models. *Journal of Statistical Physics*, vol. 51, n° 5-6, 1988, pp. 1091–1110. – New directions in statistical mechanics (Santa Barbara, CA, 1987).

[21] Privman (V.) and Švrakić (N. M.). – *Directed models of polymers, interfaces, and clusters: scaling and finite-size properties*. – Springer-Verlag, Berlin, 1989, *Lecture Notes in Physics*, vol. 338, vi+120p.

[22] Roblet (Emmanuel) and Viennot (Xavier Gérard). – Théorie combinatoire des T-fractions et approximants de Padé en deux points. In *Proceedings of the 5th Conference on Formal Power Series and Algebraic Combinatorics (Florence, 1993)*, vol. 153, pp. 271–288. – 1996.

[23] Salvy (Bruno) and Zimmermann (Paul). – Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable. *ACM Transactions on Mathematical Software*, vol. 20, n° 2, 1994, pp. 163–177. – ftp://ftp.inria.fr/INRIA/publication/publi-ps-gz/RT/RT-0143.ps.gz.

[24] Temperley (H. N. V.). – Combinatorial problems suggested by the statistical mechanics of domains and of rubber-like molecules. *Physical Review (2)*, vol. 103, 1956, pp. 1–16.

[25] Viennot (Gérard). – Problèmes combinatoires posés par la physique statistique. *Astérisque*, n° 121-122, 1985, pp. 225–246. – Seminar Bourbaki, Vol. 1983/84.

Sorted and/or Sortable Permutations

Mireille Bousquet-Mélou
LaBRI, Université de Bordeaux

June 8, 1998

[summary by Cyril Banderier]

1. Introduction

The classical railroad cars switching problem [12] (*viz.* to reorder cars in a given order with the help of a single garage-track) is here revisited and generalised in terms of permutations and trees. Permutations which are sortable by one (or more than one) stack have been studied by West [14] and some generating functions have been found [15]. By factorising permutations (following and generalising an idea of Zeilberger's), Mireille Bousquet-Mélou obtained functional equations for one-stack sortable, two-stack sortable, sorted permutations, sorted and sortable permutations. She shows q-analogues arise in counting inversions. Most of these functional equations involve divided differences. The quadratic method allows to solve some of them while the other ones remain quite mysterious. She also gives an algorithm which decides if a permutation is sorted.

2. Sorting Procedure

In his Ph.D. thesis [14], Julian West studied a procedure Π that permutes the letters of a word σ consisting of distinct letters in the alphabet $\{1, 2, 3, \dots\}$. The procedure uses a stack s and works as follows:

$\tau := \epsilon$
$s := \epsilon$
while $\sigma \neq \epsilon$ **do**
  $f :=$Firstletter(σ)
  if $s = \epsilon$ **or** $f <$ Top(s)
    then
      $s := sf$
      $\sigma := f^{-1}\sigma$
    else
      $s := s\,\mathrm{Top}(s)^{-1}$
      $\tau := \tau\,\mathrm{Top}(s)$
end
$\tau := \tau\tilde{s}$
return τ

In this procedure, ϵ is the empty word, $\tilde{s}$ is the mirror of the word s and the inverse b^{-1} of a letter b of the alphabet $\{1, 2, 3, \dots\}$ is a new letter with the property $bb^{-1} = b^{-1}b = \epsilon$. The output word τ has n letters, and we define it to be $\Pi(\sigma)$, the word obtained by *sorting σ through a stack.* This procedure extends a procedure described by Knuth [12, p. 238].

West observed that the map Π can alternatively be described recursively by

$$\Pi(\sigma^L m \sigma^R) = \Pi(\sigma^L)\Pi(\sigma^R)m$$

where m is the largest letter of the word $\sigma = \sigma^L m \sigma^R$. With at most $n-1$ iterations, σ is an increasing word, *i.e.* Π sorts the letters of σ.

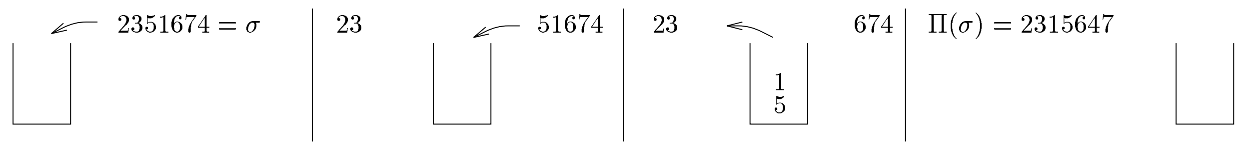


FIGURE 1. The sorting algorithm applied to $\sigma = 2351674$.

Let $\mathcal{S}_n$ be the set of permutations of $\{1, 2, \ldots, n\}$. We represent the action of Π on $\mathcal{S}_n$ by a *sorting tree*: the nodes of this tree are the elements of $\mathcal{S}_n$, and an edge connects σ to $\Pi(\sigma)$ for all $\sigma \in \mathcal{S}_n$.

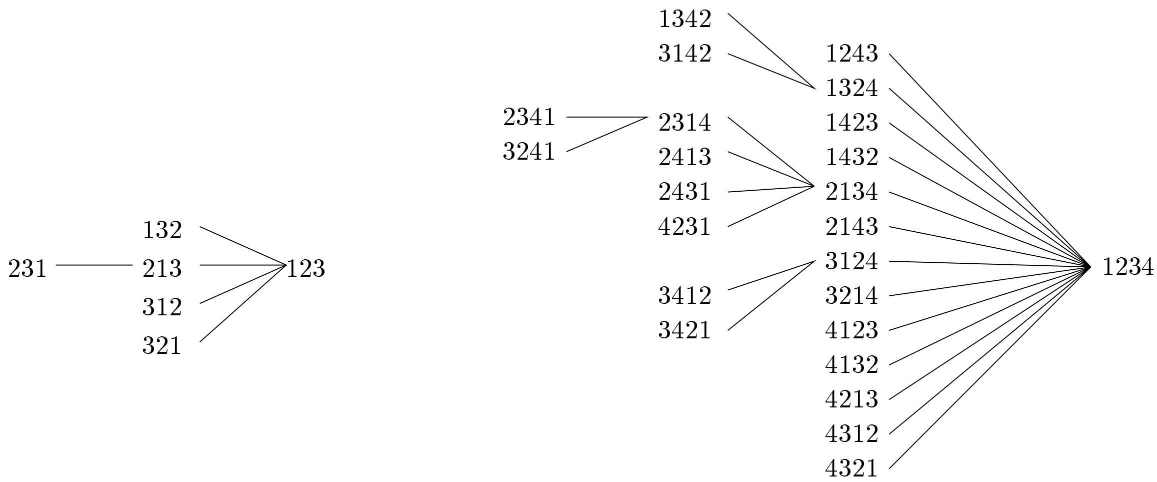


FIGURE 2. The sorting trees for $\mathcal{S}_3$ and $\mathcal{S}_4$.

We can visualise on this tree the four classes of permutations we will consider in this paper.

One-stack sortable permutations. These permutations occur in the last two columns of the sorting tree. Knuth [12] proved that the number of such permutations is $\binom{2n}{n}/(n+1)$. They are exactly the permutations avoiding the pattern 231: there exists no triple (i, j, k) with $1 \leq i < j < k \leq n$ such that $\sigma(k) < \sigma(i) < \sigma(j)$.

Two-stack sortable permutations. They occur in the last three columns of the sorting tree. Their generating function $\sum c_n x^n$ satisfies

$$x^2F^3 + x(2+3x)F^2 + (1 - 14x + 3x^2)F + x^2 + 11x - 1 = 0.$$

West conjectured that

$$c_n = \frac{2(3n)!}{(2n+1)!(n+1)!}.$$

This was proved by Zeilberger [15], who found the previous equation and then used the Lagrange inversion formula.

Sorted permutations. These are those permutations which belong to $\Pi(\mathcal{S}_n)$. Induction on the length of permutations shows that any suffix of a sorted permutation is a sorted word. Sorted permutations cannot be described in terms of forbidden patterns: in fact any pattern occurs as a factor in some sorted permutation. We shall give a functional equation satisfied by their generating function.

Sorted and (one-stack) sortable permutations. Their generating function satisfies

$$x^3F^4 + x^2(3+4x)F^3 + x(3-29x+6x^2)F^2 + (1-7x+29x^2+4x^3)F - (1-x)^3 = 0.$$

3. **Permutations and Trees**

There is a classical bijection between permutations and binary search trees: one gets a permutation from a labelled tree by reading it with a "lower reading" (you start at the root, and recursively, you read the subtrees, the left one at first, and when you have visited all the left children, you add the label of the current node to a list, the final list is the permutation associated to the tree), on the other hand one gets a tree from a permutation $\sigma = \sigma^L m \sigma^R$ by creating recursively the tree with root m and a left subtree associated to σ^L and a right subtree associated to σ^R.

We will now show on an example an algorithm that decides whether a permutation is sorted and, if it is indeed sorted, gives the pre-image. Beginning with $\tau = 6.3.11.1.4.5.2.7.9.8.10.12 \in \mathcal{S}_{12}$, one splits it after each descent: $6|3.11|1.4.5|2.7.9|8.10.12$ then one reads it from right to left, and for each factor one creates the associated tree where the root is the maximum and each node has only a right child. One gets then fives trees (12,10,8), (9,7,2), (5,4,1), (11,3) and (6). And finally one tries to create the associated binary search tree, which is possible if and only if τ is sorted. What is more, by noting σ the word given by a "lower reading" of the final tree, we get $\tau = \Pi(\sigma)$. With our example, we have $\tau = \Pi(6.11.3.12.9.5.4.1.7.2.10.8)$ is sorted.

4. **Notations**

The number of $2\underline{3}1$ patterns in a permutation σ is the number of pairs (i,k) with $i<k$ such that there exists $j \in [i,k]$ with $\sigma(k) < \sigma(i) < \sigma(j)$. Note that the number of $2\underline{3}1$ patterns in a permutation σ, denoted below $\mathrm{INV}(\sigma)$, is the number of inversions of $\Pi(\sigma)$. For instance, the permutation σ of Fig. 1 has four $2\underline{3}1$ patterns (corresponding to the pairs of letters $(2,1)$, $(3,1)$, $(5,4)$ and $(6,4)$) and $\Pi(\sigma)$ has four inversions (given by the same pairs of letters). For $\sigma \in \mathcal{S}_n$, we define $z(\sigma)$ by the largest ℓ such that n occurs before $n-1$ and $n-1$ occurs before $n-2$ and $\cdots$ and $n-(\ell-2)$ occurs before $n-(\ell-1)\}$. For instance, $z(519268374) = 3$. For $m,n \geq 0$, we define the sets $\mathcal{S}_{m,n}$ and $\overline{\mathcal{S}}_{m,n}$ by

$$\mathcal{S}_{m,n} = \{\sigma \in \mathcal{S}_{m+n} : z(\sigma) \geq n\} \qquad \text{and} \qquad \overline{\mathcal{S}}_{m,n} = \{\sigma \in \mathcal{S}_{m+n} : z(\sigma) = n\}.$$

Let $\sigma \in \overline{\mathcal{S}}_{m,n}$ and $\sigma = \sigma^L m \sigma^R$, we note m' the largest letter of σ^R, so we have the factorisation $\sigma = Am'B$. It is this factorisation which allowed the author to find equations verified by the generating functions. We will use the usual notations $[n] = 1 + q + \cdots + q^{n-1} = \frac{1-q^n}{1-q}$ and $[n]! = [1][2]\cdots[n]$. Let $\mathcal{C}$ be a set of permutations. By the *ordinary* (resp. *exponential*) *generating function of* $\mathcal{C}$ we mean the series

$$C(x,y) = \sum_{m,n\geq 0} c_{m,n} x^m y^n, \qquad \text{resp.} \quad C(x,y) = \sum_{m,n\geq 0} c_{m,n} \frac{x^m}{m!} y^n,$$

where $c_{m,n}$ is the number of permutations σ of $\mathcal{C}$ of length $m+n$ such that $z(\sigma) \geq n$. The *ordinary* (resp. *Eulerian*) INV-*generating function of* $\mathcal{C}$ is

$$C(x,y;q) = \sum_{m,n\geq 0} c_{m,n} x^m y^n, \qquad \text{resp.} \quad C(x,y;q) = \sum_{m,n\geq 0} c_{m,n} \frac{x^m}{[m]!} y^n,$$

where $c_{m,n} = \sum_{\sigma\in\mathcal{C}\cap\mathcal{S}_{m,n}} q^{\mathrm{INV}(\sigma)}$. The definition for the inv-*generating function of* $\mathcal{C}$ is similar.

5. Functional Equations

Proposition 1. *The Eulerian* INV*-generating function $A(x,y;q)$ for general permutations is completely characterised by the initial condition $A(0,y;q) = 1/(1-y)$ and the equation*

$$\frac{A(x,y;q) - A(xq,y;q)}{x(1-q)} = [1 + yA(xq,y;q)] \frac{A(x,y;q) - A(x,0;q)}{y}.$$

In the limit $q \to 1$, we find, for the series $A(x,y)$, the initial condition $A(0,y) = 1/(1-y)$ and the equation

$$\frac{\partial A}{\partial x}(x,y) = [1 + yA(x,y)] \frac{A(x,y) - A(x,0)}{y}.$$

Proposition 2. *The ordinary generating function $B(x,y)$ for one-stack sortable permutations is completely characterised by the equation*

$$B(x,y) = \frac{1}{1-y} + \frac{x}{1-y} \frac{B(x,y) - B(x,0)}{y}.$$

Proposition 3. *The ordinary* INV*-generating function $C(x,y)$ for two-stack sortable permutations is completely characterised by the equation*

$$C(x,y;q) = \frac{1}{1-y} + x\,[1 + yC(xq,y;q)] \frac{C(x,y;q) - C(x,0;q)}{y}.$$

Proposition 4. *The Eulerian* inv*-generating function $D(x,y;q)$ for sorted permutations is completely characterised by the initial condition $D(0,y;q) = 1/(1-y)$ and the equation*

$$\frac{D(x,y;q) - D(xq,y;q)}{x(1-q)} = (1-y)\,[1 + yD(xq,y;q)] \frac{D(x,y;q) - D(x,0;q)}{y}.$$

In the limit $q \to 1$, we obtain for the exponential generating function $D(x,y)$ the initial condition $D(0,y) = 1/(1-y)$ and the equation

$$\frac{\partial D}{\partial x}(x,y) = (1-y)\,[1 + yD(x,y)] \frac{D(x,y) - D(x,0)}{y}.$$

Proposition 5. *The ordinary* inv*-generating function $E(x,y;q)$ for sorted and sortable permutations is completely characterised by the equation*

$$E(x,y;q) = \frac{1}{1-y} + x(1-y)\,[1 + yE(xq,y;q)] \frac{E(x,y;q) - E(x,0;q)}{y}.$$

Remarks. The ordinary length generating function $B(x,0)$ for one-stack sortable permutations can be solved by the kernel method. The equations of Propositions 3 (two-stack sortable permutations) and 5 (sorted and sortable permutations) can be solved when $q = 1$ via the so-called *quadratic method*, which is due to Brown [6, section 2.9.1]. There is no known q-analogue of this method! On the other hand, the equations for the general permutations and for sorted permutations can be "solved" as we will see in the next section.

6. Solving Equations with a q-Derivative

Both equations are of the following form:

$$\frac{\partial F}{\partial x}(x,y) = c(y)\,[1+yF(x,y)]\,\frac{F(x,y)-F(x,0)}{y}, \tag{1}$$

where $c(y)=1$ for general permutations and $c(y)=1-y$ for sorted permutations.

One uses the two following results in order to "solve" these equations.

Lemma 1 (Bernoulli linearisation)**.** *Let $F(x,y) \in \mathbb{R}(y)[[x]]$ be defined by the initial condition $F(0,y)=1/(1-y)$ and Eq. (1), with $c(y)=1$ or $c(y)=1-y$. Let $G(x,y)$ be the following series of $\mathbb{R}(y)[[x]]$:*

$$G(x,y) = \frac{1}{c(y)\,[1+yF(x,y)]}.$$

Then $G(0,y)=(1-y)/c(y)$ and

$$y\frac{\partial G}{\partial x}(x,y) - c(y)\,[1+yF(x,0)]\,G(x,y) + 1 = 0.$$

Most importantly, $G(x,y)$ has polynomial coefficients *in y, i.e., $G(x,y) \in \mathbb{R}[y][[x]]$.*

Lemma 2 (Laplace transform)**.** *Let $h(x,y) \in \mathbb{R}[y][[x]]$ be a formal series in x with polynomial coefficients in y. Let $G(x,y)$ be the series of $\mathbb{R}(y)[[x]]$ defined by an initial condition $G(0,y) \in \mathbb{R}(y)$ and the differential equation:*

$$y\frac{\partial G}{\partial x}(x,y) - [1+yh(x,y)]\,G(x,y) + 1 = 0.$$

Let

$$H(x,y) = \exp\left[-\int_0^x h(u,y)du\right] = \sum_{i\geq 0} H_i(y)\frac{x^i}{i!}.$$

Then the coefficients of $G(x,y)$ are polynomials in y if and only if $G(0,y) \in \mathbb{R}[y]$ and

$$\sum_{i\geq 0} H_i(y)y^i = G(0,y).$$

In other words, the Laplace transform of $H(x,y)$ with respect to x is exactly $G(0,y)$ when evaluated at $x=y$:

$$\frac{1}{y}\int_0^\infty e^{-u/y}H(u,y)du = G(0,y).$$

For *general permutations*, with $c(y)=1$, one gets

$$F(x,y) = A(x,y) = \frac{1}{1-x-y}.$$

For *sorted permutations*, with $c(y)=1-y$, the series $F(x,y)$ is the exponential generating function $D(x,y)$ for sorted permutations. The series $G(x,y) = 1/\left[(1-y)(1+yD(x,y))\right]$ satisfies (1) with $h(x,y)=(1-y)D(x,0)-1$. Moreover, $G(0,y)=1$. With the notations of Lemma 2, we have:

$$H(x,y) = \exp(x+(y-1)\mathcal{D}(x))$$

where

$$\mathcal{D}(x) = \int_0^x D(u,0)du.$$

Lemma 2 gives the following result.

Proposition 6. *Let*

$$\mathcal{D}(x) = \sum_{m\geq 0} d_{m,0} \frac{x^{m+1}}{(m+1)!}$$

where $d_{m,0}$ is the number of sorted permutations of length m. Then the series $\mathcal{D}(x)$ is completely characterised by the following equation:

$$\frac{1-y}{y} \int_0^\infty e^{-u(1-y)/y} \exp\left[(y-1)\mathcal{D}(u)\right] du = 1-y.$$

In other words, let $K(x,y) = \exp\left[(y-1)\mathcal{D}(x)\right] = \sum_{i\geq 0} K_i(y)x^i/i!$, and let $\hat{K}(x,y) = \sum_{i\geq 0} K_i(y)x^i$ be its Laplace transform with respect to x. Then

$$\hat{K}\left(\frac{y}{1-y}, y\right) = 1-y, \qquad \text{or, equivalently} \quad \hat{K}\left(u, \frac{u}{1+u}\right) = \frac{1}{1+u}.$$

The first coefficients of the series are 1,1,2,5,17,68,326,1780,11033,76028,578290,4803696. One does not know if this series is algebraic, D-finite, ... Thus, the generating function for sorted permutations remains mysterious. Mireille Bousquet-Mélou will give a solving method for the full q-analogue equations in a for coming paper.

Bibliography

[1] Barcucci (Elena), Del Lungo (Alberto), Lanini (S.), Macrì (M.), and Pinzani (Renzo). – The inversion number of some permutations with forbidden subsequences. Proceedings of SOCA'96 Tianjin, 1996, pp. 21–32.

[2] Bousquet-Mélou (Mireille). – A method for the enumeration of various classes of column-convex polygons. *Discrete Mathematics*, vol. 154, n° 1-3, 1996, pp. 1–25.

[3] Bousquet-Mélou (Mireille). – Multi-statistic enumeration of two-stack sortable permutations. *Electronic Journal of Combinatorics*, vol. 5, n° 1, 1998.

[4] Bousquet-Mélou (Mireille). – Sorted and/or sortable permutation. *Preprint, LaBRI*, 1998.

[5] Brown (William G.). – Enumeration of quadrangular dissections of the disk. *Canadian Journal of Mathematics*, vol. 17, 1965, pp. 302–317.

[6] Brown (William G.). – On the existence of square roots in certain rings of power series. *Mathematische Annalen*, vol. 158, 1965, pp. 82–89.

[7] Brown (William G.). – On the enumeration of non-planar maps. *Memoirs of the American Mathematical Society*, vol. 65, 1966, p. 42.

[8] Brown (William G.) and Tutte (William Thomas). – On the enumeration of rooted non-separable planar maps. *Canadian Journal of Mathematics*, vol. 16, 1964, pp. 572–577.

[9] Cori (Robert), Jacquard (B.), and Schaeffer (Gilles). – Description trees for some families of planar maps. In *Formal Power Series and Algebraic Combinatorics*, pp. 196–208. – 1997. Proceedings of the 9th Conference, Vienna.

[10] Cori (Robert) and Richard (Jean). – Énumération des graphes planaires à l'aide des séries formelles en variables non commutatives. *Discrete Mathematics*, vol. 2, 1972, pp. 115–162.

[11] Dulucq (Serge), Gire (S.), and West (Julian). – Permutations with forbidden subsequences and nonseparable planar maps. *Discrete Mathematics*, vol. 153, n° 1-3, 1996, pp. 85–103.

[12] Knuth (Donald E.). – *The Art of Computer Programming.* – Addison-Wesley, 1973, vol. 1.

[13] Rawlings (Don). – The Euler-Catalan identity. *European Journal of Combinatorics*, vol. 9, n° 1, 1988, pp. 53–60.

[14] West (Julian). – *Permutations with restricted subsequences and stack-sortable permutations.* – PhD thesis, MIT, 1990.

[15] Zeilberger (Doron). – A proof of Julian West's conjecture that the number of two-stack-sortable permutations of length n is $2(3n)!/((n+1)!(2n+1)!)$. *Discrete Mathematics*, vol. 102, n° 1, 1992, pp. 85–93.

From Motzkin to Catalan Permutations: a "Discrete Continuity"

Renzo Pinzani
DSI, Università degli Studi di Firenze, Italy

March 2, 1998

[summary by Alain Denise]

Abstract

Let S^j be the set of all permutations with forbidden sequences 321 and $(j+2)\bar{1}(j+3)2\cdots(j+1)$. We give the generating function of S^j according to three parameters: the length of the permutations, their number of right minima, and their number of inversions. The cases $j=1$ and $j=2$ give the generating functions of the well-known Motzkin numbers and left-Motzkin numbers, while the case $j=\infty$ leads to the Catalan numbers. This is joint work with E. Barcucci, A. Del Lungo and E. Pergola.

1. Notations and Definitions

Definition 1. Let S_n be the set of permutations of $[n]$. A permutation $\pi \in S_n$ is said to contain a subsequence of type $\tau \in S_k$ if there exists a sequence of indices $1 \le i_{\tau(1)} < i_{\tau(2)} < \cdots < i_{\tau(k)} \le n$ such that $\pi(i_1) < \pi(i_2) < \cdots < \pi(i_k)$. We denote the set of permutations of S_n not containing subsequences of type τ by $S_n(\tau)$.

Example. The permutation 6145732 belongs to $S_7(2413)$ because all its subsequences of length 4 are not of type 2413. This permutation does not belong to $S_7(3142)$ because there exist subsequences of type 3142: $\pi(1)\pi(2)\pi(5)\pi(6) = 6173$, $\pi(1)\pi(2)\pi(5)\pi(7) = 6172$.

Definition 2. A *barred* permutation of $[k]$ is a permutation of S_k having a bar over one of its elements. If $\bar{\tau}$ is a barred permutation, we note τ the permutation on $[k]$ identical to $\bar{\tau}$ but unbarred, and $\hat{\tau}$ the permutation of $[k-1]$ made up of the $k-1$ unbarred elements of $\bar{\tau}$, rearranged to get a permutation on $[k-1]$.

Definition 3. We say that a permutation $\pi \in S_n$ contains a type $\bar{\tau}$ subsequence if π contains a type $\hat{\tau}$ subsequence that, in turn, is not a type τ subsequence. We denote the set of permutations of S_n not containing type $\bar{\tau}$ subsequences by $S_n(\bar{\tau})$.

Example. If $\bar{\tau} = 41\bar{3}52$, then $\tau = 41352$ and $\hat{\tau} = 3142$. The permutation $\pi = 6145732$ belongs to $S_7(\bar{\tau})$ because all its subsequences of type $\hat{\tau}$: $\pi(1)\pi(2)\pi(5)\pi(6) = 6173$, and $\pi(1)\pi(2)\pi(5)\pi(7) = 6172$ are subsequences of $\pi(1)\pi(2)\pi(3)\pi(5)\pi(6) = 61473$ and $\pi(1)\pi(2)\pi(3)\pi(5)\pi(7) = 61472$, which are of type τ.

Given some barred of unbarred permutations $\tau_1 \in S_{k_1}, \ldots, \tau_p \in S_{k_p}$ of, we denote the set $S_n(\tau_1) \cap \cdots \cap S_n(\tau_p)$ by $S_n(\tau_1, \ldots, \tau_p)$. We call the family $F = \{\tau_1, \ldots, \tau_p\}$ a *family of forbidden subsequences,* the set $S_n(F)$ a *family of permutations with forbidden subsequences.*

Example. The permutation $\pi = 6145732$ belongs to $S_7(2413, 41\bar{3}52)$.

Let $\pi \in S_n$. We denote the position lying on the left of $\pi(1)$ by s_0, the position lying between $\pi(i)$,$\pi(i+1)$, $1 \leq i \leq n-1$, by s_i and the position lying on the right of $\pi(n)$ by s_n. These positions $s_0, s_1, \ldots, s_{n-1}, s_n$ are called the *sites* of π.

Definition 4. Let $F = \{\tau_1, \ldots, \tau_p\}$. A site s_i $(0 \leq i \leq n)$ of a permutation $\pi \in S_n(F)$ is said to be *active* if the insertion of $(n+1)$ into s_i gives a permutation belonging to the set $S_{n+1}(F)$; otherwise the site is said to be *inactive*.

Definition 5. Let $\pi \in S_n$. The pair (i,j) is an *inversion* if $\pi(i) > \pi(j)$. An element $\pi(i)$ is a *right minimum* if $\pi(i) < \pi(j)$, $\forall j \in [i+1, n]$.

Example. The permutation $\pi = 6145732$ has twelve inversions:

$$(1,2)(1,3)(1,4)(1,6)(1,7)(3,6)(3,7)(4,6)(4,7)(5,6)(5,7)(6,7)$$

and two right minima: $\pi(2) = 1$ and $\pi(7) = 2$.

2. Succession Rules and Generating Trees

In this section we briefly describe the tools used to deduce our enumerative results, that is succession rules and generating trees; they were introduced in [1] for the study of Baxter permutations and further applied to the study of permutations with forbidden subsequences by others (see [2] for example).

Definition 6. A *generating tree* is a rooted, labeled tree having the property that the labels of the set of children of each node v can be determined from the label of v itself. Thus, any particular generating tree can be specified by a recursive definition consisting in:

1. *the basis:* the label of the root,
2. *the inductive step:* a set of succession rules that yield a multi-set of labeled children depending solely on the label of the parent.

A succession rule contains at least the information about the number of children. Let τ be a forbidden subsequence. Following the idea developed in [1], the generating tree for τ-avoiding permutations is a rooted tree such that the nodes on level n are exactly the elements of $S_n(\tau)$; the children of a permutation $\pi = \pi(1) \cdots \pi(n)$ are all the τ free permutations obtained by inserting $(n+1)$ into π. Labels must be assigned to the nodes and they record the number of children of a given node.

Example (Catalan tree and 123-avoiding permutations).

$$\begin{cases} \text{basis:} & (2) \\ \text{inductive step:} & (k) \to (k+1)(2)\cdots(k). \end{cases}$$

The permutation of length one has two active sites (*basis*). Let $\pi = \pi(1) \cdots \pi(n) \in S_n(123)$; and k, $2 \leq k \leq n$, be the minimum index in π such that $i_1 < k$ exists and $\pi(i_1) < \pi(k)$; then the active sites of π are $s_0, \ldots, s_{k-1}$. The insertion of $(n+1)$ into each other site on the right of s_{k-1} gives the subsequence $\pi(i_1)\pi(k)(n+1)$ that is forbidden. This means that the active sites of π are all the ones lying between the elements of π constituting the longest initial decreasing subsequence. If π has k active sites then its longest initial decreasing subsequence has length $(k-1)$. The permutation obtained by inserting $(n+1)$ into s_0 give a new permutation with $(k+1)$ active sites; the permutation obtained by inserting $(n+1)$ into s_i, $1 \leq i \leq k-1$, gives $(i+1)$ active sites, (*inductive step*). The generating tree representing 123-avoiding permutations can be obtained by developing the above rule and by labelling each permutation with the right label (k) (see figure 1).

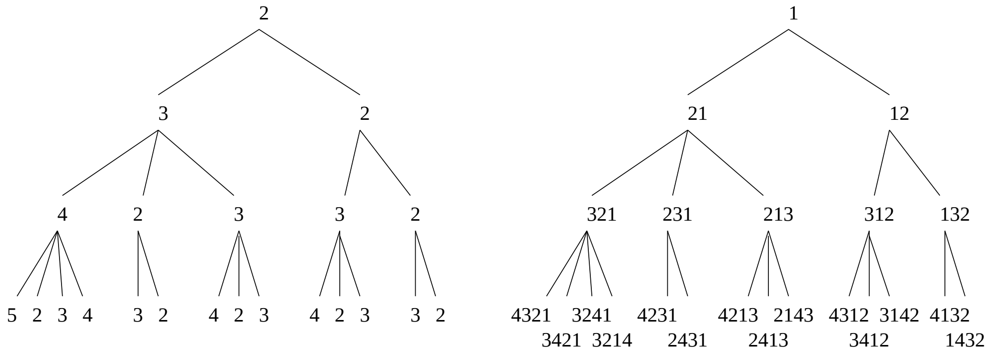


FIGURE 1. The generating tree of 123-avoiding permutations. (Left: nodes labelled by the numbers of active sites. Right: nodes labelled by the permutations.)

Example (Schröder tree and $(1234, 2134)$-avoiding permutations).

$$\begin{cases} \text{basis:} & (2) \\ \text{inductive step:} & (k) \to (k+1)(k+1)(3)\cdots(k). \end{cases}$$

The permutation of length one has two active sites (*basis*). Let $\pi = \pi(1)\cdots\pi(n) \in S_n(1234, 2134)$ and k, $3 \le k \le n$, be the minimum index in π such that there exist $i_1 < i_2 < k$ for which $\pi(i_1)\pi(i_2)\pi(k)$ is of type 123, or 213; then the active sites of π are $s_0, \ldots, s_{k-1}$. The insertion of $(n+1)$ into each other site $s_k, \ldots, s_n$ gives at least one of the forbidden subsequences $1234, 2134$. Let π be a permutation with k active sites; the permutations obtained by inserting $(n+1)$ into s_0 and s_1 have $(k+1)$ active sites; the permutation obtained by inserting $(n+1)$ into s_i, $2 \le i \le k-1$, has $(i+1)$ active sites; each other site gives at least one of the two forbidden subsequences because $(n+1)$ has at least two smaller elements on its left (*inductive step*).

3. Permutations with one Forbidden Subsequence of Increasing Length

Let

$$S^j = \bigcup_{n \ge 1} S_n(321, (j+2)\bar{1}(j+3)2\cdots(j+1)).$$

Given a permutation $\pi \in S^j$, we denote its length by $n(\pi)$, the number of its right minima by $m(\pi)$, the number of its inversions by $i(\pi)$. The generating function of S^j according to the above mentioned parameters is the following:

$$S^j(x, y, q) = \sum_{\pi \in S^j} x^{n(\pi)} y^{m(\pi)} q^{i(\pi)}.$$

Note that the permutation of length one has two active sites and a permutation π having k active sites gives k permutations with $(k)\cdots(j)(j)\cdots(2)(k+1)$ active sites respectively so the rule that describe the active sites changes has the form:

$$\begin{cases} (2) \\ (k) \to (k-1)\cdots(j)(j)\cdots(2)(k+1). \end{cases}$$

Now we can present our main result concerning the generating series $S^j(x, y, q)$. One can observe (for example by setting $j = 1, 2, 3, \ldots$ and then $j = \infty$ in $S^j(x, 1, 1)$, or by means of bijections with other combinatorial structures), that the classes of permutations described here are enumerated by numbers lying between the Motzkin and the Catalan numbers (see figure 1). We view the obtained

Index	Rule	Family of permutations	First coeffs.
$j=1$	$\begin{cases}(2)\\(k)\rightarrow(k-1)\cdots(1)(k+1)\end{cases}$	$S_n^1(321,3\bar{1}42)$	1,2,4,9,21, ...
$j=2$	$\begin{cases}(2)\\(k)\rightarrow(k-1)\cdots(2)(2)(k+1)\end{cases}$	$S_n^2(321,4\bar{1}523)$	1,2,5,13,35, ...
$j=3$	$\begin{cases}(2)\\(k)\rightarrow(k-1)\cdots(3)(3)(2)(k+1)\end{cases}$	$S_n^3(321,5\bar{1}6234)$	1,2,5,14,41, ...
j	$\begin{cases}(2)\\(k)\rightarrow(k-1)\cdots(j)(j)\cdots(2)(k+1)\end{cases}$	$S_n^j(321,(j+2)\bar{1}(j+3)$ $23\cdots(j+1))$	1,2,5,14,42, ...
$j=\infty$	$\begin{cases}(2)\\(k)\rightarrow(k)\cdots(2)(k+1)\end{cases}$	$S_n^\infty(321)$	1,2,5,14,42, ...

TABLE 1. A few permutations of S^j.

sequences of numbers as providing a "discrete continuity" between the Motzkin and the Catalan sequences.

Theorem 1. *The generating function of $S^j(x,y,q)$ is such that:*

$$S^2(x,y,q)=\frac{xy(1+f(x,y,q))}{1-xq-xq(1+q)f(x,y,q)};\qquad \textit{with}\quad f(x,y,q)=y\frac{\sum_{n\geq 0}\frac{(-1)^n x^{n+1}q^{n(j+1)}}{(xy,q)_{n+1}(q,q)_n}}{\sum_{n\geq 0}\frac{(-1)^n x^n q^{n(j+1)}}{(xy,q)_n(q,q)_n}},$$

$$S^j(x,y,q)=\frac{xy(1-xq^2)\Delta_j(x,y,q)}{(1-xq)(1-xq^2)\Delta_j(x,y,q)+xy\Delta_{j-1}(x,y,q)},\qquad j\geq 3,$$

where $(a,q)_n=\prod_{k=0}^{n-1}\left(1-aq^k\right)$, *and with* $\Delta_j(x,y,q)=c_1(x,y,q)\lambda_1^j(x,y,q)+c_2(x,y,q)\lambda_2^j(x,y,q)$ *where*

$$\lambda_1(x,y,q)=\frac{1}{2}\left[-\left(1+\frac{xy}{1-xq^2}\right)+\sqrt{\left(1+\frac{xy}{1-xq^2}\right)^2-\frac{4xy}{(1-xq^2)(1-xq^3)}}\right],$$

$$\lambda_2(x,y,q)=\frac{1}{2}\left[-\left(1+\frac{xy}{1-xq^2}\right)-\sqrt{\left(1+\frac{xy}{1-xq^2}\right)^2-\frac{4xy}{(1-xq^2)(1-xq^3)}}\right].$$

The functions $c_1(x,y,q),c_2(x,y,q)$ satisfy:

$$c_1(x,y,q)\lambda_1^2(x,y,q)+c_2(x,y,q)\lambda_2^2(x,y,q)=1+f(x,y,q)$$

$$c_1(x,y,q)\lambda_1^3(x,y,q)+c_2(x,y,q)\lambda_2^3(x,y,q)=f(x,y,q)\frac{xq^{j-1}(1+q)-xy}{1-xq^{j-1}}-\frac{1+xy-xq^{j-1}}{1-xq^{j-1}}.$$

Bibliography

[1] Chung (F. R. K.), Graham (R. L.), Hoggatt, V. E. (Jr.), and Kleiman (M.). – The number of Baxter permutations. *Journal of Combinatorial Theory. Series A*, vol. 24, n° 3, 1978, pp. 382–394.

[2] West (Julian). – Generating trees and forbidden subsequences. *Discrete Mathematics*, vol. 157, n° 1-3, 1996, pp. 363–374. – Proceedings of the 6th Conference on Formal Power Series and Algebraic Combinatorics (New Brunswick, NJ, 1994).

Equations in S_n and Combinatorial Maps

Gilles Schaeffer
LaBRI, Université de Bordeaux I,

November 3, 1997

[summary by Dominique Gouyou-Beauchamps]

This talk presents a joint work with Alain Goupil (LACIM-UQAM, Montréal).

1. Counting Maps

A *partition* $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ is a finite non-increasing sequence of positive integers λ_i such that $\lambda_1 \geq \cdots \geq \lambda_k > 0$. The non-zero terms are called the *parts* of λ and the number k of parts is the *length* of λ, denoted $\ell(\lambda)$. We also write $\lambda = 1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}$ when α_i parts of λ are equal to i $(i = 1, \ldots, n)$. When the sum $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n$, we call n the *weight* of λ and we write $\lambda \vdash n$ or $|\lambda| = n$. The conjugacy classes C_λ of the symmetric group S_n are indexed by partitions of n which are called the cycle types of the permutations $\sigma \in C_\lambda$.

There exit relations between pairs of permutations and maps on oriented surfaces. A *map* (S, G) on a compact oriented surface S without boundary is a graph G together with an embedding of G into S such that connected components of the complement $S \setminus G$ of the embedding of G in S, called the faces of the map, are homeomorphic to discs. Multiple edges are allowed and our maps are rooted, i.e., one edge of G is distinguished. Two maps (S, G) and (S', G') are isomorphic if there exits an orientation-preserving homeomorphism $f : S \to S'$ such that $f(G) = G'$. A map is *bicolored* if its vertices are colored in black or white so that each edge is incident to one vertex of each color. A map is *unicellular* if it has one face. The *type* of a bicolored unicellular map M with n edges is a pair of partitions (λ, μ) whose parts give respective degrees of black and white vertices of M.

Proposition 1 (see [3] for more details)**.** *Bicolored unicellular maps of type (λ, μ) are maps on a compact orientable surface of genus g which satisfy $g = g(\lambda, \mu)$. Moreover, the number $Bi(\lambda, \mu)$ of bicolored unicellular maps of type (λ, μ) with n edges is the number of pairs (σ, τ) such that $\sigma\tau = (1, 2, \ldots, n)$, which is also the coefficient $c_{\lambda,\mu}^{(n)}$ that we study below.*

2. Equations in S_n

Following [7], let $z_\lambda = \prod_i \alpha_i! i^{\alpha_i}$ for a partition $\lambda = 1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}$. Then

$$\mathrm{Card}(C_\lambda) = |C_\lambda| = \frac{n!}{z_\lambda}.$$

Example. The conjugacy class T of transpositions is $T = C_{1^{n-2}2}$ and $|T| = \binom{n}{2} = \frac{n!}{(n-2)!2}$.

In this talk, we are interested with the general problem of computing the number

$$C^{\pi}_{\lambda^1, \ldots, \lambda^m} = \Big| \sum (\lambda^1, \ldots, \lambda^m; \pi) \Big|$$

of solutions $(\alpha_1, \ldots, \alpha_m) \in C_{\lambda^1} \times \cdots \times C_{\lambda^m}$ of the equation $\alpha_1\alpha_2\cdots\alpha_m = \pi$ where π is any fixed permutation of S_n and where $\langle \alpha_1, \ldots, \alpha_m \rangle$ acts transitively on $\{1, 2, \ldots, n\}$.

Example. Factorization of any n-cycle into transpositions

$$C^{(n)}_{T^{n-1}} = |\{(\tau_1, \ldots, \tau_{n-1}) \text{ transpositions such that } \tau_1 \cdots \tau_{n-1} = (1, 2, \ldots, n)\}| = n^{n-2}.$$

If $\alpha \in C_\lambda$ and $\alpha = \tau_1 \cdots \tau_k$, then we have $k \geq n - \ell(\lambda) = \sum_{i=1}^{\ell(\lambda)} (\lambda_i - 1)$ and parity of α is given by parity of $n - \ell(\lambda)$. Thus if $\alpha_1\alpha_2\cdots\alpha_m = \pi$, we have the first necessary condition for existence of solutions in $\sum(\lambda^1, \ldots, \lambda^m; \pi)$:

$$\sum_{i=1}^{m} \left(n - \ell(\lambda^i)\right) \equiv n - \ell(\pi) \bmod 2.$$

If $\langle \alpha_1, \ldots, \alpha_m \rangle$ acts transitively on $\{1, 2, \ldots, n\}$, the underlying graph is connected.

Example. $\tau_1 \cdots \tau_m = 1$. We need $m = 2n - 2$ transpositions: $n - 1$ transpositions to get an n-cycle and one connected component, and $n - 1$ transpositions to return to 1.

Proposition 2. *Let $(\alpha_1, \ldots, \alpha_m)$ be in $C_{\lambda^1} \times \cdots \times C_{\lambda^m}$. If $\langle \alpha_1, \ldots, \alpha_m \rangle$ acts transitively and if $\alpha_1 \cdots \alpha_m = 1$, then $\sum_{i=1}^m \left(n - \ell(\lambda^i)\right) \geq 2n - 2$.*

Definition 1. The genus of m partitions $(\lambda^1, \ldots, \lambda^m)$ of weight n is the non negative integer g defined by the equation

$$\sum_{i=1}^{m} \left(n - \ell(\lambda^i)\right) = 2n - 2 + 2g.$$

For non transitive systems, we want to compute the number

$$d^{\pi}_{\lambda^1, \ldots, \lambda^m} = \left|\widehat{\sum}(\lambda^1, \ldots, \lambda^m; \pi)\right|$$

of solutions $(\alpha_1, \ldots, \alpha_m) \in C_{\lambda^1} \times \cdots \times C_{\lambda^m}$ of the equation $\alpha_1\alpha_2\cdots\alpha_m = \pi$ where π is any fixed permutation of S_n.

We remark that $\widehat{\sum}(\lambda^1, \ldots, \lambda^m; \pi) = \operatorname{Set}\left(\sum(\lambda^1, \ldots, \lambda^m; \pi)\right)$. From this observation we deduce the exponential generating function (in the variables $(p_j^{(i)})$, $j \geq 1$, $1 \leq i \leq m$) of $\widehat{\sum}(\lambda^1, \ldots, \lambda^m; \pi)$ for a fixed m:

$$\sum_{n \geq 0} \frac{z^n}{n!} \sum_{\lambda_1, \ldots, \lambda_n, \pi} d^{\pi}_{\lambda^1, \ldots, \lambda^m} P^{(1)}_{\lambda_1} P^{(2)}_{\lambda_2} \cdots P^{(m)}_{\lambda_m} = \exp\left(\sum_{n \geq 1} \frac{z^n}{n!} \sum_{\lambda_1, \ldots, \lambda_n, \pi} c^{\pi}_{\lambda^1, \ldots, \lambda^m} P^{(1)}_{\lambda_1} P^{(2)}_{\lambda_2} \cdots P^{(m)}_{\lambda_m}\right)$$

where $P^{(i)}_\lambda = p^{(i)}_{\lambda_1} \cdots p^{(i)}_{\lambda_k}$. Hence, in order to obtain the generating function, we only have to know all the $d^{\pi}_{\lambda^1, \ldots, \lambda^m}$.

3. Theory of Characters

Detailed proofs for this section can be found in [5, 6].

Theorem 1 (Frobenius formula). *Let G be a finite group. The number of solutions $(g_1, \ldots, g_m) \in C_{\lambda^1} \times \cdots \times C_{\lambda^m}$ of the equation $g_1 \cdots g_m = 1$ is*

$$\frac{|C_1| \cdots |C_m|}{|G|} \sum_{\chi} \frac{\chi(C_1) \cdots \chi(C_m)}{[\chi(1)]^{m-2}}$$

where the sum is extended over the irreducible characters of G.

If G is the symmetric group S_n, the irreducible characters are $\{\chi^\mu\}_{\mu\vdash n}$ and $\chi^\mu(C_\lambda)$ can be computed by the Murnaghan-Nakayama rule

$$\chi^\mu(C_\lambda) = \chi^\mu_\lambda = \sum_{T\in \mathrm{T}(\lambda,\mu)} \prod_{S\in T} (-1)^{h(S)}.$$

Hence theoretically $d^\pi_{\lambda^1,\ldots,\lambda^m}$ can be computed since it can be rewritten as

$$d^\pi_{\lambda^1,\ldots,\lambda^m} = \frac{|C_{\lambda_1}|\cdots|C_{\lambda_m}|}{n!} \sum_{\mu\vdash n} \frac{\chi^\mu_{\lambda_1}\cdots\chi^\mu_{\lambda_m}\chi^\mu_\pi}{[f^\mu]^{m-1}}$$

where f^μ is the number of standard Young tableaux of shape μ. But it is hopeless for $n \geq 15$.

4. **Results for Genus 0**

The following results are known.

Theorem 2 (Dénès theorem). *Factorization of an n-cycle into $n-1$ tranpositions:* $C^{(n)}_{T^{n-1}} = n^{n-2}$.

Theorem 3 (Hurwitz formula). *Factorization of α of cycle-type $(\alpha_1,\alpha_2,\ldots,\alpha_{\ell(\alpha)})$ into a minimal product of $n+\ell(\alpha)-2$ transpositions acting transitively on $\{1,2,\ldots,n\}$:*

$$C^\alpha_{T^{n+\ell(\alpha)-2}} = n^{\ell(\alpha)-3}(n+\ell(\alpha)-2)! \prod_{i=1}^{k} \frac{\alpha_i^{\alpha_i}}{(\alpha_i-1)!}.$$

A new bijective proof without using theory of characters is given in [2].

Theorem 4 (Tree cacti of Goulden and Jackson [4]).

$$C^{(n)}_{\lambda_1,\ldots,\lambda_m} = n^{m-1} \prod_{i=1}^{m} \frac{1}{\ell(\lambda_i)} \binom{\ell(\lambda_i)}{\alpha^i_1,\ldots,\alpha^i_m}$$

$$\textit{with } \lambda^i = 1^{\alpha^i_1} 2^{\alpha^i_2}\cdots n^{\alpha^i_n} \textit{ and minimality: } \sum_{i=1}^{m} (n-\ell(\lambda^i)) = n-1.$$

The proof uses a recursive decomposition of tree cacti and the Lagrange-Good inversion.

5. **Our Main Theorem**

Theorem 5 (A. Goupil and G. Schaeffer). *Factorization of an n-cycle into two permutations of cycle-types λ and μ with $\lambda = (\lambda_1,\ldots,\lambda_k)$, $\mu = (\mu_1,\ldots,\mu_k)$ and $\ell(\lambda)+\ell(\mu) = n+1-2g$:*

$$C^{(n)}_{\lambda,\mu} = \frac{n}{z_\lambda z_\mu 2^{2g}} \sum_{g_1+g_2=g} (\ell(\lambda)-1+2g_1)!(\ell(\mu)-1+2g_2)! S_{g_1}(\lambda) S_{g_2}(\mu)$$

$$\textit{with } S_g(\lambda) = \sum_{i_1+\cdots+i_{\ell(\lambda)}=g} \prod_{k=1}^{\ell(\lambda)} \binom{\lambda_k}{2i_k+1}.$$

$$\text{If } g=0, \qquad C^{(n)}_{\lambda,\mu} = \frac{n(\ell(\lambda)-1)!(\ell(\mu)-1)!}{z_\lambda z_\mu} \prod_{i=1}^{k} \lambda_i \prod_{j=1}^{k} \mu_j.$$

In [1] this simple expression was derived. This coefficient was later interpreted combinatorially by Goulden and Jackson [4] as the number of unicellular rooted bicolored maps with n edges on a surface of genus zero, the vertices of each color having degree distribution given by λ and μ respectively, that is the case where $m = 2$ in theorem 4.

$$\text{If } g = 1, \qquad C^{(n)}_{\lambda,\mu} = \frac{n(\ell(\lambda)-1)!(\ell(\mu)-1)!}{2z_\lambda z_\mu}\left[\binom{\ell(\lambda)+1}{2}\sum_{i=1}^{k}\binom{\lambda_i}{3} + \binom{\ell(\mu)+1}{2}\sum_{i=1}^{k}\binom{\mu_i}{3}\right].$$

Survey of the proof of Theorem 5:

1. Using explicit expressions for characters of the symmetric group, we give the following formula

$$c^{(n)}_{\lambda,\mu} = \frac{n}{z_\lambda z_\mu}\sum_{r=0}^{n-1}(-1)^r r!(n-1-r)!\chi_\lambda^{1^r(n-r)}\chi_\mu^{1^r(n-r)}. \tag{1}$$

2. The evaluation of some characters are given as weighted summations over set of "quasi-painted diagrams".
3. We use a bijection to replace quasi-painted diagrams by properly "painted diagrams" and we rewrite Formula (1) as a weighted summation over some "painted diagram matchings".
4. The introduction of "connected components" of diagram matchings allows to set apart the diagram matching from its painting and to show that the weight depends only on the painting. This is used to apply a sign reversing involution.
5. As expected, the fix-points yield positive contributions. These contributions count "colorings" of the diagram matchings.
6. We show that colored diagrams are enumerated by formula of Theorem 5.

6. Corollary for Genus > 0

$$C^{(n)}_{T^{n-1+2g}} = \frac{n^{n-2+2g}}{(n-1)!2^{2g}}\sum_{c_1,\ldots,c_{n-1}}\binom{n-1+2g}{c_1,\ldots,c_{n-1}} \sim_{n\to\infty} \frac{n^{n-2+5g}}{g!24^g}$$

where the sum is taken over the odd c_i such that $\sum c_i = n-1+2g$.

Bibliography

[1] Bédard (François) and Goupil (Alain). – The poset of conjugacy classes and decomposition of products in the symmetric group. *Canadian Mathematical Bulletin*, vol. 35, n° 2, 1992, pp. 152–160.

[2] Bousquet-Mélou (M.) and Schaeffer (G.). – Enumeration of planar constellations. *Advances in Applied Mathematics*, 1998. – To appear.

[3] Cori (Robert) and Machì (Antonio). – Maps, hypermaps and their automorphisms: a survey. I, II, III. *Expositiones Mathematicae*, vol. 10, n° 5, 1992, pp. 403–427, 429–447, 449–467.

[4] Goulden (I. P.) and Jackson (D. M.). – The combinatorial relationship between trees, cacti and certain connection coefficients for the symmetric group. *European Journal of Combinatorics*, vol. 13, n° 5, 1992, pp. 357–365.

[5] Goupil (Alain). – On products of conjugacy classes of the symmetric group. *Discrete Mathematics*, vol. 79, n° 1, 1989/90, pp. 49–57.

[6] Jackson (D. M.). – Counting cycles in permutations by group characters, with an application to a topological problem. *Transactions of the American Mathematical Society*, vol. 299, n° 2, 1987, pp. 785–801.

[7] Macdonald (I. G.). – *Symmetric functions and Hall polynomials.* – The Clarendon Press Oxford University Press, New York, 1995, second edition, *Oxford Mathematical Monographs*, x+475p. With contributions by A. Zelevinsky, Oxford Science Publications.

Multivariate Lagrange Inversion

Bruce Richmond
University of Waterloo, Canada

May 25, 1998

[summary by Danièle Gardy]

Abstract

A new formulation of Lagrange inversion for several variables will be described which does not involve a determinant. This formulation is convenient for the asymptotic investigation of numbers defined by Lagrange inversion. Examples of tree problems where the number of vertices of degree k are counted and where vertices are 2-colored will be given. Non-crossing partitions give another example and the Meir-Moon formula for powers of an inversion is a special case.

1. Running Example

Consider a rooted plane tree where internal vertices can have two or three sons and are green or red, according to the following rules: (an example of such a tree is given below.)

- a green vertex has three children; one is red and the other two are green;
- a red vertex has two children, one of each color, and the left one is red.

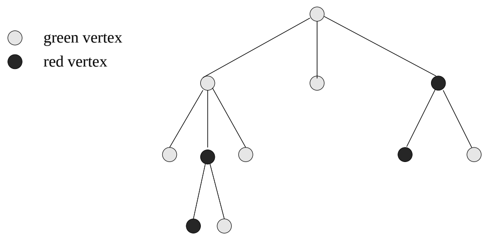
Enumeration of such trees is best done by taking into account the colors of the vertices: let x_1 and x_2 mark the green and red vertices, and define $w_1(x_1, x_2)$ and $w_2(x_1, x_2)$ as the functions enumerating the trees whose root is green (resp. red). These functions satisfy the system of equations

$$w_1(x_1, x_2) = x_1(1 + 3w_1^2 w_2); \qquad w_2(x_1, x_2) = x_2(1 + w_1 w_2).$$

Introducing the vectors $\underline{x} = (x_1, x_2)$ and $\underline{w} = (w_1, w_2)$ and the functions $f_1(\underline{w}) = 1 + 3w_1^2 w_2$ and $f_2(\underline{w}) = 1 + w_1 w_2$, one obtains the system $w_1(\underline{x}) = x_1 f_1(\underline{w}); w_2(\underline{x}) = x_2 f_2(\underline{w})$. Such equations are very similar to those that can be solved in one dimension by Lagrange inversion, and it is natural to try and solve them with a suitable extension.

2. Multivariate Lagrange Inversion

In one dimension, Lagrange inversion is used for implicit equations of the type $w(x) = xf(w(x))$, with $f(0) \neq 0$: It relates the coefficients of a solution $w(x)$, or of a function of $w(x)$, as formal



power series, to the coefficients of the simpler function f:

$$[x^n]w(x) = \frac{1}{n}[t^{n-1}]f(t)^n; \qquad [x^n]g(w(x)) = \frac{1}{n}[t^{n-1}]g'(t)f^n(t).$$

Extensions to the multivariate case have been considered for some time; surveys can be found in the paper written some twelve years back by Gessel [6], or in the recent book by Bergeron, Labelle and Leroux [4]. The version presented below is due to Good [7]:

Theorem 1. *Let $\underline{x}$ be a d-dimensional vector, $g(\underline{x})$ and $f_i(\underline{x})$ $(1 \le i \le d)$ be formal power series in $\underline{x}$, s.t. $f_i(\underline{0}) \neq 0$. Then the equations $w_i = x_i f_i(\underline{w})$ uniquely determine the w_i as formal power series in $\underline{x}$, and*

$$[\underline{t}^{\underline{n}}]g(\underline{w}(\underline{t})) = [\underline{x}^{\underline{n}}]\left(g(\underline{x})\underline{f}^{\underline{n}}(\underline{x})\left|\left|\delta_{i,j} - \frac{x_i \partial f_j(\underline{x})}{f_j(\underline{x})\partial x_i}\right|\right|\right),$$

with $\delta_{i,j}$ the Kronecker symbol, $||A||$ the determinant of the matrix A, $\underline{f} = (f_1, \ldots, f_d)$, and $\underline{f}^{\underline{n}} = f_1^{n_1} \cdots f_d^{n_d}$.

The determinant in this formula leads to trouble when one tries to get asymptotic information from it. Let us consider the univariate case to see what the problem is.

For $d = 1$, Good's formula applied to the equation $w(x) = xf(w(x))$ gives an identity equivalent to the one presented above:

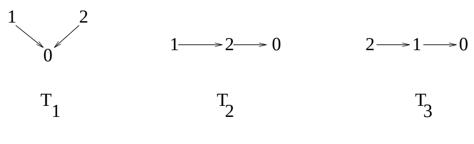
$$[x^n]w(x) = [t^{n-1}]\left(f^n(t)\left(1 - t\frac{f'(t)}{f(t)}\right)\right). \tag{1}$$

When one wishes to obtain asymptotics, a natural tool is the saddle-point method, well suited to approximating coefficients of (variations on) large powers of functions; see for example [5] for a summary of results in this area. The idea is to use Cauchy's formula $[z^n]F(z) = \oint F(z)z^{-n-1}dz$, for $F(z) = f(z)^n(1 - zf'(z)/f(z))$, with an integration path that is a circle going through the saddle-point ρ_0; ρ_0 is itself is a perturbation of the saddle-point ρ_1 that appears in the evaluation of the simpler coefficient $[x^n]f^n(x)$. Now ρ_1 is defined as the solution of the equation $1 - xf'(x)/f(x) = 0$, i.e. the integrand of the right part of (1) becomes zero close to ρ_0!

With care, it should be possible to work this out for one variable, but the outlook for a multi-dimensional extension is not favorable, as we can expect cancellation of the determinant close to the integration paths. Instead, Bender and Richmond have proposed a new multivariate version, better suited to asymptotics; this formula will use the derivatives of a vector wrt a directed graph.

3. Differentiating a Vector wrt a Directed Graph

To define the partial of a vector relative to a directed graph, consider all trees with vertices $0, 1, \ldots, d$ and edges directed to 0. There are $(d+1)^{d-1}$ such trees; for example for $d = 2$ there are three trees:



Now the derivative of a $(d+1)$-dimensional function $\underline{f}$ according to such a tree is a product on $(d+1)$ terms, where f_i is differentiated according to the incoming edges into the vertex labelled by i; this is best explained on the above example, with $\underline{f} = (f_0, f_1, f_2)$:[1]

[1]Although the definition is more general, trees are the only graphs considered here.

$$\frac{\partial \underline{f}}{\partial T_1} = \frac{\partial^2 f_0}{\partial x_1 \partial x_2} \cdot f_1 \cdot f_2; \qquad \frac{\partial \underline{f}}{\partial T_2} = \frac{\partial f_0}{\partial x_2} \cdot f_1 \cdot \frac{\partial f_2}{\partial x_1}; \qquad \frac{\partial \underline{f}}{\partial T_3} = \frac{\partial f_0}{\partial x_1} \cdot \frac{\partial f_2}{\partial x_2} \cdot f_2.$$

4. **The New Inversion Formula**

Theorem 2. *Under the assumptions of the former theorem,*

$$[\underline{t}^{\underline{n}}]g(\underline{w}(\underline{t})) = \left(\prod_{i=1}^{d} n_i\right)^{-1} [\underline{x}^{\underline{n}-\underline{1}}] \sum_T \frac{\partial(g, f_1^{n_1}, \dots, f_d^{n_d})}{\partial T},$$

where the sum is on the set of trees with $d+1$ vertices.

Proof. This result is proven in [3]; it relies on the simple formula $n[x^{n-1}]f = [x^n]\partial f/\partial x$ and on the expansion of a determinant. The terms are all positive as soon as the functions f_i and g have positive coefficients; hence the coefficient $[\underline{t}^{\underline{n}}]g(\underline{w}(\underline{t}))$, as a sum of $(d+1)^{d-1}$ such terms, is itself positive and there are no more cancellations. □

What do we obtain for the first values of d? For $d=1$, the only tree is $1 \to 0$ and one gets back the classical formula. For $d=2$, $g(t_1,t_2)$ is a function of two variables and

$$\begin{aligned}
[x_1^{n_1} x_2^{n_2}]g(w_1(x_1,x_2), w_2(x_1,x_2)) &= \frac{1}{n_1 n_2}[t_1^{n_1-1} t_2^{n_2-1}] \sum_{T \in \{T_0, T_1, T_2\}} \frac{\partial(g, f_1^{n_1}, f_2^{n_2})}{\partial T} \\
&= \frac{1}{n_1 n_2}[t_1^{n_1-1} t_2^{n_2-1}] \left(\frac{\partial^2 g}{\partial t_1 \partial t_2} f_1^{n_1} f_2^{n_2} + \frac{\partial g}{\partial t_2} f_1^{n_1} \frac{\partial (f_2^{n_2})}{\partial t_1} + \frac{\partial g}{\partial t_1} \frac{\partial (f_1^{n_1})}{\partial t_2} f_2^{n_2} \right) \\
&= \frac{1}{(n_1-1)(n_2-1)} [t_1^{n_1} t_2^{n_2}] \left(f_1^{n_1} f_2^{n_2} h \right),
\end{aligned}$$

with (f_1 and f_2 are strictly positive at the saddle-points)

$$h := \frac{\partial^2 g}{\partial t_1 \partial t_2} + n_2 \frac{\partial g}{\partial t_2} \frac{\partial f_2}{\partial t_1} \frac{1}{f_2} + n_1 \frac{\partial g}{\partial t_1} \frac{\partial f_1}{\partial t_2} \frac{1}{f_1}.$$

For general d, there is no determinant here, but a finite (although large!) sum of terms, each of which can be evaluated individually. The asymptotic value of $[\underline{t}^{\underline{n}}]g(w(\underline{x}))$ is obtained by adding the individual asymptotic values of the $(d+1)^{d-1}$ terms.

It is possible to obtain a univariate local limit theorem for the number of red vertices in trees having a fixed number of vertices, or a bivariate local limit theorem for the joint distribution of the numbers of red and green vertices.

5. **Local Limit Theorem**

The usual approach towards a limiting theorem is through the covariance matrix (see for example a former paper by the same authors [1]); checking the non-degeneracy of this matrix leads to intricate conditions, which the authors try to bypass, by requiring instead the existence of a multivariate saddle-point. A local limit theorem holds whenever the functions $g(\underline{x})$ and $f_i(\underline{x})$ $(1 \le i \le d)$ are analytic; there is also an existence condition on the exponents of the variables in the functions whose coefficients we are studying. Formally, this involves the lattice generated by the exponents $\underline{k}$ for which the coefficient of $\underline{t}^{\underline{k}}$ in f_i is not zero; see [2] for a precise formulation.

For example, for the colored trees presented in Section 1, the only non-zero coefficients are obtained, besides $\underline{k} = (0,0)$, for $\underline{k} = (2,1)$ in f_1, and for $\underline{k} = (1,1)$ in f_2. The lattice generated by $\{(1,1),(2,1)\}$ is $\mathbb{N}^2$; hence all the terms $t_1^{i_1} t_2^{i_2}$ will appear in the function $f_1^{k_1} f_2^{k_2}$.

The saddle-point condition is that we should be able to solve the system of d equations $\{k_i = \sum_{1\le l\le d} k_l \partial \log f_l / \partial \log \gamma_i\}$ (with $\gamma_i = e^{s_i}$).

We give the equations below for two variables, the better to understand what is going on, but it should be understood that it is more general and applies to d dimensions.

At some point, we have to compute a coefficient $[t_1^{n_1} t_2^{n_2}](h f_1^{n_1} f_2^{n_2})$, where the functions h, f_1 and f_2 are on the variables t_1 and t_2. The way to do this is through a saddle-point approximation; more specifically we shall look at $[t_1^{k_1} t_2^{k_2}](h f_1^{n_1} f_2^{n_2})$ for k_1 and k_2 of the same order as n_1 and n_2, but not necessarily equal. This coefficient can be written, by Cauchy's formula, as $\frac{1}{(2i\pi)^2}\oint\oint e^{h(t_1,t_2)} dt_1 dt_2$, with $h = n_1 \log f_1 + n_2 \log f_2 - k_1 \log t_1 - k_2 \log t_2$. Now the saddle-points are defined by the two equations $\partial h/\partial t_1 = 0$ and $\partial h/\partial t_2 = 0$, which give the two-dimensional system

$$k_1 = n_1 t_1 \frac{\partial f_1}{\partial t_1}\frac{1}{f_1} + n_2 t_1 \frac{\partial f_2}{\partial t_1}\frac{1}{f_2}; \qquad k_2 = n_1 t_2 \frac{\partial f_1}{\partial t_2}\frac{1}{f_1} + n_2 t_2 \frac{\partial f_2}{\partial t_2}\frac{1}{f_2}.$$

Applied to our running example, this gives the system in t_1 and t_2

$$k_1 = n_1 \frac{6t_1^2 t_2}{1+3t_1^2 t_2} + n_2 \frac{t_1 t_2}{1+t_1 t_2}; \qquad k_2 = n_1 \frac{3t_1^2 t_2}{1+3t_1^2 t_2} + n_2 \frac{t_1 t_2}{1+t_1 t_2}.$$

Define $\rho := k_1/k_2$; $\rho \in]1,2[$. Solving, we get

$$t_1 = \frac{(\rho-1)^2}{3(2-\rho)} =: r_1; \qquad t_2 = \frac{3(2-\rho)^2}{(\rho-1)^3} =: r_2.$$

This gives $(k_1,k_2) = n(\rho/(1+\rho), 1/(1+\rho))$. The covariance matrix is obtained by differentiation of $\log f$, where $f := f_1^{n_1} f_2^{n_2}$, with f_1 and f_2 defined in Section 1. For example $B_{1,1}$ is the value of $t_1 \partial(\log f)/\partial t_1 + t_1^2 \partial^2(\log f)/\partial t_1^2$, taken at the point (r_1,r_2), which gives $B_{1,1} = n(\rho-1)(4+2\rho-\rho^2)/\rho(1+\rho)$. Similar computations give the other components of the covariance matrix:

$$n\frac{\rho-1}{\rho(1+\rho)}\begin{bmatrix} 4+2\rho-\rho^2 & 2+2\rho-\rho^2 \\ 2+2\rho-\rho^2 & 1+2\rho-\rho^2 \end{bmatrix}.$$

Bibliography

[1] Bender (Edward A.) and Richmond (L. Bruce). – Central and local limit theorems applied to asymptotic enumeration. II. Multivariate generating functions. *Journal of Combinatorial Theory. Series A*, vol. 34, n° 3, 1983, pp. 255–265.

[2] Bender (Edward A.) and Richmond (L. Bruce). – *Multivariate asymptotics for products of large powers with applications to Lagrange inversion.* – Technical Report n° Technical Report 98-10, Faculty of Mathematics, University of Waterloo, 1998.

[3] Bender (Edward A.) and Richmond (L. Bruce). – A multivariate Lagrange inversion formula for asymptotic calculations. *Electronic Journal of Combinatorics*, vol. 5, n° 1, 1998, pp. Research Paper 33, 4 pp. (electronic).

[4] Bergeron (F.), Labelle (G.), and Leroux (P.). – *Combinatorial species and tree-like structures.* – Cambridge University Press, Cambridge, 1998, *Encyclopedia of Mathematics and its Applications*, vol. 67, xx+457p. Translated from the 1994 French original by Margaret Readdy, With a foreword by Gian-Carlo Rota.

[5] Gardy (Danièle). – Some results on the asymptotic behaviour of coefficients of large powers of functions. *Discrete Mathematics*, vol. 139, n° 1-3, 1995, pp. 189–217.

[6] Gessel (Ira M.). – A combinatorial proof of the multivariable Lagrange inversion formula. *Journal of Combinatorial Theory. Series A*, vol. 45, n° 2, 1987, pp. 178–195.

[7] Good (I. J.). – The generalization of Lagrange's expansion and the enumeration of trees. *Proceedings of the Cambridge Philosical Society*, vol. 61, 1965, pp. 499–517.

[8] Hwang (Hsien-Kuei). – On convergence rates in the central limit theorems for combinatorial structures. *European Journal of Combinatorics*, vol. 19, n° 3, 1998, pp. 329–343.

Coefficients of Algebraic Series

Michèle Soria and Philippe Flajolet
LIP6 and INRIA

June 15, 1998

[summary by Cyril Chabaud]

Abstract

The aim of this talk is to provide closed form formulæ for the coefficients of algebraic series using a general method involving finite sums of multinomials.

We start by giving an example of an algebraic series encountered in combinatorics.

Example. General planar trees without unary nodes can be described by

$$\mathcal{D} = o + o(\mathcal{D}\mathcal{D}) + o(\mathcal{D}\mathcal{D}\mathcal{D}) + \cdots .$$

The generating series enumerating the external nodes is a branch of the algebraic function defined by the following equation:

$$d(z) = z + d(z)^2/(1 - d(z))$$

and the coefficients of series $d(z)$ are known to be the Schröder numbers, for which we give a closed form expression in the third example while treating dissections of non-crossing configurations.

1. Form of Coefficients

The coefficients of rational generating functions satisfy linear recurrences with *constant* coefficients and they can be easily given a closed form expression in terms of exponential polynomials.

In general, algebraic generating functions satisfy linear differential equations with polynomial coefficients leading to linear recurrences with *polynomial* coefficients. One may wonder whether it is possible to obtain a finite index formula for the coefficients of algebraic generating series.

The answer is yes. The simplest case is when the series $y(z)$ satisfies an equation of the form $y = z\Phi(y)$ with Φ analytic at 0. Typically, the coefficients of such series can be given an explicit form using the Lagrange inversion theorem:

$$[z^n]y(z) = \frac{1}{n}[y^{n-1}]\Phi^n(y).$$

Example.

$$y = z(1+y^2) \quad \longrightarrow \quad y_{2n+1} = \frac{1}{2n+1}\binom{2n+1}{n},$$

$$y = z + zy^2 + z^2y^3 \quad \longrightarrow \quad y_{2n-1} = \sum_p \frac{1}{2n-1-p}\binom{2n-1-p}{n, n-1-2p, p}.$$

The following theorem provides closed form formulæ for a larger class of algebraic generating functions using a similar approach.

Theorem 1. *Let $\Phi(z,y)$ be a bivariate polynomial such that $\Phi(0,0) = 0$, $\Phi'_y(0,0) = 0$ and* $\mathrm{Val}(\Phi(z,0)) > 0$, *where* Val *denotes the valuation in y and z. Consider the algebraic function implicitly defined by $f(z) = \Phi(z, f(z))$. Then the coefficients of $f(z)$ are given by*

$$[z^n]f(z) = \sum_{m\geq 1} \frac{1}{m}[z^n y^{m-1}]\Phi^m(z,y).$$

Note that, as we have seen in the examples, the powers of Φ induce multinomial expansions and the valuation condition on Φ gives rise to finite sums of these expansions.

Indeed, $\Phi(z,y)$ can be expressed as $\Phi(z,y) = zP(z) + yQ(z,y)$ where $\mathrm{Val}_z(P) = \gamma \geq 0$ and $\mathrm{Val}_{z,y}(Q) = \alpha + \beta \geq 1$. The expansion of the mth power of Φ is

$$\Phi^m = \sum_k \binom{m}{k} z^{m-k} y^k P^{m-k} Q^k.$$

To avoid the cancellation of the quantity

$$[z^n y^{m-1}]\Phi^m = [z^{n-m+k} y^{m-1-k}] \sum_k \binom{m}{k} P^{m-k} Q^k,$$

we must have

$$n - m + k \geq (m-k)\gamma + k\alpha \quad \text{and} \quad m - 1 - k \geq k\beta.$$

This entails

$$m \leq n\frac{\beta+1}{\alpha+\gamma\beta+\beta} + \frac{\alpha-\gamma-1}{\alpha+\gamma\beta+\beta} \quad \text{whence} \quad m \leq 2n-1.$$

Example. Dissections:

$$y = z + 2y^2 - zy \longrightarrow [z^n]y = \sum_r \frac{1}{n+r}\binom{n+r}{r+1, n-r-1, r}(-1)^{n-r-1}2^r.$$

2-3 trees (edges and leaves):

$$y = z + z^2y^2 + z^3y^3 \longrightarrow [z^n]y = \sum_m \frac{1}{m}\binom{m}{n-m+1, 5m-3n-2, 2n-3m+1}.$$

2. **Proof of Theorem 1**

2.1. **Formal Proof.** Let $y(z) = \sum a_n z^n$ be the generating series implicitly defined by the functional equation $y(z) = \Phi(z,y) = zQ(z,y)$. We introduce a parameter u such that $y(z,u) = uQ(z, y(z,u))$. The expression of y is now $y(z,u) = \sum_{n,m} a_{n,m} z^{n-m} u^m$.

From the Lagrange theorem we derive

$$[u^m]y(z,u) = \frac{1}{m}[y^{m-1}]Q^m(y,z).$$

Thus we obtain

$$[z^n]y(z) = \sum_m \frac{1}{m}[y^{m-1}z^{n-m}]Q^m(y,z).$$

2.2. **Analytic Part of the Proof.** The following lemma is a classical formula derived from residue computation.

Lemma 1. *Let $\psi(y)$ be analytic and y_0 be the unique root of $\psi(y) = 0$ inside a domain defined by a closed curve γ. Then*

$$y_0 = \frac{1}{2i\pi}\int_\gamma y\frac{\psi'(y)}{\psi(y)}.$$

Since $y(z)$ is a root of $y - \Phi(z, y) = 0$ and $(0, 0)$ is an ordinary point of $y - \Phi(z, y) = 0$, a formal application of the lemma gives:

$$y(z) = \frac{1}{2i\pi}\int_\gamma y\frac{1 - \Phi'_y(z, y)}{y - \Phi(z, y)}dy.$$

A formal application (justified later) of the formula $(1 - u)^{-1} = 1 + u + u^2 + u^3 + \cdots$ entails:

$$y(z) = \sum_{m\geq 0}\frac{1}{2i\pi}\int_{\gamma'}(1 - \Phi'_y(z, y))\Phi^m(z, y)\frac{dy}{y^m}. \tag{1}$$

Using the Cauchy coefficient formula, we derive:

$$y(z) = \sum_{m\geq 1}[y^{m-1}](1 - \Phi'_y(z, y))\Phi^m(z, y).$$

Still proceeding formally, we finally get the expressions stated in theorem 1:

$$\begin{aligned} y(z) &= \sum_{m\geq 1}[y^{m-1}]\Phi^m(z, y) - \frac{m}{m+1}[y^m]\Phi^{m+1}(z, y), \\ &= \sum_{m\geq 1}\frac{1}{m}[y^{m-1}]\Phi^m(z, y). \end{aligned}$$

Hence

$$y_n = \sum_{m\geq 1}\frac{1}{m}[z^n y^{m-1}]\Phi^m(z, y).$$

Let us explicit now the contours γ and γ' used in the computations above. Since the equation $y - \Phi(y, z) = 0$ has a unique solution $f(z)$ tending to 0 with z, there exists $\rho_1 > 0$ and $r_1 > 0$ such that $|z| \leq \rho_1$ implies $|f(z)| \leq r_1$ and $|f_i(z)| > r_1$ for all other solutions. Consequently

$$\gamma = \{y; |y| = r\} \quad \text{for any} \quad 0 < r < r_1.$$

The expansion that leads to formula (1) requires the condition $|\Phi(z, y)| < |y|$ around $y = 0$. Consequently, the conditions on $\Phi(z, y)$ around the origin imply that there exist constants K, ρ_2 and r_2 such that $\Phi(z, y) \leq K(|z| + |zy| + |y^2|)$ for $|z| < \rho_2$ and $|y| < r_2$. Since

$$|z| + |zy| + |y^2| < |y| \Longleftrightarrow |z| < |y|\frac{1 - |y|}{1 + |y|},$$

it follows that:

$$\gamma' = \{(z, y); |y| < r', |z| < \rho\} \quad \text{for any} \quad r' < \min(r_1, r_2), \quad \text{with} \quad \rho = \min(\rho_1, \rho_2, r'\frac{1 - r'}{1 + r'}).$$

3. General Case

Let y be the function implicitly defined by the algebraic equation $P(z,y)=0$ where P is supposed to be square-free, and assume this equation has several analytic solutions at the origin.

We present here an analytic technique designed to isolate the appropriate branch by giving more information. Actually, it consists in a change of variable that leads to an equation of the form $Y=\Phi(z,Y)$ fulfilling the conditions of theorem 1.

Let $y_1,\ldots,y_k$ be the solutions analytic at the origin of the algebraic equation $P(z,y)=0$. To distinguish all these branches at the origin, we specify α the maximum integer such that

$$\exists i; y_1^{(j)}(0)=y_i^{(j)}(0) \quad \text{for all} \quad j=0,\ldots,\alpha-1.$$

Now, to isolate a specific branch, we perform the change of variables

$$y=\tilde{y}+a_\alpha z^\alpha+a_\beta z^{\beta-1}Y,$$

where $\tilde{y}$ is the common part of the expansions. The branch $Y_1=z+\sum_{n\geq 1}a_n z^n$ is the unique solution analytic at $(0,0)$ of the equation $Y=\Phi(z,Y)$.

Example. Take the generating series of graphs in non-crossing configurations defined by the algebraic equation

$$y^2+(-2-3z+2z^2)y+1+3z=0$$

The expansions of the branches at the origin are:

$$y_1(z)=1+z+2z^2+8z^3+48z^4+352z^5+O(z^6)$$
$$y_2(z)=1+2z-4z^2-8z^3-48z^4-352z^5+O(z^6)$$

The change of variable

$$y=1+z+zY$$

results in

$$z^2(-Y+Y^2+2z+2zY)=0.$$

The algebraic function Y implicitly defined by $-Y+Y^2+2z+2zY=0$ has only one branch tending to 0 at the origin and the general form of this equation is in the scope of theorem 1.

On the Transcendence of Formal Power Series

Jean-Paul Allouche
L.R.I., Université Paris-Sud

December 1, 1997

[summary by Philippe Flajolet]

1. Introduction

Algebraicity of generating functions (gf's) is of interest in combinatorial analysis as it is a sure sign of strong structural properties. For instance, any (unambiguous) context-free model leads to algebraic generating functions; in particular generating functions of simple families of trees and random walks (defined by a finite set of node degrees or jumps) are algebraic. In another context, the algebraic character of the gf's associated with 2-dimensional directed animals in percolation theory points to a wealth of puzzling combinatorial bijections; see [7] for a specific illustration.

Conversely, a transcendence result for the gf of a combinatorial class $\mathcal{C}$ means a sort of "structural complexity lower bound" on $\mathcal{C}$. For instance, elements of $\mathcal{C}$ cannot be encoded by an unambiguous context-free grammar. Accordingly, if $\mathcal{C}$ already admits context-free descriptions, all such descriptions must be inherently ambiguous.

Methods for establishing the transcendence of generating functions fall broadly into two categories.

- Arithmetic methods are based on number-theoretic properties of coefficients. The most famous criterion in this range is Eisenstein's criterion: *If a series of $\mathbb{Q}[[z]]$ is algebraic, then the denominators of its coefficients contain only finitely many primes.* For instance, $f(z) = \exp(z)$ is transcendental "because" its coefficients $f_n = \frac{1}{n!}$ have denominators that contain infinitely many primes (by Euclid's theorem!).
- Analytic methods are based on the presence of a transcendental element in a local behaviour, usually taken at a singular point. In this perspective, $f(z) = \exp(z)$ is transcendental "because" its growth is too fast at infinity, a fact incompatible with the fact that an algebraic function is locally described by a Puiseux series (i.e., a series involving fractional powers).

The analytic approach is reviewed in [6]. The talk focuses on the arithmetic method, and more specifically on the following powerful approach [2, 3, 4, 10].

Principle . If $f(z) = \sum_n f_n z^n$ has integer coefficients and is algebraic over $\mathbb{Q}(z)$, then its reduction $(f(z) \bmod p) := \sum (f_n \bmod p) z^n$ is algebraic over $\mathbb{F}_p(z)$.

Principle . For a series $g(z) = \sum g_n z^n$ over a finite field $\mathbb{F}_p$, the following three properties are equivalent:

(i) the correspondence $n \mapsto g_n$ is computable by a finite automaton that inputs the base-p representation of n ("the g_n are automatic");
(ii) the infinite word $(g_0, g_1, \dots)$ is generated by a regular (length homogeneous) substitution;
(iii) $g(z)$ is algebraic over $\mathbb{F}_p(z)$.

This is the classical "Christol-Kamae-Mendès France-Rauzy Theorem" [4, 5], the equivalence between (i) and (ii) being due to Cobham in 1972. For instance, the Catalan gf,

$$f(z) = \frac{1-\sqrt{1-4z}}{2} = z + z^2 + 2z^3 + 5z^4 + 14z^5 + 42z^6 + 132z^7 + 429z^8 + \cdots$$

has a reduction modulo 2

$$g(z) = z + z^2 + z^4 + z^8 + \cdots$$

where the coefficient g_n is 1 exactly when $n = 2^r$. Thus the coefficient sequence is computable by a finite automaton from the binary representation of the index n. It is also generated starting from the letter a by the regular substitution

$$a \mapsto a1, \qquad 1 \mapsto 10, \qquad 0 \mapsto 00.$$

2. Primitive words

An example originally due to Petersen serves to illustrate nicely the methods just introduced. Say that a word over some alphabet is *primitive* if it is not a "power", that is, the repetition of a shorter pattern. Thus *abbab* is primitive while *abbabbabb* is not. Let $m \geq 2$ be the alphabet cardinality, $W(z) = (1-mz)^{-1}$ the gf of all words, and $P(z)$ the gf of primitive words. Then, since each word has a "root", one has

$$W(z) = P(z) + P(z^2) + P(z^3) + \cdots,$$

so that, with $\mu(n)$ the Moebius function,

$$P(z) = \sum_{d\geq 1} \mu(d) W(z^d), \qquad P_n = \sum_{d|n} \mu(d) m^{n/d}.$$

In particular, the reduction modulo m yields

$$\frac{P_n}{n} = \mu(n) + A \cdot m \equiv \mu(n) \mod m.$$

Thus, the problem is reduced to showing that $\mu(n)$ is the coefficient sequence of a transcendental series.

Now, by a theorem a Cobham, if a sequence has an algebraic gf over a finite field, and if it assumes some fixed value with a limit density δ, then δ is a rational number. (Think of the characterization by finite automata.) But, here, $\mu(n) = 1$ whenever n is square-free, an event whose density is $\frac{6}{\pi^2}$. The transcendence of $\sum_n \mu(n) z^n$ then follows from the irrationality of π.

Reduction modulo m thus provides a proof of the fact that the language of all primitive words cannot be an unambiguous context free language.

In the analytic perspective, transcendence results from the fact that $P(z)$ has infinitely many poles inside the unit circle. Such poles, at points $m^{-1/r}\exp(\frac{2ik\pi}{r})$, arise from $W(z)$ and the Moebius inversion formula for $P(z)$.

3. Stanley's conjecture

In his fundamental paper of 1980 on D-finite series, Stanley [9] conjectured that the binomial series

$$B_t(z) := \sum_{n\geq 0} \binom{2n}{n}^t z^n$$

is transcendental for any integers $t \geq 2$. Of course, we have $B_1(z) = 1/\sqrt{1-4z}$. In the case of even t, B_t is clearly transcendental given the presence of logarithmic elements induced by the asymptotic form of coefficients,

$$\binom{2n}{n}^{2s} \approx \frac{4^{2s}}{n^s}.$$

In addition B_2 is also known to be an elliptic integral. The case of odd t is harder. An analytic proof was suggested by Flajolet [6] in 1987 and an algebraic proof was given by Woodcock and Sharif [10] in 1989.

The proof of [10] consists in reducing first $B_t(z)$ modulo a prime p. The resulting series is algebraic, since a theorem of Furstenberg states that algebraic functions over finite fields are closed under Hadamard (termwise) products. (This property is also clear from the characterization by finite automata.) However, by means of arguments from algebraic number theory, Woodcock and Sharif are able to estimate the degree of $(B_t(z) \bmod p)$ over $\mathbb{F}_p(z)$ and deduce that there exists an infinity of special prime values of p for which this degree grows without bound. This in turn implies the transcendence of $B_t(z)$.

In contrast, from the analytic standpoint, it is the examination of the Puiseux expansion of $B_t(z)$ near its singularity $\zeta = 4^{-t}$ that leads to the transcendence result via the arithmetic transcendence of the number π.

4. Miscellaneous examples

There are a great many cases where reduction modulo a prime leads to transcendence results for generating functions. Here are a few examples.

In [6], the language $\{a^n b v_1 a^n v_2\}$ was shown to be inherently ambiguous through transcendence of

$$S(z) = \sum_{n\geq 1} \frac{z^{2n}}{1-2z+z^{n+1}},$$

since poles accumulate near $1/2$. Alternatively, simple manipulations show that, modulo 2, the transcendence of $S(z)$ is equivalent to the transcendence of the divisor series

$$D(z) = \sum_{n\geq 1} \frac{z^n}{1-z^n} = \sum_{n\geq 1} d(n) z^n.$$

The latter form is transcendental over $\mathbb{F}_2(z)$ since, upon reduction modulo 2, it is the indicator series of squares, and squares are known not to be automatic (Minsky).

A similar process applies to the Goldstine language whose gf involves the theta function $\Theta(z) = \sum_{n\geq 0} z^{n(n+1)/2}$, and to the partition series $P(z) = \prod(1-z^n)^{-1}$ whose logarithmic derivative is closely related to divisor functions.

An amusing example due to Allouche, Betrema, and Shallit is the "Bourbaki definition of integers"

$$\emptyset,\ \{\emptyset\},\ \{\emptyset,\{\emptyset\}\},\ \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\},\ \ldots,$$

which, upon binary encoding, leads to the nonregular substitution $[a \mapsto aab, \quad b \mapsto b]$. The associated infinite word (interpret a as 0, b as 1) has a gf that is transcendental, being related to the series

$$D_2(z) = \sum_{k\geq 2} \frac{z^{2^k-1}}{1-z^{2^k-1}},$$

that also shows up in a formal language example of [6].

5. Lucas sequences

The talk concludes with a description of some recent results of Allouche, Gouyou-Beauchamps, and Skordev [1]. Lucas showed that

$$\binom{m}{n} \equiv \binom{m_0}{n_0}\binom{m_1}{n_1}\binom{m_2}{n_2}\cdots \mod p,$$

where the m_j, n_j are the digits of m, n in base p for prime p. More generally, following [8], define a *p-Lucas sequence* (p prime) by the property

$$a_{pn+j} \equiv a_n a_j \mod p.$$

For instance, the Apéry numbers

$$A_n = \sum_{k\geq 0} \binom{n}{k}^2 \binom{n+k}{k}^2$$

are p-Lucas. Then, Allouche *et alii* characterize the strong property for a sequence to be simultaneously algebraic (automatic) over $\mathbb{Q}$ *and* p-Lucas for all large enough p. In essence, the only possibility for such a sequence is to be, up to normalization, the sequence of values of the Legendre polynomials at some rational point. In other words, the corresponding gf $F(z)$ is of the form

$$F(z) = \frac{1}{\sqrt{1+az+bz^2}}.$$

A particular case is the central binomial coefficient $\binom{2n}{n}$. From Lucas' property and this characterization, a new proof of Stanley's conjecture can be deduced. There are also interesting extensions to Hadamard products of series involving $\binom{2n}{n}$, $\binom{3n}{n}$, etc.

Bibliography

[1] Allouche (J.-P.), Gouyou-Beauchamps (D.), and Skordev (G.). – Transcendence of binomial and Lucas's formal power series. – Preprint, December 1997.

[2] Allouche (Jean-Paul). – Note on an article of H. Sharif and C. F. Woodcock: "Algebraic functions over a field of positive characteristic and Hadamard products". *Séminaire de Théorie des Nombres de Bordeaux. Série 2*, vol. 1, n° 1, 1989, pp. 163–187.

[3] Allouche (Jean-Paul). – Finite automata and arithmetic. In *Séminaire Lotharingien de Combinatoire (Gerolfingen, 1993)*, pp. 1–18. – Univ. Louis Pasteur, Strasbourg, 1993.

[4] Christol (G.). – Ensembles presque-périodiques k-reconnaissables. *Theoretical Computer Science*, vol. 9, 1979, pp. 141–145.

[5] Christol (G.), Kamae (T.), Mendès France (M.), and Rauzy (G.). – Suites algébriques, automates et substitutions. *Bulletin de la Société Mathématique de France*, vol. 108, 1980, pp. 401–419.

[6] Flajolet (P.). – Analytic models and ambiguity of context–free languages. *Theoretical Computer Science*, vol. 49, 1987, pp. 283–309.

[7] Gouyou-Beauchamps (D.) and Viennot (G.). – Equivalence of the two-dimensional directed animal problem to a one-dimensional path problem. *Advances in Applied Mathematics*, vol. 9, n° 3, 1988, pp. 334–357.

[8] McIntosh (Richard J.). – A generalization of a congruential property of Lucas. *The American Mathematical Monthly*, vol. 99, n° 3, 1992, pp. 231–238.

[9] Stanley (R. P.). – Differentiably finite power series. *European Journal of Combinatorics*, vol. 1, 1980, pp. 175–188.

[10] Woodcock (Christopher F.) and Sharif (Habib). – On the transcendence of certain series. *Journal of Algebra*, vol. 121, n° 2, 1989, pp. 364–369.

Multidimensional Polylogarithms

David M. Bradley
Dalhousie University, Canada

July 6, 1998

[summary by Hoang Ngoc Minh]

1. Introduction

Recently, several extensions of polylogarithms, Euler sums (or multiple harmonic sums) and Riemann zeta functions have been introduced. These have arisen in number theory, knot theory, high-energy physics, analysis of quadtrees, control theory, ... In this talk, the author presents the multidimensional polylogarithms and their special values [1, 2]. After definitions related to multidimensional polylogarithms (Section 2), results, conjectures and combinatorial aspects concerning unit Euler sums and unsigned Euler sums are discussed (Section 3). Integral representations are also pointed out to understand multidimensional polylogarithms (Section 4).

2. Definitions

Definition 1. The *multidimensional polylogarithms* (MDPs) are defined as follows

$$\lambda\begin{pmatrix} s_1,\dots,s_k \\ b_1,\dots,b_k \end{pmatrix} = \prod_{j=1}^{k}\sum_{\nu_j\geq 1}\frac{b_j^{-\nu_j}}{(\nu_j+\cdots+\nu_k)^{s_j}}.$$

k is the *depth* and $s = s_1+\cdots+s_k$ is the *weight* of $\lambda\begin{pmatrix} s_1,\dots,s_k \\ b_1,\dots,b_k \end{pmatrix}$.

- When $k=0$, by convention $\lambda(\{\}) = 1$;
- When $k=1$, s is a positive integer and $|b|\geq 1$, one get the usual *polylogarithm*

$$\lambda\begin{pmatrix} s \\ b \end{pmatrix} = \sum_{\nu\geq 1}\frac{b^{-\nu}}{\nu^s} = \mathrm{Li}_s(1/b).$$

  The classical *Riemann zeta function* is obtained in the special case where $b=1$.
- When $k>1$, let $n_j = \sum_{i=j}^{k}\nu_i$ and $b_j = \prod_{i=1}^{j} a_i$. Then

$$\lambda\begin{pmatrix} s_1,\dots,s_k \\ b_1,\dots,b_k \end{pmatrix} = \sum_{n_1>\cdots>n_k>0}\frac{a_1^{-n_1}\cdots a_k^{-n_k}}{n_1^{s_1}\cdots n_k^{s_k}}.$$

  * If each $a_j=1$ then these sums are called *Euler sums*;
  * If each $a_j=\pm 1$ then they are called *alternating Euler sums*.

Definition 2. The *unit Euler sum* is defined as follows

$$\mu(b_1,\dots,b_k) = \lambda\begin{pmatrix} 1,\dots,1 \\ b_1,\dots,b_k \end{pmatrix} = \prod_{j=1}^{k}\sum_{\nu_j\geq 1}\frac{b_j^{-\nu_j}}{(\nu_j+\cdots+\nu_k)}.$$

Definition 3. The *unsigned Euler sum* is defined as follows

$$\lambda_b(s_1,\dots,s_k) = \lambda\begin{pmatrix} s_1,\dots,s_k \\ b,\dots,b \end{pmatrix} = \prod_{j=1}^{k}\sum_{\nu_j\ge 1}\frac{b^{-\nu_j}}{(\nu_j+\cdots+\nu_k)^{s_j}}.$$

- When $b=1$, λ_1 is often called the unsigned Euler sum or *multiple zeta value* (MZV)

$$\lambda_1(s_1,\dots,s_k) = \zeta(s_1,\dots,s_k) = \sum_{n_1>\cdots>n_k>0}\frac{1}{n_1^{s_1}\cdots n_k^{s_k}}.$$

- When $b=2$, λ_2 represents an iterated sum extension of the polylogarithm with argument $1/2$, and plays a crucial role in computing the MZVs.

3. Special Values of MDPs

Theorem 1. *Let p and q satisfy $1/p+1/q=1$. If in addition, $p>1$, or $p\le -1$, then for any nonnegative integer k,*

$$\mu(\{p\}^k) = \frac{(\log q)^k}{k!}.$$

The proof is done by coefficient extraction in the generating function $\sum_{k\ge 0} x^k\mu(\{p\}^k)$.

Theorem 2. *Let $A_r = \mathrm{Li}_r(1/2), P_r = (\log 2)^r/r!, Z_r = (-1)^r\zeta(r)$. Then, for $m\ge 1, n\ge 0$*

$$\mu(\{-1\}^m,1,\{-1\}^n) = (-1)^{m+1}\sum_{k=0}^{m}\binom{n+k}{k}A_{k+n+1}P_{m-k} + (-1)^{n+1}\sum_{k=0}^{n}\binom{m+k}{m}Z_{k+m+1}P_{n-k}.$$

The proof of this theorem can be done via the *duality principle* (see Section 4).

For any nonnegative integer k, the following identities provide nested sum extensions of Euler's $\zeta(2),\zeta(4),\zeta(6)$ and $\zeta(8)$ evaluations, respectively

$$\begin{aligned}
\zeta(\{2\}^k) &= \frac{2(2\pi)^{2k}}{(2k+1)!}\left(\frac{1}{2}\right)^{2k+1}, \\
\zeta(\{4\}^k) &= \frac{4(2\pi)^{4k}}{(4k+2)!}\left(\frac{1}{2}\right)^{2k+1}, \\
\zeta(\{6\}^k) &= \frac{6(2\pi)^{6k}}{(6k+3)!}, \\
\zeta(\{8\}^k) &= \frac{8(2\pi)^{8k}}{(8k+4)!}\left[\left(1+\frac{1}{\sqrt{2}}\right)^{4k+2} + \left(1-\frac{1}{\sqrt{2}}\right)^{4k+2}\right].
\end{aligned}$$

In general, for any positive integer n, $\varepsilon = \mathrm{e}^{i\pi/n}$, one has

$$\sum_{k\ge 0}(-1)^k x^{2kn}\zeta(\{2n\}^k) = \prod_{j=0}^{n-1}\frac{\sin(\pi x\varepsilon^j)}{\pi x\varepsilon^j}.$$

Theorem 3 (Zagier's conjecture [6]).

$$\zeta(\{3,1\}^n) = 4^{-n}\zeta(\{4\}^n) = \frac{2\pi^{4n}}{(4n+2)!}.$$

Conjecture 1.

$$\zeta(2,\{3,1\}^n) = 4^{-n}\sum_{k=0}^{n}(-1)^k\zeta(\{4\}^{n-k})\left[(4k+1)\zeta(4n+2) - 4\sum_{j=1}^{k}\zeta(4j-1)\zeta(4k-4j+3)\right].$$

In practice, one would like to know which unsigned Euler sums can be expressed in terms of lower depth sums. When the sum can be expressed, it is said to "reduce". Hoang Ngoc Minh and Michel Petitot have implemented in `AXIOM` an algorithm to reduce the MZVs via a table of Gröbner basis of these sums at fixed weight [5]. Here, the authors also get the following

Theorem 4. *For any positive integer k,*

$$\zeta(s_1,\dots,s_k) + (-1)^k\zeta(s_k,\dots,s_1)$$

reduces to lower depth MZVs.

The following theorem gives Crandall's recurrence for unsigned Euler sums $\zeta(\{s\}^k)$ and it can be proved by coefficient extraction in the generating function $\sum_{k\geq 0} kx^k\zeta(\{s\}^k)$.

Theorem 5 (Crandall's recurrence)**.** *For any nonnegative integer k and $\Re(s) > 0$,*

$$k\zeta(\{s\}^k) = \sum_{j=1}^{k}(-1)^{j+1}\zeta(js)\zeta(\{s\}^{k-j}).$$

For example

$$\begin{aligned}
\zeta(\{s\}) &= \zeta(s),\\
\zeta(\{s,s\}) &= \frac{1}{2}\zeta^2(s) - \frac{1}{2}\zeta(2s),\\
\zeta(\{s,s,s\}) &= \frac{1}{6}\zeta^3(s) - \frac{1}{2}\zeta(s)\zeta(2s) + \frac{1}{3}\zeta(3s),\dots
\end{aligned}$$

Crandall's recurrence is also a special case of Newton's formula

$$ke_k = \sum_{j=1}^{k}(-1)^{j+1}p_j e_{k-j}, \quad k \geq 0,$$

relating the Elementary Symmetric Functions e_k and and the Power-Sum Symmetric Functions p_r,

$$e_k = \sum_{j_1>\cdots>j_r} x_{j_1}\cdots x_{j_r}, \qquad p_r = \sum_{r>0} x_j^r,$$

with indeterminates $x_j = 1/j^s$, $e_r = \zeta(\{s\}^r)$ and $p_r = \zeta(rs)$.

Definition 4. Let $\vec{s} = (s_1,\dots,s_k)$, $\vec{t} = (t_1,\dots,t_r)$. The set $\mathtt{stuffle}(\vec{s}|\vec{t})$ is defined as follows

1. $(s_1,\dots,s_k,t_1,\dots,t_r) \in \mathtt{stuffle}(\vec{s}|\vec{t})$.
2. If (U,s_n,t_m,V) is in $\mathtt{stuffle}(\vec{s}|\vec{t})$ then also are (U,t_m,s_n,V) and (U,s_n+t_m,V).

One also has

$$\#\mathtt{stuffle}(\vec{s}|\vec{t}) = \sum_{j=0}^{r}\binom{k+j}{r}\binom{r}{j} = \sum_{j=0}^{\max(k,r)}\binom{k}{r}\binom{r}{j}2^j.$$

Theorem 6 (Stuffle Identities [4]).

$$\zeta(\vec{s})\zeta(\vec{t}) = \sum_{\vec{u}\in\texttt{stuffle}(\vec{s}|\vec{t})} \zeta(\vec{u}).$$

For example

$$\zeta(r,s)\zeta(t) = \zeta(r,s,t) + \zeta(r,s+t) + \zeta(r,t,s) + \zeta(r+t,s) + \zeta(t,r,s).$$

4. **Integral Representations for MDPs**

Let $R_1,\ldots,R_k$ be disjoint sets of partitions of $\{1,\ldots,k\}$. For each $1\le m\le n$, let

$$r_m = \sum_{i\in R_m} s_i \quad \text{and} \quad d_m = \prod_{i\in R_m} b_i.$$

From the gamma function identity

$$r^{-s}\Gamma(s) = \int_1^\infty (\log x)^{s-1}x^{-r-1}dx, \quad r,s>0.$$

one gets

Proposition 1.

$$\lambda\begin{pmatrix} r_1,\ldots,r_n \\ d_1,\ldots,d_n\end{pmatrix} = \left\{\prod_{j=1}^{k}\int_1^\infty \frac{(\log x_j)^{s_j-1}}{\Gamma(s_j)}\frac{dx_j}{x_j}\right\}\prod_{m=1}^{n}\left(d_m\prod_{j=1}^{m}\prod_{i\in R_j} x_i - 1\right)^{-1}.$$

For example, given a rational function on x and y, $R(x,y)$. Let $I(R)$ be the following *partition integrals*

$$I(R) = \int_1^\infty\int_1^\infty \frac{(\log x)^{s-1}(\log y)^{t-1}}{\Gamma(s)\Gamma(t)}\frac{dxdy}{xyR(x,y)}.$$

It follows that

$$\begin{aligned}
\lambda\begin{pmatrix} s+t \\ ab\end{pmatrix} &= I(abxy-1),\\
\lambda\begin{pmatrix} s,t \\ a,ab\end{pmatrix} &= I[(ax-1)(abxy-1)],\\
\lambda\begin{pmatrix} t,s \\ b,ab\end{pmatrix} &= I[(by-1)(abxy-1)],\\
\lambda\begin{pmatrix} s \\ a\end{pmatrix}\lambda\begin{pmatrix} t \\ b\end{pmatrix} &= I[(ax-1)(by-1)].
\end{aligned}$$

From the rational identity

$$\frac{1}{(ax-1)(by-1)} = \frac{1}{abxy-1}\left(\frac{1}{ax-1}+\frac{1}{by-1}+1\right),$$

one gets

$$\lambda\begin{pmatrix} s \\ a\end{pmatrix}\lambda\begin{pmatrix} t \\ b\end{pmatrix} = \lambda\begin{pmatrix} s,t \\ a,ab\end{pmatrix} + \lambda\begin{pmatrix} t,s \\ b,ab\end{pmatrix} + \lambda\begin{pmatrix} s+t \\ ab\end{pmatrix}.$$

One can say that *stuffle identities are equivalent to rational identities via partition integrals.*

Definition 5. Given functions $f_j : [a,c] \to \mathbb{R}$ and the 1-forms $\Omega_j = f_j(y_j)dy_j$, the *iterated integral* over Ω_j are defined as follows

$$\int_a^c \Omega_1 \cdots \Omega_n = \begin{cases} 1 & \text{if } n = 0, \\ \int_a^c f(y_1) \int_a^{y_1} \Omega_2 \cdots \Omega_n \, dy_1 & \text{if } n > 0. \end{cases}$$

It turns out that MDPs have a convenient iterated integral representation in terms of 1-forms $\omega_b = dy/(y-b)$, i.e.

$$\lambda \begin{pmatrix} s_1, \ldots, s_k \\ b_1, \ldots, b_k \end{pmatrix} = (-1)^k \int_0^1 \omega_0^{s_1-1}\omega_{b_1} \cdots \omega_0^{s_k-1}\omega_{b_k}.$$

By the iterated integral representation, Broadhurst has generalized the notion of duality principle for MZVs to include the relations between iterated integrals involving the sixth root of unity using the change of variable $y \mapsto 1-y$ at each level of integration [3]. This principle generates an involution $\omega_b \mapsto \omega_{1-b}$ holding for any complex value b. For example

$$\lambda \begin{pmatrix} 2,1 \\ 1,-1 \end{pmatrix} = \int_0^1 \omega_0\omega_1\omega_{-1} = \int_0^1 \omega_2\omega_0\omega_1 = \lambda \begin{pmatrix} 1,2 \\ 2,1 \end{pmatrix}$$

which is

$$\sum_{n\geq 1} \frac{1}{n^2} \left[\sum_{k=1}^{n-1} \frac{(-1)^k}{k} \right] = \sum_{n \geq 1} \frac{1}{n2^n} \left[\sum_{k=1}^{n-1} \frac{2^k}{k^2} \right].$$

Several results can be similarly proved by using other transformations of variables in their integral representations. Here, the authors get

Theorem 7 (Cyclotomic)**.** *Let n be a positive integer. Let $b_1, \ldots, b_k$ be arbitrary complex numbers, and let $s_1, \ldots, s_k$ be positive integers. Then*

$$\lambda \begin{pmatrix} s_1, \ldots, s_k \\ b_1^n, \ldots, b_k^n \end{pmatrix} = n^{s-k} \sum_{\varepsilon_1,\ldots,\varepsilon_k \in \{1, e^{2\pi i/n}, \ldots, e^{2\pi(n-1)/n}\}} \lambda \begin{pmatrix} s_1, \ldots, s_k \\ \varepsilon_1 b_1, \ldots, \varepsilon_k b_k \end{pmatrix}.$$

Theorem 8. *Let $s_1, \ldots, s_k$ be nonnegative integers.*

$$\lambda \begin{pmatrix} 1+s_1, \ldots, 1+s_k \\ -1, \ldots, -1 \end{pmatrix} = \sum \mu \left(\mathrm{Cat}_{j=1}^{k} \{-1\} \, \mathrm{Cat}_{i=1}^{s_j} \{\varepsilon_{i,j}\} \right) \prod_{j=1}^{k} \{-1\} \prod_{i=1}^{s_j} \varepsilon_{i,j},$$

where the sum is over all 2^s sequences of signs $(\varepsilon_{i,j})$ with each $\varepsilon_{i,j} \in \{1,-1\}$ for all $1 \leq i \leq s_j, 1 \leq j \leq k$, and Cat *denotes string concatenation.*

Bibliography

[1] Borwein (Jonathan M.), Bradley (David M.), and Broadhurst (David J.). – Evaluations of k-fold Euler/Zagier sums: a compendium of results for arbitrary k. *Electronic Journal of Combinatorics*, vol. 4, n° 2, 1997, pp. Research Paper 5, 21 pp. – The Wilf Festschrift (Philadelphia, PA, 1996).

[2] Borwein (Jonathan M.), Bradley (David M.), Broadhurst (David J.), and Petr (Lisoněk). – *Special values of multidimensional polylogarithms.* – Research report n° 98-106, CECM, 1998. Available at the URL `http://www.cecm.sfu.ca/preprints/1998pp.html`.

[3] Broadhurst (D. J.). – *Massive 3-loop Feynman Diagrams Reducible to SC* primitives of algebras of the sixth root of unity.* – Technical Report n° OUT-4102-72, hep-th/9803091, Open University, 1998.

[4] Hoffman (Michael E.). – The algebra of multiple harmonic series. *Journal of Algebra*, vol. 194, n° 2, 1997, pp. 477–495.

[5] Minh (Hoang Ngoc) and Petitot (M.). – Lyndon words, polylogarithmic functions and the Riemann ζ function. – Preprint.

[6] Zagier (Don). – Values of zeta functions and their applications. In *et al.* (A. Joseph) (editor), *Proceedings of the First European Congress of Mathematics, Paris.* vol. II, pp. 497–512. – Birkhäuser Verlag, 1994. (Progress in Mathematics, volume 120.).

Monodromy of Polylogarithms

Minh Hoang Ngoc
LIFL, Université de Lille I

July 6, 1998

[summary by David M. Bradley]

Abstract

Generalized polylogarithms are complex, multivalued functions with singularities at $z = 0$ and $z = 1$. We calculate the monodromy at the two singularities. As opposed to the classical polylogs [11, 12], the monodromy of generalized polylogs involves the so-called "multiple zeta values," [14] which play an important role in number theory, knot theory [4, 6, 5, 10], and physics [7, 9]. Via monodromy of polylogs, Radford [13] showed that the C-algebra of polylogs is isomorphic to the C-algebra of non-commutative polynomials in two variables—a "shuffle algebra" freely generated by the so-called Lyndon words. Here, monodromy is used to give an induction proof of the linear independence of the polylogarithms. We also obtain a Gröbner basis of the polynomial relations between "multiple zeta values" using the techniques of non-commutative algebra. By expressing multiple zeta values in terms of the Gröbner basis, one obtains symbolic algebraic proofs of relations between multiple zeta values.

1. Polylogarithms and Combinatorics on Words

Let $X = \{x_0, x_1\}$. To any word $w = x_0^{s_1-1}x_1x_0^{s_2-1}x_1\cdots x_0^{s_k-1}x_1$ we associate the multi-index $s = (s_1, s_2, \ldots, s_k)$ and define the generalized polylogarithm

$$\mathrm{Li}_w(z) = \mathrm{Li}_s(z) = \sum_{n_1>n_2>\cdots>n_k>0} \frac{z^{n_1}}{n_1^{s_1}n_2^{s_2}\cdots n_k^{s_k}}.$$

The associated multiple zeta value is $\zeta_w = \zeta(s) = \mathrm{Li}_w(1) = \mathrm{Li}_s(1)$. The *shuffle product* is defined on words by the recursion

$$xu ш yv = x(u ш yv) + y(xu ш v),$$

where $x, y \in X$ and u and v are words on X. We can extend the shuffle product linearly to the non-commutative polynomials $\mathbb{Q}\langle X\rangle$. The resulting polynomial algebra, denoted $\mathrm{Sh}_{\mathbb{Q}}(X)$ is commutative and associative.

The Lyndon words L are those non-empty words on X that are inferior to each of their right factors in the lexicographical order. They are algebraically independent and generate $\mathrm{Sh}_{\mathbb{Q}}(X)$, thus forming a transcendence basis. More precisely, a theorem of Radford [13] states that the algebra $\mathrm{Sh}_{\mathbb{Q}}(X)$ is isomorphic to the polynomial algebra generated by the Lyndon words, i.e. $\mathbb{Q}[L]$.

2. Relations between Multiple Zeta Values

There are countless relations between multiple zeta values [1, 3, 2]. We content ourselves here with providing only two examples:

$$\zeta(2,1)=\zeta(3) \quad \text{and} \quad \zeta(2,2,1)=-\frac{11}{2}\zeta(5)+3\zeta(2)\zeta(3).$$

It turns out that a large class of relations can be explained by the collision of two distinct shuffles obeyed by the multiple zeta values. We've already seen one type of shuffle. It provides relations of the form $\zeta_{u \sqcup\!\sqcup v}=\zeta_u\zeta_v$. A second type of shuffle provides relations of the form $\zeta_{u*v}=\zeta_u\zeta_v$ and is defined by the recursion

$$(s_1,s)*(t_1,t)=(s_1,s*(t_1,t))+(t_1,(s_1,s)*t)+(s_1+t_1,s*t),$$

where we have used the multi-index notation $s=(s_2,s_3,\ldots,s_k)$, $t=(t_2,t_3,\ldots,t_r)$ of Section 1. With a slight abuse of notation, we define a map $\zeta : w \to \zeta_w$, extended linearly in the natural way to $\mathbb{Q}\langle X\rangle$. Then ζ is a $\mathbb{Q}$-algebra homomorphism which respects both shuffle products. Thus, if I is the ideal generated by the words $u \sqcup\!\sqcup v - u*v$, then $I \subseteq \ker\zeta$. We can compute a Gröbner basis for the ideal I up to any given order using only symbolic computation. The first relation above is the unique basis element of order 3. The second relation above is one of five basis elements of order 5.

3. Monodromy of Polylogarithms

To compute the monodromy, we use the standard keyhole contours about the two singularities $z=0$ and $z=1$. The monodromy is given by

$$\begin{aligned} M_0\mathrm{Li}_{wx_0} &= \mathrm{Li}_{wx_0}+2\pi i\mathrm{Li}_w+\cdots \\ M_1\mathrm{Li}_{wx_1} &= \mathrm{Li}_{wx_1}-2\pi i\mathrm{Li}_w+\cdots, \end{aligned}$$

where the remaining terms are linear combinations of polylogarithms coded by words of lengths less than the length of w. For example, using the computational package Axiom, we find that

$$M_1\mathrm{Li}_{x_0}=\mathrm{Li}_{x_0}, \quad M_1\mathrm{Li}_{x_1}=\mathrm{Li}_{x_1}-2\pi i, \quad M_1\mathrm{Li}_{x_0x_1}=\mathrm{Li}_{x_0x_1}-2\pi i\mathrm{Li}_{x_0},$$

and so on. The generating series of the generalized polylogarithms is

$$L(z)=\sum_{w\in X^*} w\mathrm{Li}_w(z),$$

with the convention that $\mathrm{Li}_{x_0^n}(z)=(\log z)^n/n!$. Drinfel'd's differential equation [8, 9]

$$\frac{d}{dz}L(z)=\left(\frac{x_0}{z}+\frac{x_1}{1-z}\right)L(z),$$

is satisfied, with boundary condition $L(\epsilon)=\exp(x_0\log\epsilon)+O(\sqrt{\epsilon})$ as $\epsilon\to 0+$. It turns out that L is a Lie exponential, and this fact can be used to obtain asymptotic expansions of the generalized polylogarithms at $z=1$.

4. Independence of Polylogarithms

Theorem 1. *The functions* Li_w *with* $w\in X^*$ *are* $\mathbb{C}$*-linearly independent.*

Corollary 1. *The* $\mathbb{C}$*-algebra generated by the* Li_w *is isomorphic to* $\mathrm{Sh}_{\mathbb{C}}(X)$*. By Radford's theorem, the generalized polylogarithms coded by Lyndon words form an infinite transcendence basis.*

Corollary 2. *Each generalized polylogarithm* Li_w *has a unique representation as a* $\mathbb{Q}$*-polynomial in polylogarithms coded by Lyndon words. The classical* [11, 12] *polylogarithms* Li_k*, which are coded by the Lyndon words* $x_0^{k-1}x_1$*, are algebraically independent.*

Proof of Theorem 1. Given $n \geq 0$, assume that

$$\sum_{|w|\leq n} \lambda_w \mathrm{Li}_w = 0, \qquad \lambda_w \in \mathbb{C}, \tag{1}$$

where $|w|$ denotes the length of the word w. We prove by induction on n that $\lambda_w = 0$ for all w, the case $n = 0$ being trivial. Rewrite (1) as

$$\lambda_1 + \sum_{|u|<n} \lambda_{ux_0} \mathrm{Li}_{ux_0} + \sum_{|u|<n} \lambda_{ux_1} \mathrm{Li}_{ux_1} = 0.$$

Applying the operators $(M_0 - \mathrm{Id})$ and $(\mathrm{Id} - M_1)$ on this latter expression, yields two new linear relations

$$\begin{cases} 2\pi i \sum_{|u|=n-1} \lambda_{ux_0} \mathrm{Li}_u + \sum_{|u|<n-1} \mu_u \mathrm{Li}_u & = 0, \\ 2\pi i \sum_{|u|=n-1} \lambda_{ux_1} \mathrm{Li}_u + \sum_{|u|<n-1} \nu_u \mathrm{Li}_u & = 0, \end{cases}$$

for certain coefficients μ_u and ν_u. By the induction hypothesis, the coefficients λ_{ux_0} and λ_{ux_1} with $|u| = n-1$ all vanish (as well as the coefficients μ_u and ν_u). Consequently,

$$\sum_{|w|\leq n-1} \lambda_w \mathrm{Li}_w = 0,$$

whence $\lambda_w = 0$ for all w, again by the induction hypothesis. □

Bibliography

[1] Borwein (Jonathan M.), Bradley (David M.), and Broadhurst (David J.). – Evaluations of k-fold Euler/Zagier sums: a compendium of results for arbitrary k. *Electronic Journal of Combinatorics*, vol. 4, n° 2, 1997, pp. Research Paper 5, 21 pp. – The Wilf Festschrift (Philadelphia, PA, 1996).

[2] Borwein (Jonathan M.), Bradley (David M.), Broadhurst (David J.), and Petr (Lisoněk). – *Combinatorial Aspects of Euler Sums.* – Research report n° 98-107, CECM, 1998. `http://www.cecm.sfu.ca/preprints/1998pp.html`.

[3] Borwein (Jonathan M.), Bradley (David M.), Broadhurst (David J.), and Petr (Lisoněk). – *Special values of multidimensional polylogarithms.* – Research report n° 98-106, CECM, 1998. Available at the URL `http://www.cecm.sfu.ca/preprints/1998pp.html`.

[4] Broadhurst (D. J.), Gracey (J. A.), and Kreimer (D.). – Beyond the triangle and uniqueness relations: non-zeta counterterms at large N from positive knots. *Zeitschrift für Physik. C. Particles and Fields*, vol. 75, n° 3, 1997, pp. 559–574.

[5] Broadhurst (D. J.) and Kreimer (D.). – Knots and numbers in ϕ^4 theory to 7 loops and beyond. *International Journal of Modern Physics C. Computational Physics. Physical Computation*, vol. 6, n° 4, 1995, pp. 519–524.

[6] Broadhurst (D. J.) and Kreimer (D.). – Association of multiple zeta values with positive knots via Feynman diagrams up to 9 loops. *Physics Letters. B*, vol. 393, n° 3-4, 1997, pp. 403–412.

[7] Broadhurst (David J.). – On the enumeration of irreducible k-fold euler sums and their roles in knot theory and field theory. *Journal of Mathematical Physics*, 1998. – To appear. Available as Open University Preprint.

[8] Drinfel'd (V. G.). – On the structure of quasitriangular quasi-Hopf algebras. *Rossiĭskaya Akademiya Nauk. Funktsional'nyĭ Analiz i ego Prilozheniya*, vol. 26, n° 1, 1992, pp. 78–80.

[9] Kassel (Christian). – *Quantum groups.* – Springer-Verlag, New York, 1995, *Graduate Texts in Mathematics*, vol. 155, xii+531p.

[10] Le (Tu Quoc Thang) and Murakami (Jun). – Kontsevich's integral for the Homfly polynomial and relations between values of multiple zeta functions. *Topology and its Applications*, vol. 62, n° 2, 1995, pp. 193–206.

[11] Lewin (Leonard). – *Polylogarithms and associated functions.* – North-Holland Publishing Co., New York, 1981, xvii+359p. With a foreword by A. J. Van der Poorten.

[12] Lewin (Leonard) (editor). – *Structural properties of polylogarithms.* – American Mathematical Society, Providence, RI, 1991, *Mathematical Surveys and Monographs*, vol. 37, xviii+412p.

[13] Radford (David E.). – A natural ring basis for the shuffle algebra and an application to group schemes. *Journal of Algebra*, vol. 58, n° 2, 1979, pp. 432–454.
[14] Zagier (Don). – Values of zeta functions and their applications. In *First European Congress of Mathematics, Vol. II (Paris, 1992)*, pp. 497–512. – Birkhäuser, Basel, 1994.

A Combinatorial Approach to Golomb Trees

Mordecai J. Golin
Hong Kong University

September 22, 1997

[summary by Philippe Dumas and Michèle Soria]

Abstract

Given a set of weights, the problem of finding the binary-tree with minimum weighted external path length is very well understood. It can be solved using Huffman encoding. The problem of finding such an (infinite) tree, with minimal path-length for an infinite set of weights, is not nearly as well studied. Twenty years ago Gallager and Van Voorhis described such trees for the case in which the infinite set of weights is a geometric series. These trees are now known as Golomb trees. Here, the problem is handled with a combinatorial approach.

Let F be an alphabet equipped with a probability distribution. The problem is to encode the alphabet into a language on the binary alphabet $\{0, 1\}$, in such a way that the codeword length mean value is minimal. Such a code is said to be optimal. For a finite alphabet, the problem is known to be solved by Huffman encoding [3]: a tree is built in which each leaf is associated to a (prefix-free) codeword. Hence the path-length of the tree is the codeword length.

When the alphabet is infinite, the problem is solved only for the geometric case, that is the case when the set F is an infinite sequence $a_0, a_1, \ldots$ and the probability of letter a_i occurring in a message is $(1-p)p^i$ with $0 < p < 1$. For example, suppose that we have a string of x's and y's in which each character occurs independently of every other one, x's occurring with probability p, and y's occurring with probability $1-p$. Every infinite message can be uniquely written as the concatenation of words $a_i = x^i y$, each a_i occurring with probability $(1-p)p^i$. The geometric case was studied by Gallager and Van Voorhis [1], who exhibited an optimal tree. Their technique is to construct the Huffman tree for each finite case $\{a_0, a_1, \ldots, a_n\}$, and take the limit in some sense when n goes to infinity. They show that the infinite limit tree is an optimal tree.

Golin's approach is based on combinatorial transformations of trees, which preserve optimality. For his purpose, the important combinatorial feature of the tree is not the whole topological structure, but only its profile, that is the number of internal nodes at each level. He extends the problem to d-ary trees. Considering the number $p \in]0, 1[$ and the integer $d \geq 2$, there is a unique positive integer m which satisfies

$$p^m + p^{m+1} \leq 1 < p^m + p^{m-1}.$$

Define α_k to be the unique positive root of equation

$$1 - \alpha = \alpha^{k(d-1)}(1 - \alpha^d),$$

with the particular case $\alpha_0 = 0$. Using this notation, Golin's result can be stated in the following way.

Theorem 1. *If $\alpha_{m-1} < p < \alpha_m$, then there is a unique optimal tree profile: the first levels from the root are $1, d, d^2, \ldots$ as long as the powers of d are smaller than m, and all the next levels are equal to m.*

If $p = \alpha_m$, then there is an infinite set of optimal tree profiles. They all begin as in the previous case, but after the transition each level is either m or $m+1$.

Notice that this result extends the work of Gallager and Van Voorhis, who did not study the uniqueness of the solution.

The key point is that the geometric character of the distribution entails that the width of an optimal tree at each level is bounded. The proof is valid only for the geometric distribution, since it strongly uses the fact that the shift from a level to the next one translates into a multiplication of the weights p_i's. It does not extend to other types of distributions.

Bibliography

[1] Gallager (Robert G.) and Van Voorhis (David C.). – Optimal Source Codes for Geometrically Distributed Integer Alphabets. *IEEE Transactions on Information Theory*, March 1975, pp. 228–230.

[2] Golin (Mordecai J.). – A Combinatorial Approach to Golomb Forests. – September 1997. Preprint.

[3] Huffman (D. A.). – A Method for the Construction of Minimum-Redundancy Codes. *Proceedings of the IRE*, n° 40, September 1952, pp. 1098–1101.

Colouring Rules for Finite Trees and Probabilities of Monadic Second Order Sentences

Alan R. Woods
University of Western Australia

March 10, 1998

[summary by Cyril Chabaud]

Abstract

Given a set of colouring rules applying to the vertices of any finite rooted tree, we study the asymptotic behaviour of the probability that an n vertex tree has a given root colour. These results will prove that the fraction of labelled or unlabelled rooted trees satisfying any fixed monadic second-order sentence converge to limiting probabilities.

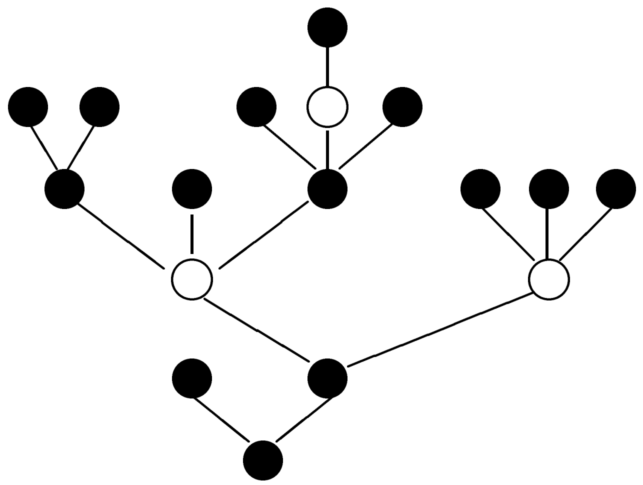
1. Introduction

Given a finite rooted tree and a set of k colours, the vertices are coloured from the leaves to the root according to a set of colouring rules, namely a function $h : \mathbb{N}^k \to \{1, 2, \ldots, k\}$. The colour assigned to a vertex depends only on the number $C_1, \ldots, C_k$ of its immediate predecessors having colour $1, \ldots, k$.

Example. Let

$$h(C_{black}, C_{white}) = \begin{cases} \text{black} & \text{if } C_{black} \text{ is even} \\ \text{white} & \text{if } C_{black} \text{ is odd} \end{cases}$$

be a set of colouring rules. From the definition of h, the leaves of the following tree are coloured black and we find its root colour is black.



Note that the root of a finite rooted tree is black iff the number of its vertices is odd, with the set of colouring rules defined above.

Let $\mu_n[i]$ be the fraction of n vertex labelled trees with root colour i.

Theorem 1. *Let $\mu[i] = \lim_{n\to\infty}\mu_n[i]$ and the corresponding Cesàro limit*

$$\bar{\mu}[i] = \lim_{n\to\infty} \frac{1}{n} \sum_{m=1}^{n} \mu_m[i].$$

For any set of colouring rules h, $\bar{\mu}[i]$ exists for all colours $i = 1, \ldots, k$ and either

1. $\bar{\mu}[i] > 0$ *or*
2. $\exists c > 1$ *such that* $\mu_n[i] < c^{-n}$ *for all sufficiently large* n.

Although the existence of $\mu[i]$ implies the existence of $\bar{\mu}[i]$ in general, the converse needs additional conditions to be true.

2. Applications to Logic

2.1. **First Order Logic.** There exists an analogous result for first order sentences about a graph. The language in which these sentences are written contains the usual quantifiers, parentheses and connectives with an additional predicate symbol $E(x, y)$ expressing the fact that vertex x and vertex y are joined by an edge.

Example. The following expression is a first order logic sentence expressing "every vertex has degree 2":

$$\forall x \exists y_1 \exists y_2 (\neg y_1 = y_2 \wedge \forall z (E(x, z) \Leftrightarrow z = y_1 \vee z = y_2)).$$

Fagin [3], Glebskiĭ, Kogan, Liogon'kiĭ and Talanov [4] have proved the following result

Proposition 1. *Let $\mu_n(\varphi)$ be the fraction of n vertex graphs with property φ. For every first order sentence φ about a graph, $\mu(\varphi) = \lim_{n\to\infty} \mu_n(\varphi)$ exists and $\mu(\varphi) = 0$ or 1.*

That the only possible values are $0, 1$ is a consequence of the fact that graphs have no roots.

2.2. **Monadic Second Order Logic.** The situation for monadic second order sentences about a rooted tree is quite different since the language provides a constant symbol R denoting the root, and it can handle sets of vertices using second order variables.

Determining the satisfiability of a monadic second order sentence φ of rank r reduces to finding the root colour of a rooted tree $\mathcal{T}$ for a particular system of colouring rules. Results arising from Compton's method of components [2] establish that if φ is a sentence of rank r, then there exists sentences $\psi_1, \ldots, \psi_k$ of rank r such that:

1. Every finite rooted tree satisfies exactly one ψ_i;
2. Every φ of rank r is equivalent to $\bigvee_{i\in S} \psi_i$ for some set S.

If $\mathcal{T}$ is a rooted tree that has component trees $\mathcal{T}_1, \ldots, \mathcal{T}_m$ that satisfy sentences $\psi_{i_1}, \ldots, \psi_{i_m}$, then there exists a unique i such that $\mathcal{T}$ satisfies ψ_i, and this particular i can be interpreted as the root colour of $\mathcal{T}$. (For details see [8]).

2.3. **Boolean Formulas.** Assume we have M boolean variables $x_1, \ldots, x_M$. Then the colours turn out to be the 2^{2^M} boolean functions Ψ_i. The existence of the limiting probability $\mu[i]$ is stated in the following theorem:

Theorem 2. *Let $\mu_n[i]$ be the fraction of formulas of size n which compute the boolean function Ψ_i, $i \in \{1, \ldots, 2^{2^M}\}$. Then $\lim_{n\to\infty} \mu_n[i] = \mu[i]$ exists and $\mu[i] > 0$.*

3. **Enumeration of Rooted Trees**

3.1. **Labelled Rooted Trees.** We use generating functions methods to determine $\bar{\mu}[i]$ in the labelled case. Note that a similar proof can be done for the unlabelled case.

Let $T(x)$ denote the generating function for labelled rooted trees:

$$T(x) = t_1 x + \frac{t_2}{2!}x^2 + \frac{t_3}{3!}x^3 + \cdots + \frac{t_n}{n!}x^n + \cdots$$

where t_i is the number of i vertex labelled rooted trees. Since this structure is decomposable, we easily obtain a functional equation on $T(x)$ and find:

$$T(x) = xe^{T(x)}.$$

Hence, using Lagrange inversion we get:

$$T(x) = x + \frac{2}{2!}x^2 + \frac{3^2}{3!}x^3 + \cdots + \frac{n^{n-1}}{n!}x^n + \cdots .$$

The radius of convergence of this series is $\rho = 1/e$, $x = \rho$ is the only singularity on the circle of convergence, where there exists a constant h_1 such that $T(x)$ behaves like $1 + h_1\sqrt{\rho - x}$. One can then apply Darboux's theorem and find that t_n behaves asymptotically like $t_n \sim C\rho^{-n}n^{-3/2}$.

3.2. **Labelled Trees with a Particular Root Colour.** Let $T_i(x)$ be the generating function for labelled trees with root colour i,

$$T_i(x) = x \sum_{\substack{M_1,\ldots,M_k \\ h(M_1,\ldots,M_k)=i}} \frac{T_1^{M_1}(x)}{M_1!} \cdots \frac{T_k^{M_k}(x)}{M_k!}.$$

To find $y_i = T_i(x)$ we have to solve the system:

$$\{y_i = g_i(x, y_1, \ldots, y_k)\}_{i\in\{1,\ldots,k\}} \text{ where } g_i(x, y_1, \ldots, y_k) = x \sum_{\substack{M_1,\ldots,M_k \\ h(M_1,\ldots,M_k)=i}} \frac{y_1^{M_1}}{M_1!} \cdots \frac{y_k^{M_k}}{M_k!}.$$

4. **Cesàro Probabilities**

To determine probability $\bar{\mu}[i]$ we use a partial converse of the following Abelian theorem:

Theorem 3. *Let $b(x) = \sum_{n\geq 0} b_n x^n$, $c(x) = \sum_{n\geq 0} c_n x^n$ and ρ be the radius of convergence of $b(x)$. If $\lim_{n\to\infty} c_n/b_n = \mu$ and $\sum_{n\geq 0} b_n \rho^n$ diverges then:*

$$\lim_{x\to\rho-} c(x)/b(x) = \mu.$$

Setting $c(x) = T_i'(x)$ and $b(x) = T'(x)$, we find that the conditions above are satisfied since $\lim_{x\to\rho-} T'(x) = \infty$. The result is given by the following Tauberian theorem:

Theorem 4 (Compton [1])**.** *Let $b_n \sim Cn^\alpha$, $\alpha > -1$, $b_n \neq 0$ for $n \geq 0$, $c_n = O(b_n)$. If*

$$\lim_{x\to\rho-} c(x)/b(x) = \mu,$$

where ρ is the radius of convergence of $b(x) = \sum_{n\geq 0} b_n x^n$ then:

$$\bar{\mu} = \lim_{n\to\infty} \frac{1}{n} \sum_{M=1}^{n} \frac{c_M}{b_M} = \mu.$$

Since

$$T_i'(x) = \frac{\partial g_i}{\partial x}(x, T_i(x), \dots, T_k(x)) + \sum_{j=1}^{k} T_j'(x) \frac{\partial g_i}{\partial y_j}(x, T_i(x), \dots, T_k(x)),$$

when $x \to \rho-$, we have

$$\bar{\mu}[i] = \sum_{i=1}^{k} \frac{\partial g_i}{\partial y_j} \bar{\mu}[j] \quad \text{for} \quad i = 1, \dots, k.$$

Thus, the $\bar{\mu}[i]$ are linearly dependent, as the following matrix relation shows:

$$\begin{bmatrix} \bar{\mu}[i] \\ \vdots \\ \bar{\mu}[k] \end{bmatrix} = \Omega(\rho) \begin{bmatrix} \bar{\mu}[i] \\ \vdots \\ \bar{\mu}[k] \end{bmatrix} \text{ where } \Omega(\rho) = \begin{bmatrix} \frac{\partial g_1}{\partial y_1} & \cdots & \frac{\partial g_1}{\partial y_k} \\ \vdots & & \vdots \\ \frac{\partial g_k}{\partial y_1} & \cdots & \frac{\partial g_k}{\partial y_k} \end{bmatrix},$$

yielding the linear system: $(\mathrm{Id} - \Omega(\rho))^T [\bar{\mu}[i] \cdots \bar{\mu}[k]] = 0$. Here $\Omega(\rho)$ is a stochastic matrix, and from the theory of nonnegative matrices, the rank of $(\mathrm{Id} - \Omega(\rho))$ is $k-1$. Consequently, the linear system above has a unique solution satisfying $\bar{\mu}[i] + \cdots + \bar{\mu}[k] = 1$.

We associate with $\Omega(\rho)$ its dependency digraph D. Namely, we put a directed edge from vertex j to vertex i iff $\frac{\partial g_i}{\partial y_i}(\rho, T_1(\rho), \dots, T_k(\rho)) > 0$. In other words, this directed edge exists iff $\exists C_1 \cdots \exists C_k (C_j > 0 \wedge h(C_1, \dots, C_k) = i)$

Property 1. *There is a unique strong component S in D with the property that, for every colour j, there is a directed edge in D from j to some colour in S. S is called the principal component of D.*

This property is the key point to prove the first part of theorem 1:

Theorem 5. *For any system of colouring rules, $\bar{\mu}[i]$ exists for all colours i. Moreover, if S is the principal component of dependency digraph D then*

$$\bar{\mu}[i] > 0 \Longleftrightarrow i \in S.$$

Proof. From the property above there exist $A(x)$ and $B(x)$ such that

$$\Omega(x) = \begin{bmatrix} A(x) & C(x) \\ & B(x) \end{bmatrix}$$

and $A(x)$ is an irreducible matrix. Matrix $A(x)$ is indexed by $S = \{1, \dots, s\}$ after renumbering. Since 1 is the largest eigenvalue of $A(\rho)$, from Perron-Frobenius theory (see for instance [7]) there is a unique normalized solution $m_1, \dots, m_s$ of

$$\begin{bmatrix} m_1 \\ \vdots \\ m_s \end{bmatrix} = A(\rho) \begin{bmatrix} m_1 \\ \vdots \\ m_s \end{bmatrix}$$

with $m_1 > 0, \dots, m_s > 0$. Then we just show that 1 cannot be an eigenvalue of $B(\rho)$ and prove that $[m_1, \dots, m_s, 0, \dots, 0]$ is a normalized eigenvector of $\Omega(\rho)$. □

The colours that do not belong to the principal component S have probabilities that converge exponentially to zero, as the following theorem shows:

Theorem 6. *For any system of colouring rules, if $i \notin S$ then there is some $c > 1$ such that $\mu_n[i] < c^{-n}$. (The same property holds in the unlabeled case).*

Sketch of proof. We prove that for each i such that $i \notin S$, $T_i(x)$ has an analytic continuation on the circle of convergence of $T(x)$, meaning that the radius of convergence of $T_i(x)$, ρ_i, is greater than ρ. Since $\mu_n[i] = t_n^i / t_n$, this leads to desired result. For details, see [8]. $\square$

5. Existence of $\mu[i]$

We examine here a sufficient condition to ensure the existence of $\mu[i]$ rather than just $\bar{\mu}[i]$. The existence of $\mu[i]$ is conditioned by the presence of a unique singularity on the circle of convergence of $T_i(x)$, indeed:

Lemma 1. *Let $A(x)$ be the irreducible block of matrix $\Omega(x)$. If $\det(A(x) - I) \neq 0$ for all $x \neq \rho$ on the circle $|x| = \rho$ then $\mu[i]$ exists for all $i \in S$. The probabilities $\mu[1], \ldots, \mu[s]$ are all strictly positive and form the unique normalized solution of*

$$\begin{bmatrix} \mu[1] \\ \vdots \\ \mu[s] \end{bmatrix} = A(\rho) \begin{bmatrix} \mu[1] \\ \vdots \\ \mu[s] \end{bmatrix}$$

Proof. See [8] $\square$

If we look again the first example, clearly $\mu[1]$ and $\mu[2]$ do not exist since series $T_{black}(x)$ and $T_{white}(x)$ have two singularities on the circle $|x| = \rho$.

The next theorem is a sufficient criterion on colouring rules to guarantee the convergence of $\mu_n[i]$:

Theorem 7. *Suppose that for each $i \in \{1, \ldots, k\}$ there exists at least one pair of rules of the following sort, namely: there exists $C_1 > 1, \ldots, C_k > 1$ such that $h(C_1, \ldots, C_i - 1, \ldots, C_k) = h(C_1, \ldots, C_i, \ldots, C_k)$. Then $\mu[i]$ exists and $\mu[i] > 0$ for all $i \in S$.*

Sketch of proof. We prove that $\det(I - \Omega(x)) \neq 0$ for all $|x| \leq \rho$ except $x = \rho$, and that each $T_i(x)$ has at most $x = \rho$ as a singularity on the circle $|x| = \rho$. $\square$

6. Open Problems and Extensions

- Characterize the asymptotic behaviour of $\mu_n[i]$ for general systems of colouring rules;
- Assume φ is a monadic second order sentence. For labeled free trees, McColm [6] proved probability $\mu_n(\varphi)$ satisfied a 0-1 law;
- What happens when we distinguish multiple roots?
- Take unary functions $y = f(x)$. If for some $\epsilon > 0$ and $\gamma > 0$, probability $\mu_n(\varphi) > \epsilon/n^\gamma$ for infinitely many n, is there always a simple asymptotic formula for $\mu_n(\varphi)$?

A partial answer to this last question is that $\mu_n(\varphi)$ converges, and it has been given in the labeled case for $\gamma = 0$ by Compton and Shelah; Woods (also in the unlabeled case) [9]; Łuczak and Thoma [5].

Bibliography

[1] Compton (Kevin J.). – Application of a Tauberian theorem to finite model theory. *Archiv für Mathematische Logik und Grundlagenforschung*, vol. 25, n° 1-2, 1985, pp. 91–98.
[2] Compton (Kevin J.). – A logical approach to asymptotic combinatorics. II. Monadic second-order properties. *Journal of Combinatorial Theory. Series A*, vol. 50, n° 1, 1989, pp. 110–131.
[3] Fagin (Ronald). – Probabilities on finite models. *Journal of Symbolic Logic*, vol. 41, n° 1, 1976, pp. 50–58.
[4] Glebskiĭ (Y. V.), Kogan (D. I.), Liogon'kiĭ (M. I.), and Talanov (V. A.). – Range of degree and realizability of formulas in the restricted predicate calculus. *Kibernetika (Kiev)*, vol. 5, n° 2, 1969, pp. 17–28. – [Engl. Transl. *Cybernetics, vol. 5,* 142–154 (1972)].

[5] Łuczak (Tomasz) and Thoma (Luboš). – Convergence of probabilities for the second order monadic properties of a random mapping. *Random Structures & Algorithms*, vol. 11, n° 3, 1997, pp. 277–295.
[6] McColm (Gregory L.). – MSO asymptotics on random free trees (and random strings). – 1996. Preprint.
[7] Minc (Henryk). – *Nonnegative matrices.* – John Wiley & Sons Inc., New York, 1988, *Wiley-Interscience Series in Discrete Mathematics and Optimization*, xiv+206p. A Wiley-Interscience Publication.
[8] Woods (Alan R.). – Coloring rules for finite trees, and probabilities of monadic second order sentences. *Random Structures & Algorithms*, vol. 10, n° 4, 1997, pp. 453–485.
[9] Woods (Alan R.). – Counting finite models. *The Journal of Symbolic Logic*, vol. 62, n° 3, 1997, pp. 925–949.

Fraïssé-Ehrenfeucht Games and Asymptotics

Alan Woods
University of Western Australia

March 23, 1998

[summary by Julien Clément and Jean-Marie Le Bars]

Abstract

Fraïssé-Ehrenfeucht games are played on two structures, where a structure might, for example, consist of a unary function mapping a finite set into itself. Via generating series and a Tauberian theorem, it is possible to investigate the asymptotic probability of having a winning strategy for such a game, when it is played using a fixed structure, and a random structure of size n, with n going to infinity. Actually for unary functions this gives a convergence law for all properties of the structure which are definable in monadic second order logic.

1. **Introduction**

We consider here structures $\mathcal{A}$ based upon a set A and finitely many relations E_j of finite arity

$$\mathcal{A} = \langle A, E_1(x,y), E_2(x), E_3(x,y,z), \dots \rangle .$$

A classical example is a set of vertices V and an edge relation $E(x,y)$ so that $\mathcal{V} = \langle V, E \rangle$ describes a graph. We can also think of simple structures $\mathcal{A} = \langle A, f \rangle$ consisting of a finite set A and a unary function mapping this set into itself (see fig. 1). This unary function induces a binary relation $F(x,y) \Leftrightarrow f(x) = y$.

In order to use generating functions (see the last section) we need to translate a decomposition property of structures to the generating functions: this will be done through the *disjoint union*. Let us consider two structures

$$\mathcal{A} = \left\langle A, E_1^{\mathcal{A}}, \dots \right\rangle \text{ and } \mathcal{B} = \left\langle B, E_1^{\mathcal{B}}, \dots \right\rangle .$$

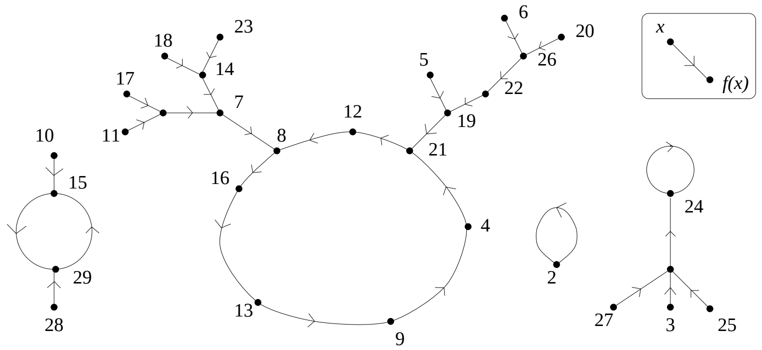


FIGURE 1. Graphical representation a structure $\mathcal{A} = \langle [29], f \rangle$ (where the unary function f maps $\{1, 2, \dots, 29\}$ on itself).

If $A \cap B = \emptyset$ and each $E_i^{\mathcal{A}}$ has the same arity as $E_i^{\mathcal{B}}$, the *disjoint union* is defined as the structure whose domain is the union of the domains and whose relations are the unions of the corresponding relations

$$\mathcal{A} \sqcup \mathcal{B} = \left\langle A \cup B, E_1^{\mathcal{A}} \cup E_1^{\mathcal{B}}, \dots \right\rangle .$$

A class of structures has *components* if each structure can be *uniquely* decomposed into disjoint unions of structures (called *component structures*) from some *components classes.* For structures $\mathcal{A} = \langle [n], f \rangle$, where $[n]$ denotes $\{1, \dots, n\}$ and f is a unary function, one can define component classes relative to the size of the unique loop present in each connected component of the graph of f. From this point of view, for the structure $\mathcal{A}$ of figure 1, we see three components. The first component of $\mathcal{A}$ consists of two component structures in the first component class (the class corresponding to loops of size one i.e. fixed elements of f). The two other components consist in two single component structures and are respectively in the component classes 2 and 7 (relatively to the size of the loop).
Let us define the *rank* $r(\varphi)$ of a formula φ in the context of the second order logic (or MSO logic for short) inductively by:

1. If φ has no quantifiers, then $r(\varphi) = 0$;
2. If φ is $\neg\sigma$, then $r(\varphi) = r(\sigma)$;
3. If φ is obtained from σ_1, σ_2 by the application of a binary propositional connective (e.g., if φ is $\sigma_1 \wedge \sigma_2$, $\sigma_1 \leftrightarrow \sigma_2$, etc.) then $r(\varphi) = \max\{r(\sigma_1), r(\sigma_2)\}$;
4. If φ is of the form $\forall v\sigma$, $\exists v\sigma$, $\forall V\sigma$ or $\exists V\sigma$ for some variable v, V, then $r(\varphi) = r(\sigma) + 1$.

A *sentence* is a formula that has *no free variables* and is a *property* of a structure.
The key observation is that *there are only finitely many inequivalent sentences* $\xi_1, \dots, \xi_m$ *of rank* r. Hence every structure $\mathcal{A}$ satisfies *exactly* one of the sentences (also of rank r)

$$\psi_1 = \xi_1 \wedge \cdots \wedge \xi_m, \psi_2 = \neg\xi_1 \wedge \cdots \wedge \xi_m, \dots, \psi_{2^m} = \neg\xi_1 \wedge \cdots \wedge \neg\xi_m.$$

Given a rank r (and implicitly the sentences $\psi_1, \dots, \psi_{2^m}$), for each $i \in \{1, \dots, 2^m\}$ we define the class of structures which satisfies ψ_i. These classes can be viewed as equivalence classes of Fraïssé-Ehrenfeucht games.

2. **Fraïssé-Ehrenfeucht Games**

The goal is to see whether or not we can distinguish two structures in a r moves game. The game is played with two structures $\mathcal{A} = \left\langle A, E_1^{\mathcal{A}}, \dots \right\rangle$ and $\mathcal{B} = \left\langle B, E_1^{\mathcal{B}}, \dots \right\rangle$.

- At move i, SPOIL chooses $\mathcal{A}$ or $\mathcal{B}$ (let's say $\mathcal{B}$) and one of the following is satisfied
  1. an element $b_i \in B$ or
  2. a subset $B_i \subseteq B$.
- DUPE responds on the other structure ($\mathcal{A}$ here) choosing one of the following
  1. an element $a_i \in A$ or
  2. a subset $A_i \subseteq A$.

DUPE wins if after r moves the map $\{a_i, \dots\} \to \{b_i, \dots\}$ taking $a_i \mapsto b_i$ is an isomorphism of the induced substructures of $\langle \mathcal{A}, A_j, \dots \rangle, \langle \mathcal{B}, B_j, \dots \rangle$ on these sets. We write

$$\mathcal{A} \equiv_r \mathcal{B} \Leftrightarrow \text{DUPE has a winning strategy.}$$

Note that there is no *ex æquo* (either SPOIL or DUPE has a winning strategy). These games are the main tools for proving the following theorems:

Theorem 1. *Let us consider some structures* $\mathcal{A}_1, \mathcal{A}_2, \mathcal{B}_1, \mathcal{B}_2$*, one has*

$$\mathcal{A}_1 \equiv_r \mathcal{B}_1, \mathcal{A}_2 \equiv_r \mathcal{B}_2 \Rightarrow \mathcal{A}_1 \sqcup \mathcal{A}_2 \equiv_r \mathcal{B}_1 \sqcup \mathcal{B}_2.$$

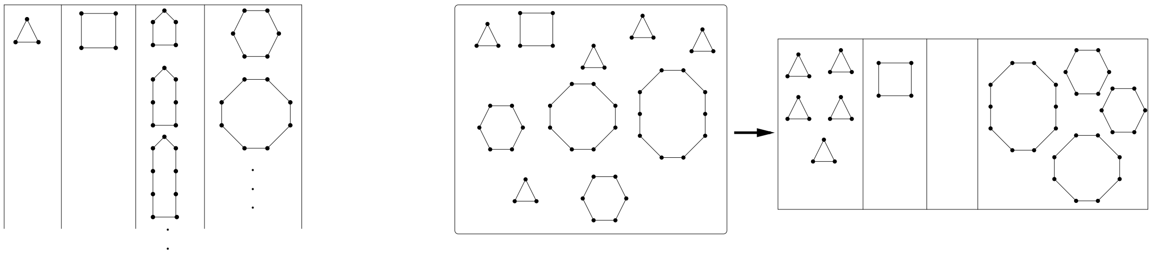


FIGURE 2. The components classes $\mathcal{C}_1, \dots, \mathcal{C}_4$ relative to $\equiv_3$ (left), the structure $\mathcal{A}$ and its four components (right).

Theorem 2. *For every structures $\mathcal{A}$ and $\mathcal{B}$, one has*

$$\mathcal{A} \equiv_r \mathcal{B} \text{ iff there exists } i \text{ such that } \mathcal{A} \models \psi_i \text{ and } \mathcal{B} \models \psi_i,$$

where the sentences ψ_i's are defined in the first section.

Corollary 1. *There are only finitely many $\equiv_r$ classes.*

Another problem consists in determining the $\equiv_r$ class of a given structure $\mathcal{A}$. It is solved if we know the number of component structures lying in each $\equiv_r$ component class (or color if we think of $\equiv_r$ as a colouring). On figure 2, we have 5 component classes $\mathcal{C}_1, \dots, \mathcal{C}_5$ relative to the $\equiv_3$ relation (namely triangles, squares, cycles of odd length strictly greater than 3, cycles of even length strictly greater than 4). The numbers of component structures in each component of the structure $\mathcal{A}$ are respectively $m_1 = 5, m_2 = 1, m_3 = 0, m_4 = 4$.

3. Counting Structures with Components

We count either

1. the number a_n of *labelled structures* with n elements, or
2. the number b_n of *unlabelled structures* with n elements (which is, also, the number of nonisomorphic structures with n elements).

Here we focus on counting labelled structures. So the exponential generating series

$$a(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n$$

will prove highly useful. Indeed, for a structure $\mathcal{A} = \mathcal{G} \sqcup \mathcal{H}$, letting $a(x)$, $h(x)$ and $g(x)$ be the corresponding exponential generating series, we write

$$a(x) = g(x)h(x) \quad \text{or} \quad a(x) = \frac{g(x)^2}{2},$$

whether $\mathcal{G}$ and $\mathcal{H}$ are in different classes or not. By induction the exponential generating series associated to $\mathcal{A} = \mathcal{G}^{(1)} \sqcup \cdots \sqcup \mathcal{G}^{(m)}$ the disjoint union of m structures $\mathcal{G}^{(1)}, \dots, \mathcal{G}^{(m)}$, is

$$a(x) = g^{(1)}(x) \cdots g^{(m)}(x) \quad \text{or} \quad (x) = \frac{g(x)^m}{m!},$$

respectively if $\mathcal{G}^{(1)}, \dots, \mathcal{G}^{(m)}$ are all from different classes or all in the same class. Hence the generating series $a(x)$ for structures with components in the component class $\mathcal{C}$ is

$$a(x) = 1 + c(x) + \frac{c(x)^2}{2!} + \cdots + \frac{c(x)^m}{m!} + \cdots = e^{c(x)},$$

where $c(x) = \sum_n \frac{c_n}{n!} x^n$ (c_n is the number of labelled structures in the component class $\mathcal{C}$ with n elements).
There is a connection with monadic second order logic due to Compton [2]. Let us consider the component classes (relatively to $\equiv_r$) $\mathcal{C}_1, \ldots, \mathcal{C}_k$ (so that the generating series for whole component class is $c(x) = \sum_{i=1}^k c_i(x)$). There is a unique k-tuple $(m_1, \ldots, m_k)$ associated to each structure $\mathcal{A}$, where m_i is the number of component structures of $\mathcal{A}$ lying in the i-th component class $\mathcal{C}_i$. Moreover for two structures $\mathcal{A}$ and $\mathcal{B}$ (with k-tuples $(m_1, \ldots, m_k)$ and $(n_1, \ldots, n_k)$), there is an integer $R = R(r)$ such that if $\forall i \in \{1, \ldots, k\}$ either $m_i = n_i$ or $m_i, n_i \geq R$, then $\mathcal{A} \equiv_r \mathcal{B}$ (plainly speaking, too many component structures of the same component class prevent to distinguish structures). Hence for a sentence φ of rank r, the number of labelled structures $\mathcal{A}$ such that $\mathcal{A} \models \varphi$ depends only on $m_1, \ldots, m_k$ where $m_i \in \{0, 1, \ldots, R-1, \infty\}$ is the number of components in $\mathcal{C}_i$ (∞ means anything equal to at least $R = R(r)$). Considering the exponential generating series $a_\varphi(x) = \sum a_n^\varphi / n!$ where a_n^φ the number of labelled structures with n elements satisfying φ, we can write

$$a_\varphi(x) = \sum_{(m_1, \ldots, m_k) \in S} \frac{c_1(x)^{m_1}}{m_1!} \cdots \frac{c_k(x)^{m_k}}{m_k!},$$

where S is *finite* and $c_i(x)^\infty / \infty!$ denotes $\sum_{m=R}^\infty c_i(x)^m / m! = e^{c_i(x)} - \sum_{m=0}^{R-1} c_i(x)^m / m!$. The series $a_\varphi(x)$ is a finite sum of very similar terms. It is enough just to consider a series of the form

$$a_\varphi(x) = \frac{c_1(x)^{m_1}}{m_1!} \cdots \frac{c_t(x)^{m_t}}{m_t!} e^{c_{t+1}(x)} \cdots e^{c_k(x)}.$$

This formula means that a structure $\mathcal{A}$ satisfying φ has exactly m_i components in the class i for $i \in \{1, \ldots, t\}$ and any number of components in the other classes. We want to know a_n^φ or equivalently $\mu_n(\varphi) = a_n^\varphi / a_n$, the fraction of structures of size n satisfying φ. We are also interested in the *asymptotic probability* $\mu_\varphi = \lim_{n\to\infty} \mu_n(\varphi)$, when this limit exists.
It is Compton's idea to use partial converses *Tauberian lemmas* to get limit laws for μ_n. Here is a sample theorem whose proof is based on such lemmas.

Theorem 3. *For any class with components, if $a_n/n! \sim C\tau^n/n^\alpha$ and $c_n/n! = O(\tau^n/n)$ (with $\alpha > -1$) then $\mu(\varphi) = \lim_{n\to\infty} \mu_n(\varphi)$ exists for all MSO sentences φ and is equal to $a_\varphi(\rho)/a(\rho)$.*

Due to known results about a_n and c_n for structures with one unary function, we have also

Corollary 2. *The asymptotic probability μ_φ always exists with one unary function.*

Bibliography

[1] Compton (Kevin J.). – Application of a Tauberian theorem to finite model theory. *Archiv für Mathematische Logik und Grundlagenforschung*, vol. 25, n° 1-2, 1985, pp. 91–98.
[2] Compton (Kevin J.). – A logical approach to asymptotic combinatorics. II. Monadic second-order properties. *Journal of Combinatorial Theory. Series A*, vol. 50, n° 1, 1989, pp. 110–131.
[3] Fagin (Ronald). – Probabilities on finite models. *Journal of Symbolic Logic*, vol. 41, n° 1, 1976, pp. 50–58.
[4] Glebskiĭ (Ju. V.), Kogan (D. I.), Liogon'kiĭ (M. I.), and Talanov (V. A.). – Volume and fraction of satisfiability of formulas of the lower predicate calculus. *Kibernetika (Kiev)*, vol. 5, n° 2, 1969, pp. 17–27. – English translation *Cybernetics*, vol. 5 (1972), pp. 142–154.
[5] Woods (Alan). – Counting finite models. *The Journal of Symbolic Logic*, vol. 62, n° 3, September 1997, pp. 925–949.

Statistical Physics of the Random Graph Model

Rémi Monasson

Laboratoire de Physique Théorique, École Normale Supérieure

April 6, 1998

[summary by Philippe Flajolet]

Abstract

This talk addresses the random graph model originally introduced by Erdős et Rényi in 1959. This model gives rise to a large number of threshold phenomena that are evocative of phase transitions in statistical physics. The talk illustrates the way several results on random graphs can be reexamined in a new perspective provided by a simple model of statistical physics, the Potts model. The problem addressed is principally that of the size of the giant component for which quantitative estimates are derived.

More generally, the talk is motivated by a desire to understand what statistical physics models may bring to the realm of threshold problems, not only in random graphs but also in the satisfiability of random boolean formulæ.

1. **The Random Graph Models**

The most natural random graph models have been introduced by Erdős and Rényi in a series of eventually famous papers that starts with [5, 6]. They are denoted by $G_{n,p}$ and $\widehat{G}_{n,e}$ and are defined as follow:

- $G_{n,p}$ considers graphs with n vertices in which each of the $N = \binom{n}{2}$ possible edges is present with probability p;
- $\widehat{G}_{n,e}$ considers all graphs with n vertices and e edges as equally likely.

The first model is of the Bernoulli type (there are N trials, each with independent probability p of success), the second one is more "combinatorial". Given the fact that the Bernoulli distribution $B(N,p)$ is narrowly centered around its mean Np, we expect the following fact.

The characteristics of $G_{n,p}$ resemble those of $\widehat{G}_{n,e}$ provided $e \approx Np$.

We refer globally to Bollobás's book [4] for a discussion of these rich models and for precise conditions that make the assertion above into a valid mathematical statement. (The transfer from $\widehat{G}_{n,e}$ to $G_{n,p}$ is an Abelian one, whereas the converse transfer has a Tauberian flavour.)

Imagine a graph as evolving in time from totally disconnected to complete, through successive additions of edges that are reflected by increasing values of p from 0 to 1. What is characteristic of $G_{n,p}$ (and thus, of the companion $\widehat{G}_{n,e}$ model) is the presence of sharp thresholds. A threshold phenomenon for a property P means that there is a function $p_0(n)$ such that, with (very) high probability (as $n \to \infty$), P does not hold when $p \ll p_0(n)$ while for $p \gg p_0(n)$, P holds. (Of course, one may look for all sorts of detailed informations near the threshold $p_0(n)$.)

Here is a simplified picture of what goes on in $G_{n,p}$, expressed in terms of the mean number of edges, $m = Np$. Only isolated vertices and edges will be present when $m \ll n^{1/2}$; but trees of size 3 will start appearing at $m \approx n^{1/2}$, trees of size 4 at $m \approx n^{2/3}$, etc. There is (almost surely) no cycle when $m \ll n$. Later when $m = \lambda n/2$ and $\lambda < 1$ there is at most one cycle in each component and the largest component almost surely has size $\Theta(\log n)$. A dramatic phase transition occurs near $m = n/2$ when one or several large components of size $n^{2/3}$ appear. Still later, when $m = \lambda n/2$ and $\lambda > 1$, we find a single "giant" component of size $\Theta(n)$. However, we'll have to wait a little longer, namely till $m \approx \frac{1}{2} n \log n$, to attain full connectedness, at which point the graph ceases to be interesting for the problems under discussion here.

There are various approaches to these problems. Most of them, following Erdős and Rényi's original papers [5, 6], are probabilistic and well explained in [4]. Roughly, one has to cope in this framework with random variables satisfying intricate dependencies; moment methods, tail inequalities, or probabilistic inequalities are then essential. The literature in this direction is immense and Bollobás's book already includes more than 700 references. The best results relative to connectedness that are available at this time (formulated in terms of $\widehat{G}_{n,e}$) are probably those of Bender, Canfield, and McKay; see [1, 2, 3]. In contrast, only a handful of papers starting with Knuth, Pittel, and collaborators resort to analytic methods[1]; see [7, 9]. Even fewer papers rely on methods from statistical physics. The work under discussion here is a pioneering attack on this range of hard problems; see [10, 11] for applications of related ideas to the random k-satisfiability problem.

2. The Potts Model

The Potts model of statistical physics considers particles or sites whose states (sometimes referred to as "colours") may assume any of q values. In the particular case of random graphs, it instantiates as follows. Consider n *sites* that we may imagine as regularly spaced on a circle. Each site may be in a certain *state* that is an integer of $\{0, 1, \ldots, q-1\}$. The integer q is a parameter of the model and when $q = 2$, one can think of the states as "spins" representing the orientation of some vector, e.g., a magnetic moment. A *configuration* $\Sigma = (\sigma_1, \ldots, \sigma_n)$ is an assignment of states to each site, so that there are q^n possible configurations. The energy of a configuration is defined as

$$E(\Sigma) = -\frac{\gamma}{n} \sum_{i<j} \mathbf{1}_{\sigma_i, \sigma_j},$$

where $\mathbf{1}_{x,y}$ is the indicator of $x = y$ that has value 1 if $x = y$ holds and 0 otherwise. There γ is a parameter; the fact that one takes all the $N = n(n-1)/2$ combinations $i < j$ corresponds to a model with complete interactions, that is, the underlying graph is the complete graph. (Models of statistical physics often consider instead an underlying graph constrained to be a regular lattice in dimension 1, 2, or 3.)

An essential object of statistical physics is the *partition function* defined here as

$$Z(\gamma, n) = \sum_{\Sigma} e^{-E(\Sigma)},$$

which is thus a sum of q^n terms. There are two main points in the talk: (i) the function Z provides information on the random graph model; (ii) it is possible to estimate analytically various characteristics of Z.

[1]As said by Frieze in his discussion of the paper by Janson, Knuth, Luczak, and Pittel [9] in the *Mathematical Reviews* [**MR**94h:05070]: "The paper [9] and its predecessor [7] mark the entry of generating functions into the general theory of random graphs in a significant way. Previously, their use had mainly been restricted to the study of random trees and mappings. However, at the early stages of the evolution of a random graph we find that it is usually not too far from being a forest, and this allows generating functions an entry."

3. The Partition Function and Random Graphs

First of all, the partition function is (almost) a counting generating function in disguise. One has

$$Z(\gamma, n) = \sum_{\Sigma} \prod_{i<j} \exp\left(\frac{\gamma}{n}\mathbf{1}_{\sigma_i,\sigma_j}\right) = \sum_{\Sigma} \prod_{i<j} \left(1 + \mathbf{1}_{\sigma_i,\sigma_j}(e^{\gamma/n} - 1)\right),$$

as results from the identity $\mathbf{1}^2 = \mathbf{1}$. Next,

$$Z(\gamma, n) \approx \sum_{\Sigma} \prod_{i<j} \left(1 + \frac{\gamma}{n}\mathbf{1}_{\sigma_i,\sigma_j})\right) \tag{1}$$

$$= \sum_{G} \left(\frac{\gamma}{n}\right)^{\epsilon(G)} q^{c(G)}. \tag{2}$$

The first line (1) is a natural approximation for n large. In the second line (2), $\epsilon(G)$ is the number of edges of the graph G, $c(G)$ the number of its connected components, and the sum is over all graphs G with n vertices. The reason why (2) is true is that the general term of the sum involves a product over all possible edges, and a product like $u_{\sigma_1,\sigma_2}u_{\sigma_2,\sigma_3}$ has value 1 only if $\sigma_1, \sigma_2, \sigma_3$ are of the same colour, in which case there are altogether q degrees of freedom.

Now, a graph G with n vertices and ϵ edges has probability

$$P_\gamma(G) = \left(\frac{\gamma}{n}\right)^{\epsilon} \left(1 - \frac{\gamma}{n}\right)^{N-\epsilon},$$

in the model $G_{n,p}$, where $p = \gamma/n$ and, like before, $N = n(n-1)/2$. Then, equation (2) yields the approximate formula,

$$Z(\gamma, n) \approx e^{\gamma n/2} \sum_{G} P_\gamma(G) q^{c(G)}. \tag{3}$$

(These approximations are stated here without error terms but it is not hard to assign them sufficient validity conditions.)

4. The Potts Model and the Process of "Analytic Continuation"

In order to approach the number of connected components, we return to the definition of the partition function and aim at transforming its expression. The energy, $E(\Sigma)$ depends on n variables, but only through their q possible values, with q the parameter of the Potts model. Indeed, for $\sigma \in \{0, \ldots, q-1\}$, define the occupancy variables,

$$X_\sigma(\Sigma) = \frac{1}{n} \sum_{i=1}^{n} \mathbf{1}_{\sigma_i,\sigma},$$

that describe how many times each value of $\{0, \ldots, q-1\}$ is used by a configuration. One finds easily that

$$E(\Sigma) = \frac{\gamma}{2} - \frac{\gamma n}{2} \sum_{\sigma=0}^{q-1} X_\sigma^2.$$

(The term $\gamma/2$ is ignored in subsequent computations.) Now, grouping states according to the values of their occupancy vectors $\{X_\sigma\}$ yields

$$Z(\gamma, n) \approx \sum_{\{X_\sigma\}} \binom{n}{nX_0, \ldots, nX_{q-1}} \exp\left(-\frac{\gamma n}{2}\sum_{\sigma=0}^{q-1} X_\sigma^2\right),$$

where the X_σ are such that $\sum_\sigma X_\sigma = 1$ and the X_σ go by steps of $\frac{1}{n}$. (The original derivation of Monasson makes use of manipulations with indicator variables that are related to the theory of "replicas".) Then, Stirling's formula employed to approximate the factorials present in the multinomial coefficient produces

$$Z(\gamma, n) \approx \sum_{\{X_\sigma\}} \exp\left(-n\left(\sum_\sigma X_\sigma \log X_\sigma + \frac{\gamma}{2}\sum_\sigma X_\sigma^2\right)\right). \tag{4}$$

The form (4) is indeed a q-fold sum and the original n-fold summations and products have been eliminated.

The next step consists in evaluating what happens with the approximation (4) taken as

$$Z(\gamma, n) \approx \sum_{\{X_\sigma\}} \exp\left(-nG(\{X_\sigma\})\right). \tag{5}$$

The idea is to estimate the sum by means of the q-dimensional Laplace method, which requires locating the *global* extrema of the exponential. It is observed that *local* extrema at least are obtained by trying

$$X_0 = \frac{1}{q}(1 + (q-1)s), \qquad X_1 = \cdots = X_{q-1} = \frac{1}{q}(1-s). \tag{6}$$

Then, the argument of the exponential in (4) is locally maximized if one fixes s as a root of

$$\log\left(\frac{1+(q-1)s}{1-s}\right) = \gamma s. \tag{7}$$

It is believed that all global extrema are obtained in this way, up to permutation of indices. Under this assumption, the Laplace method can then be applied to approximate $Z(\gamma, n)$ as

$$Z(\gamma, n) \approx e^{-nF(q,\gamma)}, \tag{8}$$

where F is essentially $G(\{X_\sigma\})$ of (5) evaluated at the X_σ given by (6) in terms of q, s, where $s = s(\gamma)$ satisfies the condition (7).

We now dive into a more conjectural world based on a special kind of formal reasoning The principle of the heuristic analysis consists in extrapolating the asymptotic approximation of the partition function that is defined a priori for integer values of q only and make it an analytic function of q. Then, let q tend to 1 and hope for consistency. Once this is done, various results that can be checked successfully against known ones (via analytic or probabilistic methods) are obtained.

Let us postulate the validity of (8) for all *real* q, and in particular for q near 1.Within this framework, the mean number of connected components of a random graph of $G_{n,\gamma/n}$ is for instance accessible as ($\langle X\rangle$ denotes expectation):

$$\langle c(G)\rangle = \frac{d}{dq}\log Z(\gamma, n)\bigg|_{q=1}, \tag{9}$$

where *real* values $q \to 1$ are used. For the region of interest which is thus q near 1, equation (7) becomes $1 - s = e^{\gamma s}$. This equation defines s as a function of γ, $s = s(\gamma)$. The parameter $s(\gamma)$ is in fact an indicator of the fraction of sites in the largest connected component of the random graph. There is a bifurcation at $s = 1$. The function $s(\gamma)$ is identically 0 when $\gamma < 1$, a fact consistent with known properties of the random graph before the emergence of the giant component. At $s = 1^+$, the function $s(\gamma)$ has a square-root singularity, while it becomes analytic for $s > 1$. Thus informations about the giant component and its "phase transition" become amenable to this approach (details omitted in this abstract).

5. **Discussion**

A summary of the methodology is as follows. For a given problem, there are a priori two "partition functions",

$$Z_{\text{comb}} := \sum_G P(G) q^{c(G)}, \qquad Z_{\text{phys}} = \sum_\Sigma e^{-E(\Sigma)}.$$

The process is then as follows.

1. Choose the configuration space and energy function so that $Z_{\text{comb}} \approx Z_{\text{phys}}$.
2. Evaluate Z_{phys} by: (i) identifying the order parameters (the X_σ); (ii) determining asymptotic approximations (here by the Laplace method); (iii) performing an analytic "continuation" according to the chain "(q integer) $\mapsto$ (q real) $\mapsto$ ($q \to 1$)".

The major question to ask is why and to what extent does this approach provide useful quantitative result. Certainly, the approximations for fixed integer q can be justified. Also there is a possibility of matching the analysis near $q = 1$ against what we know from analytic approaches. (For instance, it is known that the emergence of the giant component is related in an essential way to the occurrence of two coalescing saddle points.) So, in a way, the most surprising fact to be explained is that estimates initially conducted for integer q only (we used a q-dimensional Laplace method!) can be "analytically continued" to the region of q near 1.

We observe that complex analysis does *sometimes* provide a framework for such analytic continuation. For instance, a theorem of Carlson asserts that when a function $\phi(s)$ is analytic (holomorphic) in a right-hand half-plane and is of moderate growth, $\phi(s) = O(e^{(\pi-\epsilon)|s|})$, then: *$\phi(s)$ vanishes identically if and only if it vanishes at the nonnegative integers.* Therefore, an identity $A(s) = B(s)$ can be inferred just from its specialization at the integers[2] provided it is known a priori that A, B don't grow to fast. For instance, it suffices to establish

$$\sin^2 \frac{\pi s}{4} + \cos^2 \frac{\pi s}{4} = 1,$$

for $s = 0, 1, \ldots$, in order to be sure that it holds for all complex s. Observations of this kind however fall short of providing a basis for the analytic continuation process employed here, given the intricate nature of the approximations involved.

Bibliography

[1] Bender (Edward A.), Canfield (E. Rodney), and McKay (Brendan D.). – The asymptotic number of labeled graphs with given number of vertices and edges. *Random Structures & Algorithms*, vol. 1, n° 2, 1990, pp. 127–169.

[2] Bender (Edward A.), Canfield (E. Rodney), and McKay (Brendan D.). – Asymptotic properties of labeled connected graphs. *Random Structures & Algorithms*, vol. 3, n° 2, 1992, pp. 183–202.

[2] It is well worth pointing at Hardy's discussion in [8, Ch. 11] of "Ramanujan's heuristic" on which Ramanujan based so much of his definite integral evaluations.

[3] Bender (Edward A.), Canfield (E. Rodney), and McKay (Brendan D.). – The asymptotic number of labeled graphs with n vertices, q edges, and no isolated vertices. *Journal of Combinatorial Theory. Series A*, vol. 80, n° 1, 1997, pp. 124–150.
[4] Bollobás (Béla). – *Random Graphs.* – Academic Press, 1985.
[5] Erdős (P.) and Rényi (A.). – On random graphs. I. *Publ. Math. Debrecen*, vol. 6, 1959, pp. 290–297.
[6] Erdős (P.) and Rényi (A.). – On the evolution of random graphs. *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, vol. 5, 1960, pp. 17–61.
[7] Flajolet (P.), Knuth (D. E.), and Pittel (B.). – The first cycles in an evolving graph. *Discrete Mathematics*, vol. 75, 1989, pp. 167–215.
[8] Hardy (G. H.). – *Ramanujan: Twelve Lectures on Subjects Suggested by his Life and Work.* – Chelsea Publishing Company, New-York, 1978, third edition. Reprinted and Corrected from the First Edition, Cambridge, 1940.
[9] Janson (Svante), Knuth (Donald E.), Łuczak (Tomasz), and Pittel (Boris). – The birth of the giant component. *Random Structures & Algorithms*, vol. 4, n° 3, 1993, pp. 233–358.
[10] Monasson (Rémi) and Zecchina (Riccardo). – Entropy of the K-satisfiability problem. *Physical Review Letters*, vol. 76, n° 21, 1996, pp. 3881–3885.
[11] Monasson (Rémi) and Zecchina (Riccardo). – Statistical mechanics of the random K-satisfiability model. *Physical Review E. Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics. Third Series*, vol. 56, n° 2, 1997, pp. 1357–1370.

Statistical Physics of the Random K-Satisfiability Problem

Remi Monasson and Riccardo Zecchina
Laboratoire de Physique Théorique de l'ENS, Paris, France
International Center for Theoretical Physics, Trieste, Italy

April 6, 1998

[summary by Olivier Dubois and Remi Monasson]

The satisfaction of constrained formulae is a key issue in complexity theory. Many computational problems are shown to be NP-complete through a polynomial mapping onto the K-Satisfiability (SAT) problem. Recently, there has been much interest in a random version of the K-SAT problem defined as follows. Consider N Boolean variables x_i, $i = 1, \ldots, N$. Call clause C the logical OR of K randomly chosen variables, each of them being negated or left unchanged with equal probabilities. Then repeat this process by drawing independently M random clauses C_ℓ, $\ell = 1, \ldots, M$. The logical AND of all clauses, $\mathcal{F}$, is said to be satisfiable if there exists a logical assignment to the x's evaluating $\mathcal{F}$ to true, unsatisfiable otherwise.

Numerical experiments have concentrated upon the study of the probability $P_N(\alpha, K)$ that a given $\mathcal{F}$ including $M = \alpha N$ clauses be satisfiable. For large sizes of N, there appears a remarkable behaviour: P seems to reach unity for $\alpha < \alpha_c(K)$ and vanishes for $\alpha > \alpha_c(K)$ [6]. Such an abrupt threshold behaviour, separating a SAT phase from an UNSAT one, has indeed been rigourously confirmed for 2-SAT, which is in P, with $\alpha_c(2) = 1$ [2, 5]. For larger $K \geq 3$, K-SAT is in NP and much less is known. The existence of a sharp transition has not been proven yet but precise estimates of the thresholds have been found: $\alpha_c(3) \simeq 4.25$. Moreover, some lower and upper bounds to $\alpha_c(3)$ (if it exists), $\alpha_{l.b.} = 3.003$ and $\alpha_{u.b.} = 4.64$ respectively have been established [4, 3].

The classical approaches to study the SAT phenomenon threshold are both combinatorial and probabilistic. A statistical physics approach was used in [8, 9]. Such an approach allows properties to be predicted. It has been applied already to random graphs and it has led to large deviation results for the threshold phenomenon of random graphs in addition to previously known results. This approach seems therefore to be powerful. However it proves much harder to apply to the SAT threshold phenomenon. It yields in particular a surprising change concerning the proportion of variables fixed in the neighbourhood of the threshold between 2-SAT and 3-SAT. This could partly account for the complexity gap between these two problems. In order to apply the statistical physics approach, the following steps were carried out.

First, the energy function corresponding to the K-SAT problem is identified. The logical values of the x's can be represented by N binary variables S_i's, called spins, through the one-to-one mapping $S_i = -1$ (respectively $+1$) if x_i is false (resp. true). We then encode the random clauses into a $M \times N$ matrix $C_{\ell i}$ in the following way: $C_{\ell i} = -1$ (respectively $+1$) if the clause C_ℓ includes $\overline{x_i}$ (resp. x_i), $C_{\ell i} = 0$ otherwise. Consider now the cost-function $E[\mathbf{C}, \mathbf{S}]$ defined as the number of clauses that are not satisfied by the logical assignment corresponding to configuration $\mathbf{S}$. The minimum $E[\mathbf{C}]$ of $E[\mathbf{C}, \mathbf{S}]$, that is, the lowest number of violated clauses that can be achieved by the best possible logical assignment [8, 9], is a random variable which becomes totally concentrated around its mean value $\ll E[\mathbf{C}] \gg$ in the large size limit [1]. The latter is accessible through the knowledge of the averaged logarithm of the generating function

$$Z[\mathbf{C}] = \sum_{\mathbf{S}} \exp\left(-E[\mathbf{C},\mathbf{S}]/T\right) \tag{1}$$

since

$$\ll E[\mathbf{C}] \gg = -T \ll \log Z[\mathbf{C}] \gg + O(T^2)$$

when the auxiliary parameter T is eventually sent to zero. Being the minimal number of violated clauses, $\ll E[\mathbf{C}] \gg$ equals zero in the SAT region and is positive in the UNSAT phase, allowing the location of $\alpha_c(K)$.

The calculation of the average value of the logarithm of Z in (1) is an awkward one. To circumvent this difficulty, we compute the nth moment of Z for integer-valued n and perform an analytical continuation to real n in order to exploit the identity

$$\ll Z[\mathbf{C}]^n \gg = 1 + n \ll \log Z[\mathbf{C}] \gg + O(n^2).$$

The nth moment of Z is obtained by replicating n times the sum over the spin configuration $\mathbf{S}$ and averaging over the clause distribution [8]

$$\ll Z[\mathbf{C}]^n \gg = \sum_{\mathbf{S}^1,\mathbf{S}^2,\ldots,\mathbf{S}^n} \ll \exp\left(-\sum_{a=1}^{n} E[\mathbf{C},\mathbf{S}^a]/T\right) \gg . \tag{2}$$

It is crucial to notice that the averaged term in (2) depends on the $n \times N$ spin replicas only through the 2^n occupation fractions $c(\sigma)$ labelled by the vectors σ with n binary components; $c(\sigma)$ equals the number (divided by N) of labels i such that $S_i^a = \sigma^a$, $\forall a = 1, \ldots, n$. Taking into account the combinatorial entropy of the labels i at fixed occupation fractions,

$$\ll Z[\mathbf{C}]^n \gg \simeq \exp(N F_{max})$$

where F_{max} is the maximum over all possible xs of the functional [8]

$$F[\{c\}] = -\sum_{\sigma} c(\sigma)\log c(\sigma) + \alpha \log\left[\sum_{\sigma_1,\ldots,\sigma_K} c(\sigma_1)\cdots c(\sigma_K)\exp\left(-\frac{1}{T}\sum_{a=1}^{n}\sum_{\ell=1}^{K}\delta[\sigma_\ell^a + 1]\right)\right]. \tag{3}$$

The optimisation conditions over $F[\{c\}]$ provide 2^n coupled equations for the cs. Notice that F is a symmetric functional, that is, invariant under any permutation of the replicas a. A maximum may thus be sought in the so-called replica symmetric (RS) subspace of dimension $n+1$ where $c(\sigma)$ is left unchanged under the action of the symmetric group. Within the RS subspace, the occupation fractions may be conveniently expressed as the moments of a probability distribution $P(m)$ over the range $-1 \leq m \leq 1$ [8]. Once the number of replicas n is sent to zero, we obtain a self-consistent functional equation for the order parameter $P(m)$ that can be solved numerically.

What is the meaning of the distribution $P(m)$? Consider a formula $\mathcal{F}$ and all the spin configurations $\mathbf{S}^j$, $j = 1, \ldots, \mathcal{N}$ attaining the minimum $E[\mathbf{C}]$ of the cost-function $E[\mathbf{C},\mathbf{S}]$. Define then the average Boolean magnetisations of the spins

$$m_i = \frac{1}{\mathcal{N}} \sum_{j=1}^{\mathcal{N}} S_i^j , \tag{4}$$

over the set of optimal configurations. Call $H(\mathbf{C}, m)$ the histogram of the m_is and $H(m)$ the average of $H(\mathbf{C}, m)$ over the choices of the formulae $\mathcal{F}$. $H(m)$ is a probability distribution over the interval $-1 \leq m \leq 1$ giving information about the resulting constraints on the variables induced by the clauses. It has been shown that, if the RS solution is the global maximum of (3) (and not only a local one), $H(m)$ equals the above mentioned $P(m)$ in the limit of large sizes $N \to \infty$. Therefore, the order parameter arising in the replica calculation reflects the "microscopic" structure of the solutions of the K-SAT problem.

Of particular interest are the fully fixed variables, that is the x_i's such that $m_i = \pm 1$. In the following, the fraction of fully constrained variables will be denoted by $\gamma(\alpha, K)$. Clearly, $\gamma(\alpha, K)$ vanishes in the SAT region otherwise the addition of a new clause to $\mathcal{F}$ would lead to a contradiction with a finite probability. Two kinds of scenarii arise when entering the UNSAT phase. For 2-SAT, $\gamma(\alpha, 2)$ smoothly increases above the threshold $\alpha_c(2) = 1$. For 3-SAT (and more generally $K \geq 3$), $\gamma(\alpha, 3)$ exhibits a discontinuous jump to a finite value $\gamma_c \simeq 0.9$ slightly above the threshold. While $\alpha_c(2) = 1$ is correctly found, the RS prediction for $\alpha_c(3) = 4.6$ exceeds the experimental estimates by 10%. Work is currently under progress to refine the above calculation and enlarge the subspace where the global maximum is sought in.

Qualitatively speaking, however, we expect the main conclusion of this work to be correct: the SAT/UNSAT transition is accompanied by a smooth (respectively abrupt) change in the structure of the solutions of the 2-SAT (resp. 3-SAT) problem. Furthermore, we conjecture that this discrepancy is responsible for the difference of typical complexities of both models recently observed in numerical studies [10]. The typical solving time of search algorithms displays an easy-hard-easy pattern as a function of α with a peak of complexity close to the threshold. The peak time seems to scale polynomially with N for the 2-SAT problem and exponentially with N in the 3-SAT case. From an intuitive point of view, the search for solutions ought to be more time-consuming in the presence of a finite fraction of fixed variables since the exact determination of the latter necessarily requires an exhaustive enumeration of the variables. To test this conjecture, a mixed $2+p$-model has been introduced; it includes a fraction p (resp. $1-p$) of clauses of length two (resp. three) and thus interpolates between the 2-SAT ($p = 0$) and 3-SAT ($p = 1$) problems. The RS theory predicts that the SAT/UNSAT transition becomes abrupt when $p > p_0 = 0.41$. Precise numerical simulations support the conjecture that the polynomial/exponential crossover occurs at the same critical p_0. An additional argument in favour of this conclusion is provided by the analysis of the finite-size effects on $P_N(\alpha, K)$ and the emergence of some universality for $p < p_0$. A detailed account of these findings may be found in [7].

Bibliography

[1] Broder (Andrei Z.), Frieze (Alan M.), and Upfal (Eli). – On the satisfiability and maximum satisfiability of random 3-CNF formulas. In *Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms (Austin, TX, 1993)*. pp. 322–330. – New York, 1993.

[2] Chvátal (V.) and Reed (B.). – Miks gets some (the odds are on his side). In *Proceedings of the 33rd IEEE Symposium on Foundations of Computer Science*, pp. 620–627. – 1992.

[3] Dubois (O.) and Boufkhad (Y.). – A general upper bound for the satisfiability threshold of random r-SAT formulae. *Journal of Algorithms*, vol. 24, 1997, pp. 395–420.

[4] Frieze (Alan) and Suen (Stephen). – Analysis of two simple heuristics on a random instance of k-SAT. *Journal of Algorithms*, vol. 20, n° 2, 1996, pp. 312–355.

[5] Goerdt (Andreas). – A threshold for unsatisfiability. *Journal of Computer and System Sciences*, vol. 53, n° 3, 1996, pp. 469–486. – 1994 ACM Symposium on Parallel Algorithms and Architectures (Cape May, NJ, 1994).

[6] Mitchell (D.), Selman (B.), and Levesque (H. J.). – Hard and easy distributions of SAT problems. In *Proceedings of the American Association for Artificial Intelligence AAAI-92*, pp. 459–465. – 1992.

[7] Monasson (R.), Zecchina (R.), Kirkpatrick (S.), Selman (B.), and Troyansky (L.). – Typical-case complexity results from a new type of phase transition. – In preparation.

[8] Monasson (Rémi) and Zecchina (Riccardo). – Entropy of the K-satisfiability problem. *Physical Review Letters*, vol. 76, n° 21, 1996, pp. 3881–3885.

[9] Monasson (Rémi) and Zecchina (Riccardo). – Statistical mechanics of the random K-satisfiability model. *Physical Review E. Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics. Third Series*, vol. 56, n° 2, 1997, pp. 1357–1370.

[10] Selman (Bart) and Kirkpatrick (Scott). – Critical behavior in the computational cost of satisfiability testing. *Artificial Intelligence*, vol. 81, n° 1-2, 1996, pp. 273–295. – Frontiers in problem solving: phase transitions and complexity.

Part 2

Symbolic Computation

q-WZ-Theory and Bailey Chains

Peter Paule
RISC, J. Kepler University of Linz, Austria

February 16, 1998

[summary by Bruno Gauthier and Bruno Salvy]

Abstract

Many combinatorial identities can be formulated in terms of q-hypergeometric sums, for instance, the celebrated Rogers-Ramanujan identities from additive number theory. Identities of this type can be constructed iteratively from simpler ones, i.e., by proceeding along Bailey chains. Another construction mechanism, different from this classical one, arises within the context of q-WZ-theory. For instance, as a by-product of computer proofs, one automatically obtains the so-called "dual" identities. The talk gives a short tutorial introduction and discusses various relations between these concepts.

The talk consists of four parts. The first part is an introduction to Gaussian polynomials. The second part is a brief account of q-hypergeometric WZ theory. The parts that follow are variations on this theme.

1. Gaussian polynomials

Let $p(m,n;k)$ denote the number of partitions of k in at most m parts, each part $\leq n$. Clearly,

$$p(m,n;k) = 0, \quad \text{if } k > mn,$$
$$p(m,n;mn) = 1.$$

Therefore the generating function $G_{m,n}(q) = \sum_{k=0}^{mn} p(m,n;k)q^k$ is a polynomial in q of degree mn.

A few particular instances are:

$$G_{m,0}(q) = 1, \qquad G_{0,n}(q) = 1, \qquad G_{m,n}(q) = G_{n,m}(q), \qquad G_{m,1}(q) = \frac{1-q^{m+1}}{1-q},$$
$$G_{4,3}(q) = 1 + q + 2q^2 + 3q^3 + 4q^4 + 4q^5 + 5q^6 + 4q^7 + 4q^8 + 3q^9 + 2q^{10} + q^{11} + q^{12}.$$

From the decomposition

$$p(m,n;k) = p(m-1,n;k-n) + p(m,n-1;k) \qquad (k \geq n)$$

follows that

$$G_{m,n}(q) = q^n G_{m-1,n}(q) + G_{m,n-1}(q). \tag{1}$$

By symmetry, we also have:

$$G_{m,n}(q) = G_{m-1,n}(q) + q^m G_{m,n-1}(q). \tag{2}$$

So, by elimination between (1) and (2):

$$G_{m,n}(q) = \frac{1-q^{m+n}}{1-q^n} G_{m,m-1}(q) = \frac{(1-q^{m+n})\cdots(1-q^{m+1})}{(1-q^n)\cdots(1-q)} G_{m,0}(q).$$

Using the standard notation $(a;q)_k = (1-a)(1-aq)\cdots(1-aq^{k-1})$, $k = 1, 2, \ldots$ and $(a;q)_k = 1/(a;q)_{-k}$ for $k < 0$, we get a closed form representation of the Gaussian polynomials $G_{m,n}$:

$$\begin{bmatrix} m+n \\ n \end{bmatrix} := G_{m,n}(q) = \frac{(1-q^{m+n})\cdots(1-q^{m+1})}{(1-q^n)\cdots(1-q)} = \frac{(q;q)_{m+n}}{(q;q)_m(q;q)_n}. \tag{3}$$

2. Some facts about q-hypergeometric WZ theory

Definition 1. A sequence (t_k) is *hypergeometric* if the ratio of two consecutive terms is a rational function of the summation index k: $t_{k+1}/t_k = P(k)/Q(k)$, where P and Q are polynomials in k.

Definition 2. A sequence (t_k) is *q-hypergeometric* if the ratio of two consecutive terms is a rational function of q^k: $t_{k+1}/t_k = P(q^k)/Q(q^k)$, where P and Q are polynomials in q^k. (Note that q should be contained in the coefficient field which should be of characteristic 0.)

2.1. **From Gosper to Zeilberger.** Gosper's algorithm for indefinite hypergeometric summation [3] is given as input a hypergeometric sequence (f_k). This algorithm finds a hypergeometric sequence (g_k) such that $f_k = g_{k+1} - g_k$ (then g_k is the product of f_k and a rational function in k). From there by telescoping one gets:

$$\sum_{k=0}^{n} f_k = g_{n+1} - g_0.$$

Zeilberger's algorithm computes definite hypergeometric sums. Given a proper hypergeometric sequence $(F_{n,k})$ (with finite support in k), this algorithm finds a hypergeometric sequence (S_k) such that

$$\sum_k F_{n,k} = S_n.$$

The idea is to use an extension of Gosper's algorithm in order to find polynomials $a_j(n)$ and a proper hypergeometric term $(G_{n,k})$ such that

$$\sum_{j=0}^{J} a_j(n) F_{n+j,k} = G_{n,k+1} - G_{n,k}.$$

Then $G_{n,k}$ is necessarily of the form $R(n,k)F_{n,k}$ where R is a rational function called the "certificate". Summing this equality yields the desired recurrence on S_n:

$$\sum_{j=0}^{J} a_j(n) S_{n+j} = 0.$$

This algorithm has been implemented in Mathematica by P. Paule and M. Schorn:

Example.
```
In[1]:= <<zb_alg.m
Fast Zeilberger by Peter Paule and Markus Schorn. (V 2.2)
Systembreaker = ENullspace
In[2]:= Zb[Binomial[n,k] x^k, k, n, 1]
Out[2]= {(1 + x) F[k, n] - F[k, 1 + n] == Delta[k, R F[k, n]]}
In[3]:= Show[R]

             k
Out[3]= ---------
        1 - k + n
```

Both these algorithms extend to the q-case, a corresponding implementation in Mathematica is due to A. Riese.

2.2. **Example.** A variation of a q-analogue of Gosper's and Zeilberger's algorithms can serve in finding q-analogues of binomial identities. For instance, in order to derive a q-analogue of the binomial theorem, the question is to find $\alpha, \beta \in \mathbb{Z}$ such that the following sequence satisfies a recurrence of order one:

$$S_n(q) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k q^{\alpha\binom{k}{2}+\beta k},$$

Riese's Mathematica package `qZeil` automatically determines the candidates $\alpha \in \{1\}$, $\beta \in \mathbb{Z}$. Indeed, choosing $\alpha = 1$ and $\beta = 0$:

```
In[3]:= <<qZeil.m

Out[3]= Axel Riese's q-Zeilberger implementation version 1.8 loaded

In[4]:= qZeil[ qBinomial[n,k,q] x^k q^Binomial[k,2], {k,0,n}, n, 1]
                              -1 + n
Out[4]= SUM[n] == -((-1 - q       x) SUM[-1 + n])
```

So, we obtain the q-binomial theorem in one of its standard forms:

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k q^{\binom{k}{2}} = (1+x)(1+qx)\cdots(1+q^{n-1}x).$$

2.3. **WZ duality.** Given a hypergeometric sequence $(f_{n,k})$, assume that Zeilberger's algorithm finds a_1, a_2 and $g_{n,k}$ such that:

$$a_1(n) f_{n+1,k} + a_2(n) f_{n,k} = g_{n,k+1} - g_{n,k}.$$

Then, in case of finite support:

$$a_1(n) S_{n+1} + a_2(n) S_n = 0.$$

By using this in the form $a_2(n)/S_{n+1} = -a_1(n)/S_n$, we rewrite the relation above as:

$$\frac{a_1(n)}{S_n}\frac{f_{n+1,k}}{S_{n+1}} + \frac{a_2(n)}{S_{n+1}}\frac{f_{n,k}}{S_n} = \frac{g_{n,k+1} - g_{n,k}}{S_{n+1}S_n}.$$

Defining $F_{n,k} = f_{n,k}/S_n$, and $G_{n,k} = g_{n,k}/(a_1(n)S_{n+1})$, we arrive at:

$$F_{n+1,k} - F_{n,k} = G_{n,k+1} - G_{n,k}. \tag{4}$$

This gives rise to the following definition:

Definition 3. A pair of sequences (F, G) that satisfy (4) is called a "WZ pair".

Note that given such a WZ-pair (F having finite support), from (4) follows that $\sum_k F_{n+1,k} - \sum_k F_{n,k} = 0$, which means that the corresponding sum sequence $S_n := \sum_k F(n,k)$ is a constant.

3. A Fibonacci q-analogue

The well-known Fibonacci numbers are defined by $F_0 = 1, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$. Does there exist a q-analogue of these numbers? In order to follow the strategy explained above (example 2.2), we take as a starting point the following well-known hypergeometric sum:

$$F_n = \sum_{k=0}^{n} \binom{n-k}{k}.$$

For the (α, β)-Ansatz, we take:

$$F_n(q) = \sum_{k=0}^{n} \begin{bmatrix} n-k \\ k \end{bmatrix} q^{\alpha\binom{k}{2}+\beta k},$$

and we want to determine $\alpha, \beta \in \mathbb{Z}$ such that $(F_n(q))$ satisfies a linear recurrence of order 2. Riese's implementation delivers as candidates: $\alpha \in \{1, 2, 3\}$ and $\beta \in \mathbb{Z}$, but only the choice $\alpha = 2$ is successful. This means, only for $\alpha = 2$, the q-analogue of Zeilberger's algorithm delivers $(\forall \beta \in \mathbb{Z})$ a recurrence of order 2, namely:

$$F_{n+2}(q) = F_{n+1}(q) + q^{n+\beta} F_n(q). \tag{5}$$

Let us fix (for instance) $\beta = 1$, and we obtain for this choice:

$$F_n(q) = \sum_{k=0}^{n} \begin{bmatrix} n-k \\ k \end{bmatrix} q^{k^2}.$$

In the limit $n \to \infty$:

$$F_\infty(q) = \sum_{k=0}^{\infty} \frac{q^{k^2}}{(q;q)_k} = 1 + \sum_{n=1}^{\infty} b_n q^n = \prod_{k=1}^{\infty} \frac{1}{(1-q^{5n+1})(1-q^{5n+4})}, \tag{6}$$

where b_n is the number of partitions of n into parts with minimal difference two and the right-hand side is one of the celebrated Rogers-Ramanujan identities [1].

Starting from (5), it is also possible to conjecture and then prove (by q-Zeilberger) the following identity due to I. Schur

$$F_{2n}(q) = \sum_k q^{k(10k+1)} \begin{bmatrix} 2n \\ n-5k \end{bmatrix} - \sum_k q^{(2k-1)(5k-2)} \begin{bmatrix} 2n \\ n-5k+2 \end{bmatrix}.$$

4. The Bailey chain approach

Proposition 1.

$$\sum_{j=0}^{n} \frac{q^{j^2-k^2}}{(q;q)_{n-j}} \frac{(q;q)_{n-k}(q;q)_{n+k}}{(q;q)_{j-k}(q;q)_{j+k}} = 1. \tag{7}$$

Proof. Denote by $f_{n,j}$ the summand. Riese's implementation yields:

$$f_{n,j} - f_{n-1,j} = g_{n,j} - g_{n,j-1}, \qquad \text{where} \qquad g_{n,j} = \frac{q^{k+n}(q^j - q^n)}{(q^n - q^k)(1-q^{k+n})} f_{n,j}.$$

This (q)WZ-pair implies that the sum over $f_{n,j}$ is constant. That this constant is 1 follows from instance from the evaluation for $n = k$ [1, 4]. □

This identity is a special case of a q-hypergeometric formula that can be proved combinatorially as explained in [4].

Multiplying (7) by an arbitrary sequence (c_k), we obtain the following special case of "Bailey's Lemma":

$$\sum_k \frac{c_k}{(q;q)_{n-k}(q;q)_{n+k}} = \sum_{j\geq 0} \frac{q^{j^2}}{(q;q)_{n-j}} \sum_k \frac{c_k q^{-k^2}}{(q;q)_{j-k}(q;q)_{j+k}}. \tag{8}$$

Definition 4. Two sequences $((a)_{k\in\mathbb{Z}}, (b)_{n\in\mathbb{N}})$ are called a *Bailey-pair* when

$$b_n = \sum_k \frac{a_k}{(q;q)_{n-k}(q;q)_{n+k}}.$$

Now, let's walk in a "Bailey-chain" (using proposition 1) starting with: $a_k = q^{\binom{k}{2}}(-1)^k$ and b_n as above. Using `qZeil`, we get:

$$b_n = \sum_k \frac{q^{\binom{k}{2}} x^k}{(q;q)_{n-k}(q;q)_{n+k}} = \frac{(-x;q)_n(-q/x;q)_n}{(q;q)_{2n}}.$$

Note that in the limit $n \to \infty$, this turns into Jacobi's triple product identity:

$$\sum_k q^{\binom{k}{2}} x^k = \prod_{j=1}^{\infty} (1-q^j)(1+q^{j-1}x)(1+\frac{q^j}{x}).$$

From there (6) follows when substituting q by q^5 and x by $-q^2$.

Now, with $c_k = q^{k^2} a_k$ and $x = -1$, (8) yields an identity due to Rogers:

$$\sum_k \frac{(-1)^k q^{\frac{3}{2}k^2 - \frac{1}{2}k}}{(q;q)_{n-k}(q;q)_{n+k}} = \frac{1}{(q;q)_n},$$

which can be found by the q-Zeilberger algorithm after "creative symmetrizing" (i.e., multiplying the summand by $1+q^k$ in this example).

The second step in the Bailey chain approach uses $c_k = q^{2k^2} a_k$. This gives:

$$\sum_k \frac{(-1)^k q^{\frac{5}{2}k^2 - \frac{1}{2}k}}{(q;q)_{n-k}(q;q)_{n+k}} = \sum_{j\geq 0} \frac{q^{j^2}}{(q;q)_{n-j}(q;q)_j}.$$

In the limit $n \to \infty$ and by Jacobi's triple product identity, this gives again (6). The third step of the Bailey chain gives:

$$\sum_k \frac{(-1)^k q^{\frac{7}{2}k^2 - \frac{1}{2}k}}{(q;q)_{n-k}(q;q)_{n+k}} = \sum_{j\geq 0} \frac{q^{j^2}}{(q;q)_{n-j}} \sum_{l=0}^{j} \frac{q^{l^2}}{(q;q)_{j-l}(q;q)_l},$$

resulting when $n \to \infty$ in an identity due to B. Gordon

$$\frac{1}{(q;q)_\infty} \prod_{n=0}^{\infty} (1-q^{7n+3})(1-q^{7n+4})(1-q^{7n+7}) = \sum_{l,j=0}^{\infty} \frac{q^{(j+l)^2+l^2}}{(q;q)_j(q;q)_l},$$

whose first automatic proof was given by Chyzak [2].

Bibliography

[1] Andrews (George E.). – *q-series: their development and application in analysis, number theory, combinatorics, physics, and computer algebra.* – Published for the Conference Board of the Mathematical Sciences, Washington, D.C., 1986, *CBMS Regional Conference Series in Mathematics*, vol. 66, xii+130p.

[2] Chyzak (Frédéric). – Groebner bases, symbolic summation and symbolic integration. In Buchberger (B.) and Winkler (F.) (editors), *Groebner Bases and Applications.* – Cambridge University Press, 1998. Proceedings of the Conference 33 Years of Gröbner Bases.

[3] Gosper (R. William). – Decision procedure for indefinite hypergeometric summation. *Proceedings of the National Academy of Sciences USA*, vol. 75, n° 1, January 1978, pp. 40–42.

[4] Paule (Peter). – Über das Involutionsprinzip von Garsia und Milne. *Bayreuther Mathematische Schriften*, n° 21, 1986, pp. 295–319. – Diskrete Strukturen, algebraische Methoden und Anwendungen (Bayreuth, 1985).

[5] Paule (Peter) and Riese (Axel). – A Mathematica q-analogue of Zeilberger's algorithm based on an algebraically motivated approach to q-hypergeometric telescoping. In *Special functions, q-series and related topics*, pp. 179–210. – American Mathematical Society, Providence, RI, 1997. Proceedings of a workshop held in Toronto, ON, June 1995.

[6] Paule (Peter) and Schorn (Markus). – A Mathematica version of Zeilberger's algorithm for proving binomial coefficient identities. *Journal of Symbolic Computation*, vol. 20, 1995, pp. 673–698.

[7] Petkovšek (Marko), Wilf (Herbert), and Zeilberger (Doron). – $A = B$. – A. K. Peters, Wellesley, MA, 1996, xii+212p.

Summability of Power Series Solutions of q-Difference Equations

Changgui Zhang
Université de La Rochelle

January 19, 1998

[summary by Michèle Loday-Richaud]

The $\mathbb{C}$-algebra $\mathbb{C}\{x\}[\sigma_q]$ of (linear analytic) q-difference operators is the algebra of polynomials in σ_q where $\sigma_q x = qx\sigma_q$ and where the coefficients are taken in the algebra $\mathbb{C}\{x\}$ of convergent power series at $x = 0$ in $\mathbb{C}$. The elementary operator σ_q acts on x by multiplication by the number q and we make it act on functions of x by $\sigma_q f(x) = f(qx)$. The theory is very different depending on whether $|q|$ is smaller, equal or greater than 1. We deal here with the case when $|q| > 1$ and, for simplicity, we assume that q is a real number.

Like differential equations, q-difference equations may have divergent power series solutions and the aim is to develop a theory of summability for such series like it has been done by Martinet-Ramis and Écalle for solutions of differential equations. A theory of summability means having a rule to change in a unique well-defined way a series solution into an actual solution.

The similarity with differential equations is very strong. However new concepts had to be developed and new phenomena occur.

1. Jacobi equation

The simplest non trivial example is given by the Theta series

$$\Theta(x) = \sum_{n\geq 0} q^{n(n-1)/2} x^n,$$

solution of the Jacobi q-difference equation

$$(J) \qquad xy(qx) - y(x) = -1.$$

The Θ series can be viewed as an analog of the Euler series

$$\sum_{n\geq 0} (-1)^n n! x^{n+1}$$

solution of the Euler equation

$$x^2 y' + y = x.$$

The function

$$y(x) = q^{-\frac{1}{2}(\log_q x - 1)\log_q x},$$

solution of the homogeneous q-difference equation $xy(qx) - y(x) = 0$, is the analog of the exponential function $\exp(1/x)$, solution of the homogeneous differential equation $x^2y' + y = 0$ and it plays with respect to (J) a like role. Notice however that the series Θ is more divergent than the series solutions of linear differential equations which are known to be of Gevrey type.

Letting
$$y = zq^{-\frac{1}{2}(\log_q x - 1)\log_q x}$$
changes (J) into the equation
$$z(qx) - z(x) = -q^{\frac{1}{2}(\log_q x - 1)\log_q x}$$
and, letting then $x = q^t$ and $u(t) = z(x)$, into the equation
$$(\Delta) \qquad u(t+1) - u(t) = -q^{\frac{1}{2}(t-1)t}.$$
This latter equation is a linear difference equation the second member of which has an essential singularity at infinity. However the Fourier method can be used to solve it as follows.

Denote by
$$\mathcal{F}(u(t))(\tau) = \frac{1}{2i\pi}\int_{a-i\infty}^{a+i\infty} u(t)e^{-\tau t}dt \qquad \text{and} \qquad \mathcal{F}^{-1}(\varphi(\tau))(t) = \int_{-\infty+ib}^{+\infty+ib} \varphi(\tau)e^{\tau t}d\tau$$
the Fourier and the inverse Fourier transform. Assume that a solution $u(t)$ of (Δ) is left invariant by successive application of $\mathcal{F}$ and $\mathcal{F}^{-1}$. Using the identity $\mathcal{F}(u(t+1))(\tau) = e^{\tau}\mathcal{F}(u(t))(\tau)$ we get
$$\mathcal{F}(u(t))(\tau) = \frac{1}{\sqrt{2\pi \log q}} \frac{q^{-\frac{1}{2}(\frac{1}{2}+\frac{\tau}{\log q})^2}}{1-e^{\tau}}$$
and then solutions of (Δ) in the form
$$u_\theta(t) = \frac{1}{\sqrt{2\pi \log q}} \int_{-\infty+i\theta_q}^{+\infty+i\theta_q} \frac{q^{-\frac{1}{2}(\frac{1}{2}+\frac{\tau}{\log q})^2}}{1-e^{\tau}} e^{\tau t}d\tau.$$
There correspond the following solutions of (J) defined on all of the Riemann surface of log:
$$y_\theta(x) = \frac{q^{-1/8}}{\sqrt{2\pi \log q}} \int_{d_\theta} q^{-\frac{1}{2}(\log_q \frac{x}{\zeta} - 1)\log_q \frac{x}{\zeta}} \frac{1}{\zeta(1-\zeta)} d\zeta$$
the integral being taken on the half line d_θ starting from 0 to infinity with angular direction $\theta = \theta_q \log q$ provided that $\theta \neq 0 \bmod 2\pi$. When θ varies between two successive forbidden values $2k\pi$ and $2(k+1)\pi$ the corresponding $y_\theta(x)$ are equal. When θ is taken in different such intervals they are equal up to a multiplicative q-constant (a q-constant is a constant in the algebra $\mathbb{C}\{x\}[\sigma_q]$, i.e., a function $C(x)$ satisfying $C(qx) = C(x)$). Thus we can concentrate on one of them. We choose $\theta \in]0, 2\pi[$ and denote by f_0 the corresponding y_θ solution. Such a solution can be taken as a model for q-sums of q-Borel-Laplace summable series.

We emphasize its main property. Writing, for all $\xi \neq 1$, the identity $1/(1-\xi) = \sum_{m=0}^{n-1} \xi^m + \xi^n/(1-\xi)$ yields the equality
$$f_0(x) = \sum_{m=0}^{n-1} q^{m(m-1)/2}x^m + \frac{q^{-1/8}}{\sqrt{2\pi \log q}} \int_{d_\theta} q^{-\frac{1}{2}(\log_q \frac{x}{\xi} - 1)\log_q \frac{x}{\xi}} \frac{\xi^{n-1}}{\xi(1-\xi)} d\xi$$
and then the inequality
$$\left| f_0(x) - \sum_{m=0}^{n-1} q^{m(m-1)/2}x^m \right| \leq C_\theta q^{\frac{n(n-1)}{2} + \frac{1}{2}\arg_q^2(xe^{-i\theta})} |x|^n$$
where C_θ is the constant $C_\theta = \max(1, 1/|\sin\theta|)$ and $\arg_q = \frac{1}{\log q}\arg$. Note that the constant C_θ is locally uniform in θ. Such a condition can be taken as a model for f_0 to be the q-sum of level 1 of its Taylor series $\sum_{m\geq 0} q^{m(m-1)/2}x^m$.

We will see that, in all generality, q-Borel-Laplace summable series and q-summable series of level 1 are the same series.

2. q-Borel-Laplace summability or q-summability of level 1

Translating the Fourier and inverse Fourier transforms in terms of the variables $x = q^t$ and $\xi = q^\tau$ yields the q-Borel and q-Laplace transforms

$$\mathcal{B}q(f)(\xi) = \frac{-iq^{1/8}}{\sqrt{2\pi \log q}} \int_{|x|=\rho} q^{\frac{1}{2}(\log_q \frac{x}{\xi} - 1)\log_q \frac{x}{\xi}} f(x) \frac{dx}{x},$$
$$\mathcal{L}q^\theta(\varphi)(x) = \frac{q^{-1/8}}{\sqrt{2\pi \log q}} \int_{d_\theta} q^{-\frac{1}{2}(\log_q \frac{x}{\xi} - 1)\log_q \frac{x}{\xi}} \varphi(\xi) \frac{d\xi}{\xi},$$

where $\rho > 0$ is chosen small enough for $f(x)$ to exist. The formal analog of $\mathcal{B}q$ is given by

$$\widehat{\mathcal{B}q}(\sum_{n\geq 0} a_n x^n) = \sum_{n\geq 0} \frac{a_n \xi^n}{q^{n(n-1)/2}}.$$

Definition 1. A series $\sum_{n\geq 0} a_n x^n$ is a q-Borel-Laplace summable series for the direction θ if it can be applied a q-Borel and q-Laplace transform relative to the direction θ and close directions.

The Theta series is the typical example of a q-Borel-Laplace summable series.

Definition 2. – A series $\sum_{n\geq 0} a_n x^n$ is of q-Gevrey type (of level 1) if it satisfies a growth condition $|a_n| \leq K q^{n(n-1)/2} A^n$ for all n and suitable constants K and A.

– A function f is q-asymptotic of level 1 to a series $\widehat{f}(x) = \sum_{n\geq 0} a_n x^n$ for the direction θ if, for suitable constants $K_\theta > 0$ and $A_\theta > 0$, the inequality

$$(*_\theta) \qquad \left| f(x) - \sum_{m=0}^{n-1} a_m x^m \right| \leq K_\theta q^{\frac{1}{2}(n^2 + \arg_q(xe^{-i\theta}))} A_\theta^n |x|^n$$

holds for all n and small enough x on the Riemann surface of Log.

The Jacobi function f_0 is q-asymptotic to the Theta series for all directions but the directions $\theta = 0 \bmod 2\pi$.

A q-asymptotic expansion is also an asymptotic expansion in the usual Poincaré sense. Hence, if it exists, it is unique and can be called the Taylor series of the function. There exist q-flat functions. However one has the following result.

Proposition 1. *The unique function to be q-flat in two different directions is the null function.*

Definition 3. A series $\widehat{f}(x) = \sum_{n\geq 0} a_n x^n$ is said q-summable of level 1 with q-sum f for the direction θ if the condition $(*_\theta)$ holds locally uniformly with respect to θ, i.e., if there exist a neighbourhood $(\theta - \varepsilon, \theta + \varepsilon)$ of θ and constants K and A such that

$$(**_\theta) \qquad \left| f(x) - \sum_{m=0}^{n-1} a_m x^m \right| \leq K q^{\frac{1}{2}(n^2 + \arg_q(xe^{-i\tilde{\theta}}))} A^n |x|^n$$

for all n, all $\tilde{\theta} \in (\theta - \varepsilon, \theta + \varepsilon)$ and all small enough x.

It results from Proposition 1 that the q-sum of level 1 of $\widehat{f}$ if it exists for the direction θ is unique.

Theorem 1. *A series is q-summable of level 1 for the direction θ if and only if it is q-Borel-Laplace summable in the direction θ and the sums are equal.*

Definition 4. A series $\widehat{f}(x) = \sum a_n x^n$ is said q-summable of level 1 (or q-Borel-Laplace summable) if it is q-summable of level 1 for all directions but locally finitely many which are called singular directions.

The series Theta is q-summable of level 1 with singular directions $\theta = 0 \bmod 2\pi$.
One can extend the previous notions to any level k by substituting x^k to x or so.

3. Summability of series solutions of q-difference equations

Using the elementary operator σ_q instead of the derivation $\frac{d}{dx}$ one can define the Newton polygon of a linear q-difference operator like it can be done for a linear differential operator. A fundamental set of formal solutions was given by Adams in [1]. It is made of finite linear combinations of terms of the form

$$\widehat{f}(x) x^{\alpha} \log^m x \, e^{\frac{\mu}{2}\log^2 x} \quad \text{where} \quad \alpha \in \mathbb{C}, m \in \mathbb{N}, \mu \in \mathbb{Q}$$

and where $\widehat{f}(x)$ is a power series (possibly in a fractional power of x). The numbers μ are the different slopes of the Newton polygon $N(\Delta)$. It was proved by Carmichael [2] that when $N(\Delta)$ has the unique slope 0 then there are no exponential terms and all the power series are convergent. The origin 0 is then either an ordinary or a regular singular point.

When there is the slope 0 and a non zero slope then the origin 0 is an irregular singular point; the number of solutions without an exponential factor is equal to the length of the zero slope. Those solutions we will call the formal series solutions even though they can contain a factor $x^{\alpha}\log^m x$.

Theorem 2. *Suppose that the Newton polygon $N(\Delta)$ of a linear q-difference operator Δ admits a unique non zero slope equal to k. Then, the formal series solutions of Δ are q-summable of level k.*

Following the same kind of idea one can also define q-accelerators like it was done by J. Écalle for differential and difference equations and introduce a notion of q-accelero-summability, also called q-multisummability for finitely many levels $\mu_1, \ldots, \mu_p$.

Theorem 3. *Suppose that the Newton polygon $N(\Delta)$ of a linear q-difference operator Δ admits the non zero slopes $\mu_1, \ldots, \mu_p$. Then, the formal series solutions of Δ are q-multisummable of levels $(\mu_1, \ldots, \mu_p)$.*

Proposition 2. *q-summable series of level k are naturally given a structure of $\mathbb{C}\{x\}$-module, not a structure of algebra.*

For example, if $\widehat{f}$ is a non convergent q-summable series of level 1 then $\widehat{f}^2$ is not q-summable of any level k; however it is q-multisummable of levels $(1, 2)$.

Bibliography

[1] Adams (C. R.). – Linear q-difference equations. *Bulletin of the American Mathematical Society*, 1931, pp. 361–382.
[2] Carmichael (R. D.). – The general theory of q-difference equations. *American Journal of Mathematics*, vol. 34, 1912, pp. 146–168.
[3] Zhang (Changgui). – Les développements asymptotiques q-gevrey, les séries Gq-sommables et leurs applications. *Annales de l'Institut Fourier*, 1998. – To appear.

Isolde, a Package for Computing Invariants of Systems of Ordinary Linear Differential Equations

Eckhard Pflügel
LMC-IMAG, Grenoble

October 6, 1997

[summary by Frédéric Chyzak]

The Maple package Isolde is a package for studying and solving systems of linear differential equations. More specifically, it deals with two main kinds of problems:

- local problems: compute *formal invariants* at a point; compute *formal solutions* at a point;
- global problems: compute *closed form* solutions in a certain class, like that of polynomial, rational, or exponential functions.

The approach followed is a direct treatment of the system, avoiding any method akin to that of *cyclic vectors*. Formal invariants of linear first-order differential systems are introduced in the next section, where we also briefly list the operations available in Isolde. Then, we focus in the last two sections on an efficient algorithm due to E. Pflügel to search for *exponential solutions* [4].

The package Isolde is developed by A. Barkatou and E. Pflügel and is available at

`http://www-lmc.imag.fr/CF/logiciel.html`.

1. Formal Invariants, Formal Solutions, Closed Form Solutions

For a subfield $\mathbb{K}$ of the field $\mathbb{C}$ of complex numbers with algebraic closure $\overline{\mathbb{K}}$, and a matrix $A \in \mathcal{M}_n(\mathbb{K}(x))$, consider the linear first-order differential system

$$Y' = AY. \tag{1}$$

One either looks for vector solutions or for matrix solutions, i.e., whose columns are vector solutions. A *formal fundamental matrix* at $x_0 \in \overline{\mathbb{K}} \cup \{\infty\}$ is a matrix solution of rank n of the form [6]

$$\Phi(t) = H(t)t^{\Lambda}e^{Q(t)} \qquad \text{where } t^r = x - x_0 \text{ for a positive integer } r, \tag{2}$$

for a matrix of formal power series $H \in \mathcal{M}_n(\overline{\mathbb{K}})[[t]]$, a constant matrix $\Lambda \in \mathcal{M}_n(\overline{\mathbb{K}})$ and a diagonal matrix Q with Laurent polynomial entries in $t^{-1}\overline{\mathbb{K}}[t^{-1}]$. Note that

$$\Phi(t) = H(t)\exp\left(\int W(t)\,dt\right) \qquad \text{for } W = \Lambda t^{-1} + Q' \in t^{-1}\mathcal{M}_n(\overline{\mathbb{K}})[t^{-1}].$$

The expression $\exp\left(\int W(t)\,dt\right) = t^{\Lambda}e^{Q(t)}$ is called the *exponential part* of Φ. A *formal invariant* is any quantity appearing in or related to Φ, like Newton polygons, Newton polynomials, exponential parts and *formal solutions*, i.e., linear combinations of columns of Φ. Formal solutions are asymptotic expansions of functional solutions near x_0. Their general expression is

$$y(t) = z(t)t^{\lambda}e^{q(t)} = z(t)\exp\left(\int w(t)\,dt\right) \tag{3}$$

with $z(t) = z_0(t) + z_1(t)\ln t + \cdots + z_s(t)\ln^s t$ for vectors $z_i \in \overline{\mathbb{K}}[[t]]^n$, a constant $\lambda \in \overline{\mathbb{K}}$ and a Laurent polynomial $q \in t^{-1}\overline{\mathbb{K}}[t^{-1}]$. Here again $w = \lambda t^{-1} + q'$. ISOLDE implements algorithms to compute several formal invariants, in particular exponential parts and formal solutions.

Specialized algorithms have been developed to solve for solutions in several elementary classes of closed form expressions. Their principle is that local data contains essential information on potential closed form solutions. In particular, ISOLDE implements algorithms to solve for:

- *polynomial solutions*, that are related to formal solutions at ∞ with trivial exponential parts and with no logarithmic component;
- *rational solutions*, whose denominators are bounded by computing the *indicial equation* (i.e., the Newton polynomial of slope 0) at all finite singularities;
- *exponential solutions*, for which candidates can be computed from the exponential parts at all singularities, as detailed in the next two sections.

2. Exponential Solutions

We now use the formal invariants previously introduced to compute *exponential solutions* of a linear differential system. Throughout this section, we assume that we know the set of all possible exponential parts of exponential solutions, whose determination is the topic of the next section.

An *exponential solution* is a vector solution y obtained when the vector z in the general expression (3) reduces to a polynomial vector:

$$y(x) = p(x)\exp\left(\int u(x)\,dx\right) \qquad \text{for } u \in \overline{\mathbb{K}}(x) \text{ and } p \in \overline{\mathbb{K}}[x]^n.$$

As an example, an exponential solution of the system described by the matrix

$$(4) \qquad A = \begin{bmatrix} \frac{-7}{x^2} & -x^2 & \frac{x^2}{1-x} \\ \frac{6-2x+x^2}{x^6(1-x)} & \frac{1}{x^2} & \frac{-4+9x}{x(1-x)^2} \\ \frac{8-8x+5x^2}{x^6} & \frac{1-x}{x^2} & \frac{-4+8x}{x(1-x)} \end{bmatrix} \text{ is } \exp\left(\int u\,dx\right)\begin{bmatrix} 0 \\ 1 \\ 1-x \end{bmatrix}, \text{ where } u = \frac{1}{x^2} - \frac{4}{x} + \frac{5}{1-x}.$$

Note the more explicit form $\exp\left(\int u\,dx\right) = x^{-4}(1-x)^{-5}\exp(-x^{-1})$.

Methods to determine exponential solutions of a system first evaluate or give constraints on the exponential part before computing the polynomial part p. This bases on the *local analysis* of u. One distinguishes between the *singular* and *regular* parts $S_{x_0}(u)$ and $R_{x_0}(u)$ of u at a point $x_0 \in \overline{\mathbb{K}} \cup \{\infty\}$, defined by:

$$u = S_{x_0}(u) + R_{x_0}(u), \qquad \text{with } S_{x_0}(u) \in t^{-1}\overline{\mathbb{K}}[t^{-1}] \text{ and } R_{x_0}(u) \in \overline{\mathbb{K}}[[t]].$$

For the example above, one gets

$$S_0(u) = \frac{1}{t^2} - \frac{4}{t} \qquad \text{and} \qquad R_0(u) = 5 + 5t + 5t^2 + \cdots$$

Basic known algorithms allow us:

1. for each singularity x_0 of a given rational function u, to compute the singular parts $S_{x_0}(u)$ and a finite number of terms of the regular parts $R_{x_0}(u)$ in an efficient way;
2. to reconstruct a rational function u from its singular parts at all its singularities.

Two different methods based on these algorithms allow the calculation of exponential solutions:

1. Beke's method:
   (a) compute candidates for u by combining the singular parts allowed at all singularities;
   (b) set $Y = Z\exp\left(\int u\,dx\right)$ and search for polynomial solutions Z.
2. Alternative approach based on Padé approximants:

(a) bound numerator and denominator of u;
(b) determine the singular part $S_{x_0}(u)$ of u at a (single) singularity x_0 so as to be able to compute a Padé approximant for $R_{x_0}(u)$ next.

The methods contrast to one another inasmuch as Beke's method requires splitting fields for its completeness but avoids the use of Gröbner bases, while the alternative Padé-based approach does not appeal to splitting fields but generally requires Gröbner bases. Besides, note the combinatorial exponential complexity of step (a) in Beke's algorithm.

Solving the example (4) by Beke's method, one first obtains the following sets of exponential parts at 0 and 1:

$$E_0 = \left\{ \frac{1}{x^2} - \frac{4}{x}, \frac{\alpha}{x^2} + \frac{20\alpha - 44}{57x} \right\}, \qquad E_1 = \left\{ 0, \frac{5}{1-x} \right\}, \qquad \text{where } \alpha^2 + 7\alpha - 2 = 0.$$

With this simple example, this yields only two candidates:

$$u_1 = \frac{1}{x^2} - \frac{4}{x} + \frac{5}{1-x} \qquad \text{and} \qquad u_2 = \frac{\alpha}{x^2} + \frac{20\alpha - 44}{57x}\frac{5}{1-x}.$$

With the first candidate, the system (1) reduces to $Z' = (A - u_1)Z$. One then verifies that it admits the polynomial solution already mentioned in (4).

For a formal solution $y = z \exp\left(\int w\, dt\right)$ such that z has valuation 0 at x_0, w is called a *generalized exponent*. Noticing that each $S_{x_0}(u)$ is a generalized exponent, the idea of the second method is to compute $R_{x_0}(u)$ from a formal series solution, more specifically from the series z after setting $w = S_{x_0}(u)$. More explicitly, for an exponential solution $y = p \exp\left(\int u\, dt\right)$ with logarithmic derivative U, we have $S_{x_0}(u) = S_{x_0}(U)$, so that

$$R_{x_0}(U) = R_{x_0}(u) + (\ln p)' = (\ln z)'$$

is a vector of rational functions, which can be computed from z as a Padé approximant. By integration, one obtains $R_{x_0}(u)$ as the rational part and p as the logarithmic part, next an exponential solution if there exists any for this u.

Following up the example (4), choosing the singularity $x_0 = 0$ and the exponential part candidate $w = S_0(u) = x^{-2} - 4x^{-1}$, one first computes the following formal solution (at 0):

$$y = \exp\left(\int S_0(u)\, dx\right) \begin{bmatrix} 0 \\ 1 + 5x + 15x^2 + \cdots \\ 1 + 4x + 14x^2 + \cdots \end{bmatrix}.$$

Taking the logarithmic derivative and computing Padé approximations yields

$$R_0(U) = \begin{bmatrix} 0 \\ 5 + 5x + \cdots \\ 4 + 4x + \cdots \end{bmatrix} = \begin{bmatrix} 0 \\ \frac{5}{1-x} \\ \frac{4}{1-x} \end{bmatrix} = - \begin{bmatrix} 0 \\ \ln(1-x)^5 \\ \ln(1-x)^4 \end{bmatrix}',$$

from which one gets the exponential solution already mentioned in (4).

3. **Exponential Parts**

To complete the description of the previous algorithms, we finally describe how to compute all possible exponential parts of solutions of a linear first-order ordinary differential system.

As opposed to the case of a (single) scalar higher order ODE, exponential parts cannot be obtained immediately in the case of the system (1). An obvious indirect method is to compute the Newton polygon by transforming it into an nth order scalar equation, which becomes very costly with the increase of n. This is why several other methods have been developed to transform the initial matrix A into a form from which exponential parts can be read off. All such methods use two special transformations:

1. the change of unknown $Y = TZ$, where T is a polynomial matrix with non-zero determinant transforms the system (1) into the equivalent system $Z' = (T^{-1}AT - T^{-1}T')Z$;
2. the change of exponential part $Y = Z \exp\left(\int a\, dt\right)$ leads to the new system $Z' = (A - a)Z$.

Using the above, algorithms have been proposed to put a differential system into:

1. *companion form*, as obtained by the method of *cyclic vectors*;
2. Turrittin's *canonical form* [5], however obtained by a not so constructive process;
3. Moser's *irreducible form* [3];
4. Hilali's and Wazner's *super irreducible form*, a refined version of Moser's form [2].

We now comment on applications of the last two forms. If a system

$$x^{q+1}Y' = AY, \qquad \text{for a series } A = A_0 + A_1x + \cdots \tag{5}$$

admits a solution of the form

$$z \exp\left(\int \frac{a}{x^{q+1}}\, dx\right), \tag{6}$$

then the matrix $A_0 - a$ necessarily has a zero determinant. Elaborating on this fact, Moser [3] proved that when A is an *irreducible system*, if A_0 is not nilpotent and a is a non-zero root of $\det(A_0 - \lambda)$ with multiplicity m, then there exist m solutions of A of the form (6). Based on this, Barkatou used diagonalization by blocks to devise an algorithm to compute exponential parts [1].

Similarly, a necessary condition for a system like (5) to admit a solution of the form

$$z \exp\left(\int \frac{a}{x^{k+1}}\, dx\right), \qquad \text{for } 0 \le k \le q,$$

takes the form $\det(N_0 - aD_0) = 0$ for two matrices N_0 and D_0 computed from $A_0, \ldots, A_{q-k}$. Consider the non-zero polynomial

$$\theta_k(\lambda) = x^s \det(x^{-k}A + \lambda)|_{x=0}$$

obtained for the appropriate exponent s. Hilali and Wazner [2] proved that when A is a *super irreducible system*, if a is a non-zero root of multiplicity m of the polynomial θ_k, then there exist precisely m generalized exponents equal to $-ax^{-(q-k)}$ up to higher valuation terms. Using this fact, Pflügel [4] obtained a recursive algorithm to compute all exponential parts *of ramification 1*, i.e., for the case $r = 1$ in (2). The case of higher ramifications r is work in progress.

Bibliography

[1] Barkatou (M. A.). – An algorithm to compute the exponential part of a formal fundamental matrix solution of a linear differential system. *Applicable Algebra in Engineering, Communication and Computing*, vol. 8, n° 1, 1997, pp. 1–23.

[2] Hilali (A.) and Wazner (A.). – Formes super-irréductibles des systèmes différentiels linéaires. *Numerische Mathematik*, vol. 50, n° 4, 1987, pp. 429–449.

[3] Moser (Jürgen). – The order of a singularity in Fuchs' theory. *Mathematische Zeitschrift*, vol. 72, 1959/1960, pp. 379–398.

[4] Pflügel (Eckhard). – An algorithm for computing exponential solutions of first order linear differential equations. In Küchlin (Wolfgang W.) (editor), *ISSAC'97 (July 21–23, 1997. Maui, Hawaii, USA)*. pp. 164–171. – ACM Press, 1997. Proceedings of ISSAC'97. ISBN 0-89791-875-4.

[5] Turrittin (H. L.). – Reduction of ordinary differential equations to the Birkhoff canonical form. *Transactions of the American Mathematical Society*, vol. 107, 1963, pp. 485–507.

[6] Wasow (Wolfgang). – *Asymptotic expansions for ordinary differential equations.* – Dover Publications Inc., New York, 1987, x+374p. Reprint of the John Wiley 1976 edition.

Algebra and Algorithms for Differential Systems

Évelyne Hubert
University of Waterloo, Ontario[1]

May 14, 1998

[summary by François Ollivier]

Abstract

This talk investigates algorithmic issues related to the formal resolution of algebraic differential systems, with a stress on the problem of testing components inclusion. Index reduction and applications to control theory are also considered.

News are also given of the `diffalg2` maple package which improves upon Boulier's work and will be part of a future Maple distribution.

1. Basic Algebraic Results

1.1. **Differential Algebras.** Details may be found in the classical book by Ritt [12], which remains an illuminating reference. The two first chapters provide a clear exposition of basic definitions and results. Some details on the low power theorem may be found in chapter 3. The book by Kolchin [9] is a reference book reserved to those having a good familiarity with the subject. Chapter 2 of Buium's book [3] is also a good introduction to differential algebra. The remaining chapters may be quite hard without a good previous knowledge of "modern" algebraic geometry, but contain many interesting new results. The paper [6], and thesis [8] contain details on the components problem. Details on Boulier's algorithm can also be found in [1, 2].

Differential algebra is a generalization of classical commutative algebra. We complete the ring structure with the datum of a set of mutually commuting derivations $\Delta = \{\delta_1, \dots, \delta_n\}$. We may then define differential fields, modules and algebras in a straightforward way. A differential ideal of a differential ring A is an ideal I such that $\delta I \subset I$, for all $\delta \in \Delta$. Let A be a differential ring, and I be a differential ideal, then A/I has a natural structure of differential ring. The smallest differential ideal containing a set Σ is denoted by $[\Sigma]$.

We define differential polynomials in the following way: if A is a differential ring with derivation set Δ, Θ the free commutative monoid generated by Δ and X a set, the differential polynomial algebra $A\{X\}$ is the polynomial algebra $A[\Theta X]$ equipped with the only derivation set whose action restricted to A and ΘX is that of Δ.

Let A be a Ritt ring, i.e. a differential ring containing $\mathbb{Q}$. Then for every differential ideal $I \subset A$, the radical ideal $\sqrt{I}$ is differential. A differential ring A is radically Noetherian if for every set $\Sigma \subset A$ there exists a finite set B such that $\sqrt{[\Sigma]} = \sqrt{[B]}$. In the sequel, we will denote the perfect closure $\sqrt{[\Sigma]}$ by $\{\Sigma\}$.

Theorem 1 (Ritt-Raudenbush). *If A is radically Noetherian, then for all finite set X, $A\{X\}$ is radically Noetherian.*

[1] `http://daisy.uwaterloo.ca:80/~ehubert/Diffalg/`

Corollary 1. *Le I be a radical differential ideal, then I is a finite intersection of prime ideals $\cap_{i=1}^{r}\mathcal{P}_i$.*

1.2. **Differential Field Extensions.** Let $\mathcal{F}$ be a differential field, and $\mathcal{P}$ be a prime differential ideal of $\mathcal{F}\{X\}$, then the quotient ring $\mathcal{F}\{X\}/\mathcal{P}$ is a differential domain, and we can consider its fraction field K. So we can associate to any prime differential field $\mathcal{P}$ a differential field extension $K/\mathcal{F}$.

It is clear from the theorem above that a system of equations $\Sigma \subset \mathcal{F}\{X\}$ admits solutions in some field extension of $\mathcal{F}$ iff $\{\Sigma\} \neq 1$. So we need an algorithm to test if a system is consistent.

2. Algorithmic Tools

2.1. **Boulier's Algorithm.** Boulier's algorithm [2] is able to solve such problems as eliminating differential variables, and testing consistency of a differential system. It provides a description of the set of solutions as a finite union of algebraic quasivarieties, i.e. Zariski open subsets of differential algebraic varieties. Each of them is described by a characteristic set A (see [12] for a precise definition of this notion), according to a compatible ranking on the set of derivatives, and an inequation $h_A \neq 0$. Let u_P denote the greatest derivative of a polynomial P. The separant of P is $S_P := \partial P/\partial u_P$. As h_A is a multiple of the products of separants of polynomials in the characteristic set, the ideal $[A] : h_A^\infty$ is radical. Unlike Ritt's algorithms, Boulier's avoids factorizations for better efficiency. This is why it cannot return prime components.

Boulier's algorithm first proceeds by constructing an autocoherent set by repeated pseudo Euclidean reductions. An autocoherent set A being found, one need to test that it is the characteristic set of a radical differential ideal. According to *Rosenfeld's Lemma*, this may be reduced to an algebraic problem. We only have to test that A is a characteristic set of the algebraic ideal $(A) : h_A^\infty$. This may be done by computing a Gröbner basis of the ideal $(A, h_A w - 1)$, using an extra variable w and Rabinovich's trick.

2.2. **Singular Solutions and Inclusion of Components.** A difficult problem of differential algebra is to test whether two irreducible components defined by their characteristic sets are included one in the other. We are only able to test equality, and have necessary conditions, sufficient conditions, but no necessary and sufficient condition in the general case.

Consider a single polynomial equation: $P(t, y, \ldots, y^{(r)})$, where P is prime. The perfect ideal $\{P\}$ is a finite intersection of prime ideals, $\mathcal{P}_i$, associated to characteristic sets reduced to a single polynomial A_i. The general component A_1 is associated to P. The other correspond to essential prime components assuming that the $\mathcal{P}_i$ are not included one in the other.

Boulier's algorithm, like Ritt's algorithm, produces the characteristic sets A_i of singular components, but also characteristic sets B_j corresponding to the singular locus of the differential algebraic variety corresponding to the general solution. (Notice that, as we avoided factorizations, the A_i need not be prime and can represent more than one prime component.) The B_j and the A_i correspond to the solutions of the perfect ideal $\{P, S_P\}$. We have $\{P\} = \{P, S_P\} \cap \{P\} : S_P$. The solutions corresponding to non essential singular components are Zariski adherent to the regular place of the general component.

We may remark, that according to [11], determining the essential singular components is equivalent to finding a finite basis of $\{P\} : S_P$, i.e. to have an *effective* version of the Ritt-Raudenbush theorem.

2.3. **Some Effective Criteria of Inclusion.** For a differential equation of order 1, the singular solutions are envelopes of regular ones. E.g., for the equation $(y')^2 - 4y$, the solutions in the general component are parabolas $y(t) = (t + c)^2$, and the essential singular solution $y = 0$ is the envelope of these parabolas.

If we have a prime decomposition, we can obtain an algorithm for finding the minimal essential components of $\{P\}$ by using the low power theorem of Ritt.

Theorem 2. *The prime differential ideal $\{y\}$ is an essential component of $\{P\}$, iff the lower degree terms of P do not contain any strict derivative of y.*

From this, we deduce that $\{y\}$ is not an essential component of $y'^2 - 4y^3$. In such a case, the regular solutions are of the form $y(t) = 1/(t + c)^2$. When t goes to infinity, then y goes to 0. So the solution $y = 0$ is adherent to the the set of regular solutions. See [12, Chap. 6] for analytical versions of this adherence property.

The necessity proof relies of Levi's lemma which characterizes the monomials belonging to the differential ideal $[y^p]$ [12, Chap. 2], or on Kolchin's domination lemma. The sufficiency proof was obtained by Ritt, using a Puiseux series expansion.

In the case where we want to test the inclusion $\{P\} : S_P \subset \{Q\} : S_Q$, where $Q \neq y$, we need to find a *preparation polynomial*, i.e. a polynomial $M(z) = \sum_{\gamma=0}^{\ell} c_\gamma m_\gamma(z)$ such that c_γ does not belong to $\{Q\} : S_Q$, $CP = M(Q)$ and C is not a zero divisor modulo $\{Q\} : S_Q$. An algorithm is given to compute a preparation polynomial.

We also have a low power theorem for regular differential polynomials (see Hubert [7]). This theorem, together with Boulier's algorithm allows to find a minimal regular decomposition for $\{P\}$ without performing factorizations.

Theorem 3. *(Sufficiency) Let P be a non zero differential polynomial of $\mathcal{F}\{Y\}$, Q a square free polynomial. Assume that the preparation polynomial of P with respect to Q is $M = cz^p + R$, where $R \in [z]^{p+1}$, $p > 0$ and c is partially reduced with respect to Q. Then, $Q/\gcd(Q, c)$ is the characteristic set of an essential singular component of P.*

(Necessity) Under the same hypotheses, if the preparation polynomial is $M = c_0 z^p + \sum_{\gamma=1}^{\ell} c_\gamma m_\gamma + R$, where $R \in [z]^{p+1}$, the c_γ are partially reduced with respect to Q, then $Q/\gcd(Q, c_0, \ldots, c_\ell)$ is a characteristic set of a redundant component.

2.4. **Implementations.** The Rosenfeld-Gröbner algorithm of Boulier, implemented in the Maple package `diffalg`, has been improved with the new version `diffalg2`. Functions for computing preparation polynomials and finding initial components were added. It is available on the Web with a clear documentation, and an impressing set of examples.

3. Applications

3.1. **Control Theory.** Elimination in differential algebra allows to go from state-space to input-output representation by eliminating the state variables. It allows to test *observability* [4] and *identifiability* [5, 10].

Consider a system of the form $x_i' = P_i(x, u), y_j' = Q_j(x)$. To test observability, one has to compute a characteristic set for an ordering eliminating the variables x. The system is observable iff for each variable x_ℓ, the characteristic set contains a polynomial whose x_ℓ is the main derivative. Such a polynomial gives an implicit expression of x_ℓ as an algebraic function of the outputs y and the inputs or commands u *and their derivatives*. This makes such an expression of little applicability, due to the noise.

3.2. **Implicit Systems.** If we consider an implicit system $P_i(x', x) = 0$ where $\det(\partial P_i/\partial x_j')$, it is not possible to compute a power series or a numerical solution in a direct way. The system is not formally integrable. In fact, solutions, if any, do not exist for all initial conditions, and one may need first to determine the variety of compatible initial conditions. For this, one will need to differentiate the equation a number of time which is known as the *index* of the system. Computing characteristic sets, using the Rosenfeld Gröbner algorithm is a way of doing it.

Bibliography

[1] Boulier (François), Lazard (Daniel), Ollivier (François), and Petitot (Michel). – Computing representations for radicals of finitely generated differential ideals. – 1997. Submitted to JSC.

[2] Boulier (Frangois), Lazard (Daniel), Ollivier (Frangois), and Petitot (Michel). – Representation for the radical of a finitely generated differential ideal. In Levelt (A. H. M.) (editor), *ISSAC'95*. pp. 158–166. – Montréal, Québec, 1995.

[3] Buium (Alexandru). – *Differential Algebra and Diophantine Geometry*. – Hermann, Paris, 1994, *Actualités mathématiques*.

[4] Fliess (Michel) and Diop (Sette). – On nonlinear observability. In *Proceedings of the First European Control Conference*. vol. 1, pp. 152–157. – Hermès, July 1991.

[5] Glad (S. T.) and Ljung (L.). – Parametrization of non-linear model structures as linear regressions. In *Proceedings of IFAC World Congress*. – August 1990.

[6] Hubert (Évelyne). – The general solution of an ordinary differential equation. In Lakshman (Y. N.) (editor), *ISSAC'96*, pp. 196–203. – Zürich, Switzerland, July 1996.

[7] Hubert (Évelyne). – Essential components of an algebraic differential equation. – 1997. Submitted.

[8] Hubert (Évelyne). – *Étude algébrique et algorithmique des singularités des équations différentielles implicites (Algebra and Algorithms for Implicit Differential Equations)*. – PhD thesis, Institut national polytechnique de Grenoble, April 1997.

[9] Kolchin (E. R.). – *Differential Algebra and Algebraic Groups*. – Academic Press, New York, 1973.

[10] Ollivier (François). – *Le problème de l'identifiabilité structurelle globale : étude théorique, méthodes effectives et bornes de complexité*. – PhD thesis, École polytechnique, Palaiseau, France, June 1990. URL: http://medicis.polytechnique.fr/gage/ollivier.html.

[11] Péladan-Germa (Ariane). – *Tests effectifs de nullité dans les extensions d'anneau différentiels*. – PhD thesis, École polytechnique, January 1997.

[12] Ritt (Joseph Fels). – *Differential Algebra*. – American Mathematical Society, New York, N. Y., 1950, *American Mathematical Society Colloquium Publications*, vol. XXXIII, viii+184p.

Solving Diophantine Equations

Guillaume Hanrot
Projet Polka, Inria Lorraine

December 1st, 1997

[summary by F. Morain]

1. Introduction

Solving Diophantine equations, that is finding integer solutions to polynomial equations, is one of the oldest mathematical problems. The very name "Diophantine" reminds us of the great Greek mathematician Diophante who solved some of the most basic equations.

At the beginning of the twentieth century, Hilbert asked about the existence of a universal algorithm that would compute all integer solutions of a polynomial equation, and it was not until 1970 that Matiyasevich [13] showed the inexistence of such an algorithm.

Even before the negative answer to this problem, many mathematicians have developed algorithms for special cases. For the univariate case, the problem is related to good rational approximations of a non rational root α of a polynomial P with integer coefficients. Let n be the degree of P and p/q a rational number. Put $\delta(\alpha) = |\alpha - p/q|$. Thue [19] showed that

$$\delta(\alpha) \geq \frac{C_1}{q^{n/2+\varepsilon}},$$

with the consequence that there are only a finite number of solutions of the equation $Q(X,Y) = 1$, where Q is an homogeneous, irreducible polynomial of degree ≥ 3. Siegel [17] improved the bound to:

$$\delta(\alpha) \geq \frac{C_2(\varepsilon)}{q^{2\sqrt{n}+1+\varepsilon}}$$

which was enough to prove the finiteness of the number of solutions of $y^p = f(x)$ for f a separable polynomial of degree ≥ 3 and $p \geq 2$ [18]. Later, in 1955, Roth proved [16]:

$$\delta(\alpha) \geq \frac{C_3(\varepsilon)}{q^{2+\varepsilon}}$$

a result that is the best possible, due to well known results in continued fraction theory, namely that if α is irrational, then there exists an infinite number of rational numbers p/q such that

$$\delta(\alpha) \leq \frac{1}{2q^2}.$$

As is often the case, the constants are ineffective and this does not help us when we want to find the solutions of a given equation. Around 1966, Baker [1] (see also [3]) found a very deep bound:

Theorem 1. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ denote algebraic numbers. Then for every n-tuple of integers $(b_1, b_2, \ldots, b_n)$, we have*

$$K = 0 \quad \text{or} \quad K \geq \exp(-C_4 \log \max_i |b_i|), \quad \text{where} \quad K = |b_1 \log \alpha_1 + b_2 \log \alpha_2 + \cdots + b_n \log \alpha_n|.$$

Unfortunately, the constant C_4, though effective, is very huge and specialists thought it was completely useless. However, Baker and Davenport [2] gave the first use of such a bound, for solving a system of simultaneous Pell equations.

2. Solving Homogeneous Equations

2.1. Statement of the Problem. Let $P(X,Y)$ be a homogeneous polynomial of degree n, monic in Y, and let α_i denote the roots of $P(1,Z)$. In this section, we want to solve the equation $P(X,Y)=1$ in integers X and Y, which we rewrite as:

$$\prod_{i=1}^{n}(Y-\alpha_i X)=1. \tag{1}$$

Suppose (X_0,Y_0) is an integer solution of this equation. In view of (1), it is obvious that at least one of the terms $Y_0-\alpha_i X_0$ is small. This implies that:

$$Y_0-\alpha_j X_0 \approx (\alpha_j-\alpha_i)X_0$$

when $j\neq i$. Using (1) again, we get that:

$$\left|\alpha_i-\frac{Y_0}{X_0}\right| \approx \frac{1}{|X_0|^n}\prod_{j\neq i}\frac{1}{|\alpha_j-\alpha_i|}$$

or in other words, Y_0/X_0 is a very good approximation of α_i.

2.2. Using the Baker Bound. In algebraic terms, equation (1) tells us that for each i, the number $Y_0-\alpha_i X_0$ is a unit in $\mathbb{Q}(\alpha_i)$.

One knows that the set of units of a number field $\mathbb{Q}(\alpha)$ is a group of finite type. There exists a set of units, the so-called *fundamental units* $\eta_1,\eta_2,\ldots,\eta_r$ such that every unit can be written as: $\zeta^{b_0}\prod_{i=1}^{r}\eta_i^{b_i}$ where ζ denotes a root of unity in $\mathbb{Q}(\alpha)$ and the b_i's are integers. Without loss of generality, it can be shown that we can restrict to the case where $\zeta=-1$.

Now suppose that α_1 is a real root of $P(1,Z)$. If $j\neq k\neq 1$, we can write:

$$\left|\frac{Y_0-\alpha_j X_0}{Y_0-\alpha_k X_0}\frac{\alpha_k-\alpha_1}{\alpha_j-\alpha_1}-1\right| \leq \frac{C_5(P)}{|X_0|^n}.$$

From this, we deduce that:

$$\left|\log\frac{Y_0-\alpha_j X_0}{Y_0-\alpha_k X_0}\frac{\alpha_k-\alpha_1}{\alpha_j-\alpha_1}\right| \leq \frac{C_6(P)}{|X_0|^n}.$$

Write $Y_0-\alpha_k X_0=\eta_{k,1}^{b_1}\cdots\eta_{k,r}^{b_r}$. We can rewrite the last inequality as:

$$\left|-\log\frac{\alpha_k-\alpha_1}{\alpha_j-\alpha_1}+\sum_{\ell=1}^{r}b_\ell\log\frac{\eta_{k,\ell}}{\eta_{j,\ell}}+2ik\pi\right| \leq \frac{C_7}{|X_0|^n}. \tag{2}$$

It is not hard to see that $\log|X_0|\approx B=\max_\ell|b_\ell|$, so that the right-hand side of the inequality is bounded by

$$C_7\exp(-nC_8B).$$

For the left hand side, we use the Baker bound to finally obtain the lower bound

$$\exp(-C_9\log B)\leq C_7\exp(-nC_8B).$$

This clearly gives a bound $\mathcal{B}$ on B.

Unfortunately, this bound is much too large to be useful. For instance, in the case of the equations

$$X^{19} + 2Y^{19} = \pm 1, \text{ or } \pm 2, \tag{3}$$

one finds $\mathcal{B} = 2.32 \times 10^{92}$.

2.3. **Refining the Bound.** Once we know that the b_i's are bounded, we would like to find a better bound. The idea is the following. Suppose the b_i's are integers subject to $|b_i| \leq \mathcal{B}$. We would like to prove some result on the minimum of the quantity $|\sum_{\ell=1}^{r} b_\ell \lambda_\ell|$ where the λ_ℓ's are real numbers. Using the Lenstra-Lenstra-Lovász theory [12] as in [8], it is possible to show that this minimum is bounded from below by $C_{10}/\mathcal{B}^{r-1}$. Since we also have the Baker bound:

$$\exp(-C_{11}\mathcal{B}) \geq \left|\sum_{\ell=1}^{r} b_\ell \lambda_\ell\right|,$$

we get

$$\mathcal{B} \leq \log(\mathcal{B}^{r-1}/C_{10}) = (r-1)\log \mathcal{B} - \log C_{10}$$

or a bound which is logarithmically smaller.

For instance, for our example, we find that $\mathcal{B} = 29$ instead of 2.32×10^{92}.

2.4. **Finishing the Computations.** At this point, one can finish the computations by enumerating all solutions. As easy as it seems, do not forget that there could be a lot of computations still to be done. In our example, there are 9 values for the b_i's, with $|b_i| \leq 29$, which amounts to 59^9 combinations.

This is enough when n is small, but can be quite cumbersome when n increases, since the computational determination of units in a general number field is no easy task at all (see for example [7, 14, 15]).

3. A Faster Approach

The idea of Bilu and the speaker [4, 5] is the following: we can rewrite equation (2) as:

$$\mathcal{L}_{0,j} + \sum_{\ell=1}^{r} b_\ell \mathcal{L}_{\ell,j},$$

that is we have r linear forms in $r+1$ logarithms. The idea is to transform these forms so as to obtain a new form of the type $\theta = |a\alpha + b\beta + \delta|$ where the integers a and b are bounded. Minimizing such a form can be done using continued fractions, and therefore is very fast. Once this is done, and using a bound as $C/|X_0|^n$, there are two cases. Either $\theta < 1/2$ and we can easily deduce b from a, or $\theta > 1/2$ and since $C/|X_0|^n > 1/2$, $|X_0|$ is quite small and we are done. In brief, we have reduced a large enumeration problem in a large number of unknowns to one in a single unknown.

For our leading example, we get that $\mathcal{B} = 4$ and it takes 12 seconds on a workstation to find all the solutions.

4. Conclusions

We have shown how to solve some special cases of Diophantine equations by a clever use of Baker's bound combined with casual ingenuity. It is possible to use more tricks, for example using units that are not fundamental, or to work with relative norms. For instance, the speaker has the world record in the field, with the solution of the equation

$$\prod_{k=1}^{2505}(Y-\cos(2k\pi/5011)X)=\pm 1$$

using an intermediate field of degree 3. The original Baker bound, 10^{40}, was reduced to 46, yielding a total running time of 8 minutes. More examples are given in [6] and in [10, 11], refinements are given when one does not have the full unit group of the number field under consideration.

The ideas we have described above can be used *mutatis mutandis* to solve equations of the type $Y^p = f(X)$. The only difference comes from the construction of the units. We refer to the speaker's thesis for this.

As a final comment, we note that similar techniques can be used to solve equations on elliptic curves [9, 20].

Bibliography

[1] Baker (A.). – Linear forms in the logarithms of algebraic numbers I, II, III, IV. *Mathematika*, vol. 13, 14, 14, 15, 1966, 1967, 1967, 1968, pp. 204–216, 102–107, 220–228, 204–216.

[2] Baker (A.) and Davenport (H.). – The equations $3x^2-2=y^2$ and $8x^2-7=z^2$. *Quarterly Journal of Mathematics, Oxford Series*, vol. 20, 1969, pp. 129–137.

[3] Baker (A.) and Wüstholz (G.). – Logarithmic forms and group varieties. *Journal für die reine und angewandte Mathematik*, vol. 442, 1993, pp. 19–62.

[4] Bilu (Yu.) and Hanrot (G.). – Solving Thue equations of high degree. *Journal of Number Theory*, vol. 60, 1996, pp. 373–392.

[5] Bilu (Yu.) and Hanrot (G.). – Solving superelliptic diophantine equations by Baker's method. – 1998. To appear in Compositio Mathematica.

[6] Bilu (Yu.) and Hanrot (G.). – Thue equations with composite fields. – 1998. To appear in Acta Arithmetica.

[7] Cohen (Henri). – *A course in computational algebraic number theory.* – Springer-Verlag, Berlin, 1993, *Graduate Texts in Mathematics*, vol. 138, xii+534p.

[8] de Weger (B. M. M.). – Solving exponential diophantine equations using lattice basis reduction algorithms. *Journal of Number Theory*, vol. 26, 1987, pp. 325–367.

[9] Gebel (J.), Pethő (A.), and Zimmer (H.). – Computing S-integral points on elliptic curves. In Cohen (H.) (editor), *Algorithmic Number Theory.* – Springer-Verlag, 1996. Proceedings of the Second International Symposium ANTS II.

[10] Hanrot (G.). – *Résolution effective d'équations diophantiennes : algorithmes et applications.* – PhD thesis, Université de Bordeaux I, 1997.

[11] Hanrot (G.). – Solving Thue equations without the full unit group. – 1998. To appear in Mathematics of Computation.

[12] Lenstra (A. K.), Lenstra (H. W. Jr.), and Lovász (L.). – Factoring polynomials with rational coefficients. *Mathematische Annalen*, vol. 261, 1982, pp. 515–534.

[13] Matiyasevich (Yu.). – Enumerable sets are diophantine. *Soviet Mathematics. Doklady*, vol. 12, 1971, pp. 249–254.

[14] Pohst (M.). – *Computational Algebraic Number Theory.* – Birkhäuser, 1993, *DMV Seminar*, vol. 21.

[15] Pohst (M.) and Zassenhaus (H.). – *Algorithmic Algebraic Number Theory.* – Cambridge University Press, 1989.

[16] Roth (K. F.). – Rational approximations to algebraic numbers. *Mathematika*, vol. 2, 1955, pp. 1–20.

[17] Siegel (C. L.). – Approximation algebraischer Zahlen. *Mathematische Zeitschrift*, vol. 10, 1921, pp. 173–213.

[18] Siegel (C. L.). – The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$ (extract from a letter to Prof. L. J. Mordell unter dem Pseudonym X). *Journal of the London Mathematical Society*, vol. 1, 1926, pp. 66–68.

[19] Thue (A.). – Über Annäherungswerte algebraischer Zahlen. *Journal für die reine und angewandte Mathematik*, vol. 135, 1909, pp. 284–305.

[20] Tzanakis (N.). – Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. the case of quartic equations. *Acta Arithmetica*, vol. 75, 1996, pp. 165–190.

Algorithm for Approximating Complex Polynomial Zeros

Victor Pan
Lehman College, CUNY

June 8, 1998

[summary by Bruno Salvy]

Abstract

An algorithm for approximating complex polynomial zeros is presented. Its complexity is optimal up to polylogarithmic factors and holds the current record.

Finding roots of a complex polynomial numerically in a guaranteed way with a fixed prescribed accuracy is difficult when no approximation is known in advance. This task cannot be performed in a fixed precision environment and implementations in computer algebra systems (where arbitrary precision is available) are seldom able to treat polynomials of degree a few hundreds. However, polynomials of very high degree arise frequently when solving a polynomial system by elimination. The work summarized here provides an algorithm supporting the following theorem.

Theorem 1. *Let $p(x)$ be a monic polynomial of degree n and $z_1, \dots, z_n$ its zeros, with $|z_i| \leq 1$, $i = 1, \dots, n$. For a fixed positive b, approximations $z_i^\star$ satisfying*

$$|z_i - z_i^\star| < 2^{-b}, \qquad i = 1, \dots, n \tag{1}$$

can be computed at a cost bounded by $\tilde{O}(n)$ arithmetic operations and $\tilde{O}(n^2(b+n))$ boolean operations. The notation $\tilde{O}$ means that factors $\log n$, $\log b$ or smaller are neglected.

Much more precise statements, proofs and parallel complexity estimates can be found in [5] and a pedagogical introduction to this area is [6].

The statement of the theorem can be modified to accommodate polynomials which are not monic (by first scaling the coefficients) or with roots of modulus larger than 1 by computing a bound on the moduli (see below) and then scaling the polynomial.

1. Lower Bounds

It is clear that the arithmetical complexity $\tilde{O}(n)$ is optimal, since n coefficients of the input polynomial have to be treated. The boolean complexity $\tilde{O}(n^2(b+n))$ is optimal in the very frequent case $n = O(b)$.

Actually, $O(n^2 b)$ is even a lower bound for the computation of *one* root of polynomials of degree n. This bound follows from the high susceptibility of the roots of a polynomial with respect to the coefficients. For instance, the polynomial $x^n - a$ with a small $a > 0$ has for root $a^{1/n}$. If this root is of order 2^{-b}, changing a to 0 is a change of the nb-th bit of a coefficient that changes the b-th bit of the root. This reasoning extends to other coefficients: let $p = O(n)$ and consider $x^n - ax^p$. Then again a change of a bit at position $O(nb)$ modifies the b-th bit of the solution. Thus b bits of the solution depend on $O(nb)$ bits of each of $O(n)$ coefficients, whence the $O(n^2 b)$ lower bound. This example also illustrates why clusters of zeros defeat many numerical algorithms.

2. Outline of the Algorithm

The algorithm is based on a splitting technique where the polynomial p is split into factors of degree k and $n-k$ with $k=\alpha n$, for some $\alpha \in (1/2, \rho)$, ρ being fixed. Applying this process recursively, any polynomial can be completely factored in $O(\log n)$ steps.

The splitting itself is computed in 3 steps:

1. Find a "splitting" circle not "too close" to roots of p and containing αn of them;
2. Compute the polynomial vanishing at these αn roots;
3. Divide p by this polynomial to obtain the other factor.

Each of these steps has to be performed in $O(n^2 b + n^3)$ boolean operations to yield the theorem.

The factors p_k and p_{n-k} of p are computed numerically. The following two lemmas show how the precision with which they are required can be bounded by ensuring that $\epsilon^\star$ is sufficiently small in the following inequality:

$$\|p(x) - p_k(x)p_{n-k}(x)\| \leq \epsilon^\star \|p(x)\|, \tag{2}$$

where $\|q(x)\|$ denotes the sum of the moduli of the coefficients of a polynomial q.

Lemma 1. [8] *If*

$$\left\| p(x) - \prod_{i=1}^{n} (x - z_i^\star) \right\| < \epsilon \|p(x)\|,$$

with $-\log_2 \epsilon \geq bn + n + 2$, *the inequalities* (1) *are satisfied.*

Lemma 2. [8] *Let* $p(x)$, $f_1(x), \ldots, f_k(x)$ *and* $f(x), g(x)$ *be polynomials such that*

$$\|p(x) - f_1(x) \cdots f_k(x)\| \leq \epsilon \frac{k}{n} \|p(x)\| \tag{3}$$

$$\|f_1(x) - f(x)g(x)\| \leq \epsilon_k \|f_1(x)\|, \tag{4}$$

then

$$\|p(x) - f(x)g(x)f_2(x) \cdots f_k(x)\| \leq \epsilon \frac{k+1}{n} \|p(x)\|$$

holds, provided

$$\epsilon_k \leq \epsilon \frac{\|p(x)\|}{n \prod_{i=1}^{k} \|f_i(x)\|}.$$

From these lemmas follows that it is sufficient to compute the splitting with $\epsilon^\star \leq \epsilon/(n 2^n)$ in (2), where ϵ comes from Lemma 1.

The splitting circle method was introduced by Schönhage [8, 9]. We now review the algorithms used in steps 1 and 2, together with the recent progress due to Victor Pan.

3. Numerical Factorization

To simplify the notation, assume the unit circle is a splitting circle for the polynomial $p(x)$. Let $p_k(x)$ be the monic polynomial whose k roots are those roots of p lying inside the circle. The computation of $p_k(x)$ relies on the following integral representation of the power sums s_j of its zeros:

$$s_j = \frac{1}{2i\pi} \int_{|z|=1} \frac{p'(z)}{p(z)} z^j \, dz.$$

This idea originates in [2] and was refined by [8] to produce error bounds, i.e., to bound Q such that the s_j's can be computed by the discretization

$$s_j^\star = \frac{1}{Q}\sum_{q=0}^{Q-1} \omega^{(i+1)q}\frac{p'(\omega^q)}{p(\omega^q)}.$$

The value of Q depends on a lower bound for $|p(z)|$ on the unit circle, which in turns is related to a bound on the distance from this circle to the closest root of p, hence the need for a circle "not too close" to the roots in Step 1 of the algorithm.

Efficiency is attained at the price of quite technical developments [8]. If the closest root to the circle is at distance $O(1/n)$, a value of Q of order $O(n^2)$ is used[1] and the corresponding $p'(\omega^q)$ and $p(\omega^q)$ are computed by a discrete Fourier transform. From there, the sums $s_j^\star$ for $j = 0, \dots, K$ are computed by DFT, K being the smallest power of 2 larger than $k = s_0$. An approximation of the factor $p_k(x)$ can then be recovered efficiently by a variant of Newton-Hensel's lifting (see [1, p. 34]). Then the other factor is obtained by division. In order to reach the right level of complexity, it is necessary to compute only $O(n)$ bits for these steps and then refine the factorization by another Newton like algorithm as follows. Starting from the approximate factorization

$$\|p(x) - p_k^{(0)}(x)p_{n-k}^{(0)}(x)\| \le \epsilon,$$

where $p_k^{(0)}$ has degree k, the aim is to find a refinement $p_k^{(1)} = p_k^{(0)} + q_k$, $p_{n-k}^{(1)} = p_{n-k}^{(0)} + q_{n-k}$ with $\deg q_i < i$, improving the error. Since

$$p - p_k^{(1)}p_{n-k}^{(1)} = (p - p_k^{(0)}p_{n-k}^{(0)}) - p_k^{(1)}p_{n-k}^{(0)} - p_k^{(0)}p_{n-k}^{(1)} - p_k^{(1)}p_{n-k}^{(1)},$$

the Newton iteration is obtained by satisfying

$$(p - p_k^{(0)}p_{n-k}^{(0)}) = p_k^{(1)}p_{n-k}^{(0)} + p_k^{(0)}p_{n-k}^{(1)}, \tag{5}$$

which determines $p_k^{(1)}$ and $p_{n-k}^{(1)}$ uniquely. These polynomials could be found by Euclid's algorithm, but this is too expensive. Instead, one also computes an inverse $q^{(i)}$ of $p_{n-k}^{(i)}$ modulo $p_k^{(i)}$ by a second, parallel, Newton iteration and then $p_k^{(i)}$ is given by $q^{(i)}p = q^{(i)}(p - p_k^{(i)}p_{n-k}^{(i)}) \bmod p_k^{(i)}$. A similar formula gives $p_{n-k}^{(i)}$. Then the required precision is obtained after a few iteration at a cost bounded by $O(n \log \epsilon^\star)$.

4. **Finding Splitting Circles**

The basic technique to find discs containing a known number of roots of a polynomial is the iteration of Graeffe's method (see [3]). Starting from $p(x)$ of degree n, one performs the following iteration:

$$p_{i+1}(x^2) = (-1)^n p_i(x)p_i(-x),$$

which transforms the polynomial $p_i(x)$ into a polynomial $p_{i+1}(x)$ whose roots are the squares of the roots of $p_i(x)$. This process emphasizes the differences of moduli between the roots. The coefficients of these iterates are Newton sums from which precise information about the different moduli of the roots of the original polynomial can be recovered at a low cost. More precisely, one gets the following lemma.

[1] More precise values are given in [8, p. 35].

Lemma 3. *Let $z_1, \dots, z_n$ be the roots of $p(x)$, satisfying $|z_1| \leq \cdots \leq |z_n| \leq 1$. Given $c > 0$ and $d \geq 0$, it is possible to compute $\underline{r}_1, \overline{r}_1, \dots, \underline{r}_n, \overline{r}_n$ such that $\underline{r}_k \leq |z_k| \leq \overline{r}_k = (1 + c/n^d)r_k$, $k = 1, \dots, n$ with $\tilde{O}(n)$ arithmetic operations.*

This iteration is applied after having first shifted the origin to the center of gravity of the roots, which is given by the first two coefficients of the polynomial. When it follows from this computation that there is a $k = \alpha n$, α in a fixed interval $(\rho, 1-\rho)$, with some $\rho < 1$ such that $|z_{k+1}|/|z_k| \geq 1+c/n$ for some c fixed in advance, then this yields a splitting circle and the factoring algorithm of the previous section can be applied.

It is when no such circle can be found that progress has been made by Victor Pan recently. In this case, there is an annulus centered at 0 which contains most of the roots of the polynomial. Now the idea is to shift the origin to each of $r' = 2\overline{r}_{11n/12}$ and ir', and apply the same method. Then either a good splitting circle is found, or there is a small circle which is easily computed and contains the intersection of these three annuli, itself containing an important cluster of zeros (at least half of the zeros of p if $c = 1/100$). In this case, the idea is that one of the zeros of a derivative of p of high order (for instance, one can take $p^{(\lfloor n/2 \rfloor + 1)}$) is either the center of a good splitting circle or makes it possible to isolate a *massive cluster* of zeros, where more than half of the zeros of p are at distance less than the desired accuracy 2^{-b}. In both cases, the polynomial can then be factored numerically and the computation proceeds on those factors that do not correspond to a massive cluster. Many refinements are given in [5], in particular it is shown that it is not necessary to compute all the zeros of $p^{(\lfloor n/2 \rfloor + 1)}$.

Conclusion

This summary is a very rough sketch of a very detailed study given in [5]. For practical polynomial solving, other algorithms are known to perform extremely well, but their complexity analysis has yet to be done.

The talk also mentioned extensions to the multivariate case, this is described in [4].

Bibliography

[1] Bini (Dario) and Pan (Victor Y.). – *Polynomial and matrix computations. Vol. 1.* – Birkhäuser Boston Inc., Boston, MA, 1994, *Progress in Theoretical Computer Science*, xvi+415p. Fundamental algorithms.

[2] Delves (L. M.) and Lyness (J. N.). – A numerical method for locating the zeros of an analytic function. *Mathematics of Computation*, vol. 21, 1967, pp. 543–560.

[3] Henrici (Peter). – *Applied and computational complex analysis.* – Wiley-Interscience, New York, 1974, *Pure and Applied Mathematics*, vol. Volume 1: Power series, integration, conformal mapping, location of zeros, xv+682p.

[4] Mourrain (Bernard) and Pan (Victor Y.). – Asymptotic acceleration of solving multivariate polynomial systems of equations. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing.* pp. 488–496. – ACM Press, 1998.

[5] Pan (V. Y.). – Optimal and nearly optimal algorithms for approximating polynomial zeros. *Computers & Mathematics with Applications*, vol. 31, n° 12, 1996, pp. 97–138.

[6] Pan (Victor). – Solving polynomials with computers. *American Scientist*, vol. 86, 1998, pp. 62–69.

[7] Pan (Victor Y.). – Optimal (up to polylog factors) sequential and parallel algorithms for approximating complex polynomial zeros. In *SIAM Journal on Computing.* pp. 741–750. – ACM Press, 1995.

[8] Schönhage (Arnold). – *The fundamental theorem of algebra in terms of computational complexity.* – Technical report, Mathematisches Institut der Universität Tübingen, 1982. Preliminary report.

[9] Schönhage (Arnold). – Equation solving in terms of computational complexity. In *Proceedings of the International Congress of Mathematicians*, pp. 131–153. – 1987. Berkeley, California, 1986.

A Test for Absolute Irreducibility of Polynomials with Rational Coefficients

Jean-François Ragot
Université de Limoges

October 6, 1997

[summary by Bruno Salvy]

While univariate polynomials with coefficients in a field k can always be factored as products of linear polynomials over the algebraic closure $\overline{k}$ of k, in the multivariate case irreducible polynomials over $\overline{k}$ may have arbitrary degree. A multivariate polynomial with coefficients in k which is irreducible over $\overline{k}$ is called *absolutely irreducible* and the decomposition of a multivariate polynomial as a product of absolutely irreducible polynomials is called its *absolute factorization.* Geometrically, absolutely irreducible polynomials correspond to irreducible algebraic varieties. Factorization is available in all the general computer algebra systems, but absolute factorization is much harder. There are algorithms that compute the absolute factorization of polynomials over $\mathbb{Q}$ and one of them is available in Maple. There are other algorithms that only test whether polynomials over $\mathbb{Q}$ are absolutely irreducible. Both these operations are computationally expensive. In this work, J.-F. Ragot gives a probabilistic test for absolute irreducibility.

1. Algorithms

The property on which are based the algorithms dealing with absolute irreducibility is related to *simple* solutions of polynomials.

Definition 1. Let k be a field. The polynomial $f \in k[x_1, \ldots, x_r]$ is said to have a *simple solution* at a point $P \in \overline{k}^r$ when

$$f \in I(P) \setminus I(P)^2,$$

$I(P)$ being the ideal of polynomials vanishing at P:

$$I(P) := \{g \in k[x_1, \ldots, x_r], g(P) = 0\}.$$

For instance, the polynomials belonging to $I(0)^p$ are those that do not have any monomial of degree less than p.

Theorem 1. *If $f \in k[x_1, \ldots, x_r]$ is irreducible over the perfect field k and has a simple solution at a point $P \in k^r$, then f is absolutely irreducible.*

Proof. Examples of perfect fields are fields of characteristic 0 and the fields $\mathbb{Z}/p\mathbb{Z}$ (for prime p). The polynomial f being irreducible over k, its absolutely irreducible factors are conjugate over k. Thus if P cancels one of them it must cancel the other ones; simplicity then implies uniqueness. $\square$

For instance, the polynomial

$$f = x^3 + 2xy + 5x - 3xy^2 - y^3$$

can be seen to be irreducible over $\mathbb{Q}$ (e.g., by attempting to factor it). Since $(0,0)$ is obviously a simple solution, f is absolutely irreducible.

One of the algorithms for absolute factorization then proceeds by constructing extension fields where the polynomials have simple solutions. Absolute factorization is thus reduced to factorization over algebraic extensions, which is possible but expensive when the degree of the extension is large.

Theorem 1 can also be used to prove absolute irreducibility when one can find simple solutions. While this is difficult in characteristic 0, it is relatively easier in characteristic p. Then, one can use the following theorem to obtain the conclusion over $\mathbb{Q}$.

Theorem 2. [3] *Let f be a polynomial in $\mathbb{Z}[x_1, \ldots, x_r]$ and p be a prime number. If $\deg(f \bmod p) = \deg(f)$ and $f \bmod p$ is absolutely irreducible (i.e., over $\overline{\mathbb{F}_p}$) then f is absolutely irreducible (i.e, over $\overline{\mathbb{Q}}$).*

For instance, the polynomial

$$g = x^3 + y^3 + 7xy + 4y + x^2 + 5$$

is irreducible mod 5 and there (0,0) is a simple solution. Therefore, g is absolutely irreducible.

Now the good news is that by a theorem of Emmy Noether, there are only finitely many p for which an absolutely irreducible f over $\mathbb{Q}$ is not absolutely irreducible mod$p$. Moreover, there are also finitely many p for which f does not have simple solutions mod p. Combining these two results it is even possible to compute an explicit upper bound $B(f)$ for the largest "bad" prime p. This gives a deterministic algorithm. However, the bound is so large that this approach is completely impractical. Instead, J.-F. Ragot's idea is to use a few prime numbers to check whether a polynomial is absolutely irreducible. This is implemented by a very simple procedure which loops over a finite set of prime numbers p until the polynomial is found to be irreducible modulo p and to have a simple root in $\mathbb{F}_p$ (success) or the set of prime numbers is exhausted (failure).

The remaining question is to evaluate the probability of success of this technique and bound the probability that a failure corresponds to an absolutely irreducible polynomial.

2. Probability Estimates

2.1. **Irreducible Polynomials.** Let $q = p^n$ for p a prime number and n a positive integer. The number of polynomials of degree at most d over $\mathbb{F}_q[X] = \mathbb{F}_q[x_1, \ldots, x_r]$ is $q^{\omega(d,r)}$ where $\omega(d,r) = \binom{r+d}{d}$. From there and the fact that $\mathbb{F}_q[X]$ is a unique factorization domain it is possible to compute an exact formula for the number of irreducible polynomials of $\mathbb{F}_q[X]$ of degree at most d [1, 2]. Then very sharp inequalities can be obtained: for $r \geq 2$ and $d \geq 3$ the probability p that a polynomial of $F_q[X]$ of degree at most d be reducible obeys

$$\frac{q^r}{q^{\omega(d,r-1)}}\left(1 - \frac{5}{q}\right) \leq p \leq \frac{q^r}{q^{\omega(d,r-1)}}\left(1 + \frac{6}{q}\right).$$

2.2. **Polynomials having simple solutions.** For any $P \in \mathbb{F}_q^r$, the set of polynomials of degree at most d in $I(P) \setminus I(P)^2$ is a subspace of the vector space $\mathbb{F}_q[X]_d$ of polynomials of degree at most d. This makes it easier to compute the probability that a polynomial of degree d has a simple solution at a fixed point P or at a point P in a given set of points, since from the dimension D of a vector space over $\mathbb{F}_q$, its cardinality is given by q^D.

The quotients $\mathbb{F}_q[X]/I(P)^q$. We first consider the point $P=0$. There are $\omega(p-1,r)$ monomials that cannot occur in a polynomial of $I(0)^p$. In terms of dimensions, this is equivalent to

$$\dim F_q[X]/I(0)^p = \omega(p-1,r). \tag{1}$$

This enumeration applies to any point P possibly different from 0.

Chinese remainder theorem. If $P_1 \neq P_2$ are two points of $\mathbb{F}_q^r$, it follows for instance from Bézout's theorem that $\mathbb{F}_q[X] = I(P_1)^p + I(P_2)^q$ for any p, q. One can therefore apply the Chinese remainder theorem which states the ring isomorphism

$$\mathbb{F}_q[X]/\bigcap_{i=1}^n I(P_i)^{p_i} = \prod_{i=1}^n \mathbb{F}_q[X]/I(P_i)^{p_i},$$

when the points P_i, $i=1,\ldots,n$ are distinct. This translates into a result on the dimensions of the corresponding vector spaces:

$$\dim\left(\mathbb{F}_q[X]/\bigcap_{i=1}^n I(P_i)^{p_i}\right) = \sum_{i=1}^n \dim \mathbb{F}_q[X]/I(P_i)^{p_i}.$$

It follows from (1) that the quantity D in the left-hand side is finite, and for any degree $d \geq D$,

$$\dim\left(\mathbb{F}_q[X]_d \cap \bigcap_{i=1}^n I(P_i)^{p_i}\right) = \omega(d,r) - D. \tag{2}$$

Inclusion-Exclusion. Let again $P_1 \neq P_2$ be two points of $\mathbb{F}_q^r$. Then the number of polynomials having a simple solution at either P_1 or P_2, or both, is the cardinality of

$$\begin{aligned}\big(I(P_1)\setminus I(P_1)^2\big) &\cup \big(I(P_2)\setminus I(P_2)^2\big)\\ &= I(P_1)\cup I(P_2)\setminus I(P_1)^2\setminus I(P_2)^2\setminus (I(P_1)\cap I(P_2))\\ &\qquad \cup \big(I(P_1)^2\cap I(P_2)\big)\cup\big(I(P_1)\cap I(P_2)^2\big)\setminus\big(I(P_1)^2\cap I(P_2)^2\big).\end{aligned}$$

The cardinalities are evaluated from the right-hand side by (1) and (2), which gives for $d \geq \omega(1,r) = 2r+2$

$$\begin{aligned}2q^{\omega(d,r)-\omega(0,r)} - 2q^{\omega(d,r)-\omega(1,r)} - q^{\omega(d,r)-2\omega(0,r)} + 2q^{\omega(d,r)-\omega(0,r)-\omega(1,r)} - q^{\omega(d,r)-2\omega(1,r)}\\ = q^{\omega(d,r)}\left(1-\left(1-q^{\omega(0,r)}+q^{\omega(1,r)}\right)^2\right).\end{aligned}$$

This extends to the case of n distinct points $P_1,\ldots,P_n$ to give that for $d > (r+1)n$, the proportion of polynomials in $\mathbb{F}_q[X]_d$ having at least one simple solution at one of the P_i's is

$$1-\left(1-\frac{1}{q}+\frac{1}{q^{r+1}}\right)^n. \tag{3}$$

Now it is sufficient to take $n=q^r$ the cardinality of $\mathbb{F}_q^r$ in the previous expression to obtain the probability that a random polynomial of degree $d \geq n$ has a simple solution at a point of $\mathbb{F}_q^r$.

Refining the Bound. The bound $d \geq q^r$ that we have just derived can be made much more precise by having a better look at the quotient on the left-hand side of (2) in the case $n = q^r$. The system of polynomials

$$\{(x_1^q - x_1)^2, \ldots, (x_r^q - x_r)^2\}$$

generates the ideal of polynomials having multiplicity at least 2 at every point of $\mathbb{F}_q^r$. This ideal is responsible for the largest value of D in (2), whence the bound q^r. It is easy to see that the system above is a *Gröbner basis* of this ideal for the lexicographic order. This means that one can take a basis of the quotient (as a vector space) where the polynomials of largest degree have degree $2q-1$. This way, one gets the following.

Proposition 1. [3] *For $d \geq r(2q-1)$, the proportion of polynomials of $\mathbb{F}_q[X]_d$ having a simple solution in $\mathbb{F}_q^r$ is*

$$1 - \left(1 - \frac{1}{q} + \frac{1}{q^{r+1}}\right)^{q^r}.$$

2.3. **Conclusion.** We are interested in polynomials that are irreducible *and* have a simple solution. Using both previous results yields a bound on the complementary event: the probability that a polynomial of degree $d > r(2p-1)$ is reducible or does not have a simple solution is upper bounded by

$$\frac{p^r}{p^{\omega(d,r-1)}}\left(1 + \frac{6}{p}\right) + \left(1 - \frac{1}{p} + \frac{1}{p^{r+1}}\right)^{p^r},$$

where the first term is neglectible compared to the second one, the sum being of order

$$\exp(1/p)\exp(-p^{r-1}).$$

By taking several prime numbers p, we get a product of similar quantities which can be made as small as desired. Polynomials whose degree decreases when reduced mod p have to be taken into account, but their quantity does not change the final result much. Thus we get a bound on the probability that an absolutely irreducible polynomial hold the probabilistic algorithm in check.

Bibliography

[1] Carlitz (L.). – The distribution of irreducible polynomials in several indeterminates. *Illinois Journal of Mathematics*, vol. 7, 1963, pp. 371–375.

[2] Carlitz (L.). – The distribution of irreducible polynomials in several indeterminates. II. *Canadian Journal of Mathematics*, vol. 17, 1965, pp. 261–266.

[3] Ragot (Jean-François). – *Sur la factorisation absolue des polynômes.* – PhD Thesis, Université de Limoges, 1997.

The Lazy Hermite Reduction

Manuel Bronstein
INRIA, Sophia Antipolis

May 4, 1998

[summary by Grégoire Lecerf]

Abstract

The Hermite reduction is a symbolic integration technique that reduces algebraic functions to integrands having only simple affine poles [1, 2, 7]. While it is very effective in the case of simple radical extensions, its use in more general algebraic extensions requires the precomputation of an integral basis, which makes the reduction impractical for either multiple algebraic extensions or complicated ground fields. In this work, Manuel Bronstein shows that the Hermite reduction can be performed without a priori computation of either a primitive element or integral basis, computing the smallest order necessary for a particular integrand along the way.

1. Preliminaries

We recall in this section some terminology and results from [2, 4, 6] that will be needed in the main algorithm. Let R be an integral domain, K its quotient field and E a finitely generated algebraic extension of K. An element $\alpha \in E$ is called *integral over* R if there is a *monic* polynomial $p \in R[X]$ such that $p(\alpha) = 0$. The set

$$\mathcal{O}_R = \{\alpha \in E \text{ such that } \alpha \text{ is integral over } R\}$$

is called the *integral closure of* R *in* E. It is a ring and a finitely generated R-module. A basis of E over K that generates $\mathcal{O}_R$ over R is called an *integral basis*. Any submodule of $\mathcal{O}_R$ is finitely generated over R.

Let now k be a differential field of characteristic 0 with derivation '. An element t in a differential extension of k is called a *monomial over* k if t is transcendental over k and $t' \in k[t]$, which implies that both $k[t]$ and $k(t)$ are closed under differentiation. We say that $p \in k[t]$ is *normal (with respect to ')* if $\gcd(p, p')$=1, and *special (with respect to ')* if $\gcd(p, p')$=p. Factors and products of specials are special, and factors and least common multiples of normals are normal. Note that normal polynomials are squarefree. Conversely, for $p \in k[t]$ squarefree, let $p_s = \gcd(p, p')$ and $p_n = p/p_s$. Then, p_s is special and p_n is normal.

2. Extending a Module

Let R be a Euclidean domain, K its quotient field, V a finite-dimensional vector space over K with basis $(w_1, \ldots, w_n)$ and $M_w = Rw_1 + \cdots + Rw_n$ the module generated by $(w_1, \ldots, w_n)$. Let $w \in V$ and $M = Rw + M_w$ be the module generated by $(w, w_1, \ldots, w_n)$. We describe in this section an algorithm for computing a generating set $(m_1, \ldots, m_n)$ of M over R.

Since $(w_1, \ldots, w_n)$ generates V over K, we can write

$$w = \frac{1}{d}(a_1 w_1 + \cdots + a_n w_n)$$

where $d, a1, \ldots, a_n \in R$ and $d \neq 0$. This implies that M is the submodule of $R(1/d)w_1 + \cdots + R(1/d)w_n$ generated by $w_1, \ldots, w_n, w$, *i.e.*, by the rows of

$$\mathcal{M} = \begin{pmatrix} d & & & \\ & d & & \\ & & \ddots & \\ & & & d \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

Using Hermitian row reduction, we can zero out the last row of $\mathcal{M}$, obtaining a matrix of the form

$$\mathcal{N} = \begin{pmatrix} b_{1,1} & b_{1,2} & \ldots & b_{1,n} \\ b_{2,1} & b_{2,2} & \ldots & b_{2,n} \\ \vdots & \vdots & & \vdots \\ b_{n,1} & b_{n,2} & \ddots & b_{n,n} \\ 0 & 0 & \ldots & 0 \end{pmatrix}$$

with $b_{i,j} \in R$. A generating set for M over R is then given by

$$m_i = \frac{1}{d}\sum_{j=1}^{n} b_{i,j} w_j \quad \text{for} \quad 1 \leq i \leq n.$$

The cost of this computation is $O(n^3)$ operations in $k[t]$.

3. I-Bases

Let k be a differential field of characteristic 0 with derivation $'$, t a monomial over k, $R = k[t]$, $K = k(t)$, E a finitely generated algebraic extension of K and $\mathcal{O}$ the integral closure of R in E. Given any vector-space basis $(w_1, \ldots, w_n)$ of E over K, let $f_{i,j} \in K$ be such that

$$w_i' = \sum_{j=1}^{n} f_{i,j} w_j \quad \text{for} \quad 1 \leq i \leq n \tag{1}$$

and $F_w \in R$ be the least common multiple of the denominators of all the $f_{i,j}$'s.

Definition 1. With the above notations, we say that $(w_1, \ldots, w_n)$ is an *I-basis* if F_w is normal and $w_i \in \mathcal{O}$ for each i.

For any vector-space basis of E over K we have an algorithm for transforming it into an I-basis within $O(n^3)$ operations in $k(t)$.

4. The Lazy Reduction

With the notations as in the previous section, let $(w_1, \ldots, w_n)$ be an I-basis for E over K, the $f_{i,j}$'s be given by (1), F_w be the least common multiple of the denominators of all the $f_{i,j}$'s, and $\mathcal{M}_w$ be the n by n matrix with entry $F_w f_{i,j}$ at row i and column j. Let $f \in E$ and write

$$f = \frac{A_1 w_1 + \cdots + A_n w_n}{D}$$

where $D, A_1, \dots, A_n \in k[t]$ and $\gcd(A_1, \dots, A_n, D) = 1$. Let $D = d_1 d_2^2 \cdots d_{m+1}^{m+1}$ be a squarefree factorization of D, $d_{i,s} = \gcd(d_i, d_i')$ and $U_i = d_i / d_{i,s}$ for each i, $S = d_{1,s} d_{2,s}^2 \cdots d_{m+1,s}^{m+1}$, $U = U_1 U_2^2 \cdots U_m^m$ and $V = U_{m+1}$. Then,

$$D = SUV^{m+1}$$

where S is special, V and all the squarefree factors of U are normal, and $\gcd(U, V) = 1$. Let $G_w = F_w / \gcd(F_w, UV)$. Note that $G_w \mid F_w \mid G_w UV$. In addition, $\gcd(G_w, V) = 1$ by construction, and since the basis is an I-basis, F_w, and therefore G_w, are normal.

Consider the following linear system in $k[t]/(V)$:

$$\left(\frac{G_w UV}{F_w}\mathcal{M}_w^t - mG_w UV' I_n\right)\begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix} = G_w S^{-1}\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{pmatrix} \tag{2}$$

where $\mathcal{M}_w^t$ is the transpose of $\mathcal{M}_w$, I_n is the n by n identity matrix, and S^{-1} is the inverse of S modulo V. The classical Hermite reduction (where the w_i's form an integral basis) proceeds by computing a solution of (2) in $k[t]/(V)$ and using it to reduce the poles of the integrand. Even with an I-basis, any solution in $k[t]/(V)$ does reduce the poles of the integrand.

Theorem 1. *For any solution $(B_1, \dots, B_n)$ of (2) in $k[t]/(V)$,*

$$f = \left(\frac{\sum_{i=1}^n B_i w_i}{V^m}\right)' + \frac{\sum_{i=1}^n C_i w_i}{SG_w UV^m} \tag{3}$$

where

$$C_i = \frac{G_w A_i}{V} - SG_w UB_i' + m\frac{SG_w UV' B_i}{V} - \sum_{j=1}^m SG_w U f_{j,i} B_j \quad \in k[t]. \tag{4}$$

It remains to study under which circumstances the system (2) has a solution in $k[t]/(V)$: we show that, whenever the system has no solution, we can extend the module $k[t]w_1 + \cdots + k[t]w_n$. Let

$$S_i = SUV^{m+1}\left(\frac{w_i}{V^m}\right)', \quad \text{for} \quad 1 \le i \le n. \tag{5}$$

Theorem 2. *Suppose that $m > 0$ and that $\{S_1, \dots, S_n\}$ as given by (5) are linearly independent over $k(t)$, and let $T_1, \dots, T_n \in k[T]$ be not all zero and such that $\sum_{i=1}^n T_i S_i = 0$. Then,*

$$w = \frac{SU}{V}\sum_{i=1}^n T_i w_i \in \mathcal{O}.$$

Furthermore, if $\gcd(T_1, \dots, T_n) = 1$, *then $w \notin \mathcal{O}_w = k[t]w_1 + \cdots k[t]w_n$.*

Theorem 3. *Suppose that $m > 0$ and that $\{S_1, \dots, S_n\}$ as given by (5) are linearly independent over $k(t)$, and let $Q, T_1, \dots, T_n \in k[t]$ be such that*

$$\sum_{i=1}^n A_i w_i = \frac{1}{Q}\sum_{i=1}^n T_i S_i.$$

Then,

$$w = \frac{SU(V/\gcd(V, Q))}{\gcd(V, Q)}\sum_{i=1}^n T_i w_i \in \mathcal{O}.$$

Furthermore, if $\gcd(Q, T_1, \ldots, T_n) = 1$ *and (2) has no solution in* $k[t]/(V)$*, then* $w \notin \mathcal{O}_w = k[t]w_1 + \cdots + k[t]w_n$.

The lazy reduction algorithm follows from Theorems 1, 2, and 3: if $m = 0$, then $D = SU_1$, where S is special and U_i is normal. Otherwise, we solve the system

$$\sum_{i=1}^{n} A_i w_i = \sum_{i=1}^{n} h_i S_i$$

for $h_1, \ldots, h_n \in k(t)$. Any solution in $k(t)$ whose denominators are coprime with V is a solution of (2) in $k[t]/(V)$. In that case, (3) reduces integrating f to a new integrand whose denominator divides SG_wUV^m. If the above equation has no solution in $k(t)$ whose denominators are coprime with V, then either the S_i's are linearly dependent over $k(t)$ or there is a solution whose denominator has nontrivial common factor with V, so either Theorem 2 or 3 produces $w \in \mathcal{O}$ such that $w \notin \mathcal{O}_w$, and the algorithm of Section 2 produces a new basis $b_1, \ldots, b_n$ for the submodule $k[t]w + \mathcal{O}_w$ of $\mathcal{O}$. We transform that basis into an I-basis, express f in the new basis and continue the reduction process. In both of the above cases, the integrand after the reduction step has an expression whose denominator has strictly less zeroes of multiplicity $m+1$ than before (it has none when the system has a solution), so after finitely many reduction steps, we have produced a new basis made of integral elements, and a new integrand, whose denominator with respect to that basis is the product of a special and a normal polynomial. This is the same result as obtained by the Hermite reduction (with an integral basis) as presented in [1, 2, 7].

Conclusion

We have presented a lazy Hermite reduction for which each reduction step uses only rational operations and performs Gaussian or Hermitian elimination on matrices of size n by n or $n+1$ by n, while computing an integral basis requires Hermitian elimination on matrices of sizes n^2 by n, so the lazy reduction is expected to cost $O(n^3)$ operations in $k(t)$ as compared to $O(n^4)$ for computing rationally an integral basis. In the case of pure algebraic functions, this yields a complete algorithm for determining whether the integral of an algebraic function is itself an algebraic function. The natural direction in which to extend this work is to ask whether the complete algebraic integration algorithm can be performed rationally without computing an integral basis. Another interesting direction would be to generalize the Hermite reduction (and its lazy variant) to solve equations of the form $y' + fy = g$ in a finitely generated algebraic extension of $k(t)$, as was done for the transcendental case in [5]. This could yield a better algorithm than the reduction to a linear differential system in $k(t)$ [3].

Bibliography

[1] Bertrand (Laurent). – *Calcul Symbolique des Intégrales Hyperelliptiques.* – PhD thesis, Université de Limoges, Mathématiques, 1995.

[2] Bronstein (Manuel). – On the integration of elementary functions. *Journal of Symbolic Computation*, vol. 2, n° 9, February 1990, pp. 117–173.

[3] Bronstein (Manuel). – The Risch differential equation on an algebraic curve. In Watt (Stephen) (editor), *Symbolic and algebraic computation.* pp. 241–246. – New York, 1991. Proceedings of ISSAC'91, Bonn, Germany.

[4] Bronstein (Manuel). – *Symbolic Integration I - Transcendental Functions.* – Springer, Heidelberg, 1997.

[5] Davenport (James Harold). – The Risch differential equation problem. *SIAM Journal on Computing*, vol. 15, 1986, pp. 903–918.

[6] Lang (Serge). – *Algebra.* – Addison Wesley, Reading, Massachussets, 1970.

[7] Trager (Barry). – *On the integration of algebraic functions.* – PhD thesis, MIT, Computer Science, 1984.

ECPP Comes Back

François Morain
LIX, École Polytechnique

April 20, 1997

[summary by Guillaume Hanrot]

1. Introduction

Prime numbers have always attracted attention from both mathematicians and computer scientists. One of the reasons is perhaps the fact that the definition of a prime is very simple, most of the famous conjectures concerning primes can be stated in elementary terms, yet these problems are extremely high and the techniques involved are most often very sophisticated.

We outline a few more concrete motivations to study prime numbers and to try to discover huge prime numbers (that is, apart from trying to understand the asymptotic properties of primes via experimentation):

- prime numbers are the elementary particles of the arithmetician; we just do as physicists do!
- primality testing/proving can be used as a benchmark for complexity studies (does there exist any polynomial-time algorithm for factoring?), devising and programming efficient algorithms;
- prime numbers are heavily used in modern, number-theory based cryptography (RSA, discrete logarithms, etc.). Thus it is an important matter to be able to produce large primes at will, and to be able to *prove* them prime.

The main trends in the computational study of primality are the following:

- Let N be a large integer. Can one tell if N is prime?
- Find large Mersenne numbers, i.e., primes of the form $2^p - 1$;
- construct large "general" primes.

In this talk we will describe the solutions to the first problem, the so-called "primality testing" problem, but we shall call it *"primality proving"*, to emphasize the fact that we shall describe an algorithm with produces an easy-to-check proof together with its yes/no answer.

We shall first make a quick overview of existing primality tests; we will then concentrate on the ECPP test, describing its principles, its main features and recent progresses in theory and implementation. We shall end by a list of current records and perspectives.

2. Primality Tests: an Overview

A general reference for all the tests mentioned in this section is [9].

2.1. Compositeness Tests. This section covers the so-called "compositeness tests". Given a number N, these tests check whether N verifies a certain criterion, which is known to be the case if N is prime. If it is not so, the number is known to be composite, whence the name of this group of tests. However, if the test is passed, one can by no means be sure that N is prime.

In a nutshell, they are fast ($O((\log N)^3)$), but can only provide one with negative answers to the question "is N prime". Examples of such tests include:

- Fermat tests and extensions, where the criterion is $2^{N-1} \equiv 1 \bmod N$;
- Field extensions tests: cyclotomic fields (Lucas), general fields (Arno [3], Gurak [13]);
- Elliptic curves tests (Bosma [6], Gordon [11]);
- Polynomial tests (Grantham [12]);
- Combination of several of those last tests (PRIKIN).

Due to their efficiency, and their relative accuracy concerning "small" numbers N when suitably combined, those tests are usually implemented under the name `isprime` in various computer algebra packages (Maple, Pari, ...).

2.2. **Primality Proving.** A real primality proof is somewhat different from the tests described in the last section. It should be able to give an answer, either yes or no, *together with a proof*, for any given number N. Of course, it should at the same time be as fast as possible.

Examples of such tests include:

- cyclotomy tests: $O((\log N)^{c \log\log\log N})$
  * Gauss sums test: Adleman, Pomerance, Rumely (1979) [2, 15].
  * Jacobi sums test: Cohen, Lenstra, Lenstra (1980) [8].
  * cyclotomy tests: Bosma & van der Hulst (1990), Mihăilescu (1997) [17].
- elliptic curves tests: $O((\log N)^c)$: Bosma, Chudnovsy & Chudnovsky (1985) [7]; Goldwasser & Kilian [10], Atkin & Morain (1986) [5, 4].
- genus 2 curves: $O((\log N)^?)$, Adleman & Huang (1986) [1], the interest of which is mostly theoretical (can be proved to be polynomial probabilistic).

3. The Principles of ECPP

In this section, we shall describe the principles on which rests ECPP (which, by the way, stands for Elliptic Curves Primality Proving). This test is an analog of the $N-1$ test which has been known for long, and is very efficient when the number $N-1$ is *smooth*, i.e., has only small prime factors.

3.1. **The $N-1$ Test.** Assume that N is neither even nor a prime power (these two possibilities can be easily avoided). Then we have the following

Theorem 1. *N is prime iff $(\mathbb{Z}/N\mathbb{Z})^*$ is a cyclic group. In other words, there exists $a \in \mathbb{Z}$ such that $a^{N-1} \equiv 1 \bmod N$, and for all prime p dividing $N-1$, $a^{(N-1)/p} \not\equiv 1 \bmod N$.*

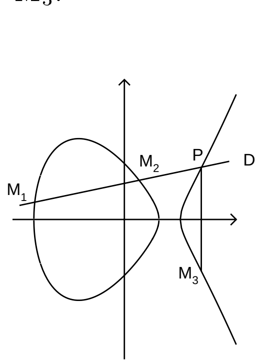
The triple $(N, \{p|(N-1)\}, a)$ is a certificate of primality for N. It is very easy to check from these data that N is indeed prime.

A more practical version of this theorem (due to Pocklington, 1914) allows one to restrict to a set of prime factors of $(N-1)$ whose product is larger that $\sqrt{N}$. This however does not address the main problem of the method, which is the need to factor $N-1$, at least to some extent. Compared to this, finding a is a merely trivial matter: if the generalized Riemann hypothesis is true, there exists one such a smaller than $2(\log N)^2$.

3.2. **Elliptic Curves.** The main idea in the $N-1$ test is that if a certain group is cyclic, then N is prime. Thus we just need to find a generator. Proving that a given number is a generator amounts mostly, from a computational point of view, to factor to some extent the order of the group.

The idea of Goldwasser and Kilian was to construct a vast number of groups of different orders with the same property that the $N-1$ test, so that one can hope to find at least one such group with a smooth order.

Let us introduce quickly elliptic curves. Let $\mathbb{K}$ be a field of characteristic $\neq 2, 3$. An elliptic curve defined over $\mathbb{K}$ is a projective nonsingular curve defined by an equation $Y^2Z = X^3 + aXZ^2 + bZ^3$, where $(a, b) \in \mathbb{K} \times \mathbb{K}$. More concretely, $E(\mathbb{K}) = \{(X, Y, 1), Y^2 = X^3 + aX + b\} \cup \{(0, 1, 0)\}$, this last point being "at infinity". The non-singularity can be expressed by the condition $\Delta := 4a^3 + 27b^2 \neq 0$. To an elliptic curve, we can attach an invariant defined by $j(E) = 1728(4a^3/\Delta)$. Conversely, given $j_0 \in \mathbb{K}$, the family of elliptic curves $Y^2 = X^3 + 3j_0/(1728-j_0)c^2X + 2j_0/(1728-j_0)c^3$ has j-invariant j_0 (except when $j_0 = 0$ or 1728; for $j_0 = 1728$, take $Y^2 = X^3 + aX$, for $j_0 = 0$, take $Y^2 = X^3 + b$). The set of points of an elliptic curve over a certain field can be given a group structure by using the following rules: the neutral element 0_E is the point at infinity; if A, B, C lie on the same line, then $A + B + C = 0_E$. (Note that if a line has at least two points of intersection with a cubic (counting multiplicities) over a given field, then it has three, so that the addition is well-defined over the ground field.) This rule is illustrated on the following picture: $M_1 + M_2 + P = 0_E$ and $0_E + P + M_3 = 0_E$, so that $M_1 + M_2 = M_3$.



If $\mathbb{K} = \mathbb{F}_p$ is a prime finite field, the group $E(\mathbb{K})$ is finite. We can however be much more precise:

Theorem 2 (Hasse, 1933; Deuring, Waterhouse). 1. *One has* $|\#(E(\mathbb{F}_p)) - (p+1)| \leq 2\sqrt{p}$,

2. *for all t integer in* $]-2\sqrt{p}, 2\sqrt{p}[$, *there is a curve E defined over $\mathbb{F}_p$ with exactly $p + 1 - t$ points over $\mathbb{F}_p$.*

We now have to (a) find a primality criterion linked with these groups (b) make the second part of this theorem effective. The main feature of ECPP is the use of complex multiplication to solve problem (b).

3.3. **A Primality Criterion.** Both Goldwasser and Kilian's method and the ECPP test are based on the following

Theorem 3. *Let B be an integer, m and s two integers such that $s|m$, E an elliptic curve defined over $\mathbb{Z}/N\mathbb{Z}$ and P a point on E. Then $mP = O_E$ and*

$$\forall q \text{ prime}|s, [m/q]P = (X : Y : Z), \gcd(Z, N) = 1 \Rightarrow \forall p|N, \#E(\mathbb{Z}/p\mathbb{Z}) \equiv 0 \bmod s.$$

If we can find a point P satisfying the conditions of left part of this implication with $s > (\sqrt[4]{N} + 1)^2$, then using Hasse's theorem we see that any prime p dividing N is larger than $\sqrt{N}$, which means that N is prime. The primality can be easily checked given $(E, m, s, \{q|s\}, P)$ (the certificate).

This theorem, together with Schoof's algorithm which enables one to compute the number of points of an elliptic curve on a finite field in time $O((\log N)^8)$, leads to the following algorithm (Goldwasser and Kilian, [10]):

Repeat Choose a random elliptic curve E modulo N, compute $\#E(\mathbb{Z}/N\mathbb{Z})$.
until the primality criterion can be applied [i.e., $\#E(\mathbb{Z}/N\mathbb{Z})$ is smooth]

Note that the application of the criterion is most often recursive: one factors $\#E(\mathbb{Z}/N\mathbb{Z})$, and gets one large factor presumably prime. ECPP is then recursively used to actually prove the primality of this large factor. Since this factor is at worst $N/2 + o(N)$, the recursion depth is $O(\log(N))$. The complexity is thus $O((\log N)(\log N)^8)$, under the heuristic assumption (verified in practice) that there are many good curves (giving smooth $\#E(\mathbb{Z}/N\mathbb{Z})$).

This algorithm has been generalized to the case of curves of genus 2 (i.e., curves $Y^2 = f(X)$, where $\deg(f)$=5 or 6) by Adleman and Huang. In that context, the algorithm can be proved to be polynomial probabilistic.

However, both of these algorithms are definitely unpractical. First, Schoof algorithm has never been very efficient, and even with the more recent improvements which reduce the complexity to $O((\log N)^6)$, 4000 hours are needed to compute the cardinality of a single curve linked with the primality of a 500-digits number.

3.4. **Complex Multiplication, or Finding Curves with a Smooth Number of Points.** A partial answer to the question (b) raised above is given by the theory of complex multiplication.

Let p be a prime number such that $4p$ is of the form U^2+DV^2, where (U,V,D) are integers, with $D>0$. Class field theory of imaginary quadratic fields tells us that given D, one can construct a polynomial $H_D(X)$, of degree $h(-D)$ (the class number of $\mathbb{Q}(\sqrt{-D})$), the roots of which generate the maximal abelian unramified extension (class field) of $\mathbb{Q}(\sqrt{-D})$. Moreover, this polynomial splits on $\mathbb{F}_p$ as a product of linear factors, and its roots are the j-invariants of elliptic curves E with $\#E(\mathbb{F}_p) = p+1-U$.

For instance, for $D = 4$, $H_D(X) = X - 1728$ and one can take for E the curve of equation $Y^2 = X^3 + aX$. If $p \equiv 1 \bmod 4$ or $p = 2$, $4p = U^2 + V^2$ and $\#E = p+1-U$. Note that U is only defined up to sign, and according to the choice of a (square or non-square mod p), both possibilities can occur.

The previous algorithm becomes:

repeat
    repeat
        Find D such that $4N = U^2+DV^2$, and compute (U,V) using Cornacchia's algorithm.
    until $N+1-U$ is smooth;
    find a root of $H_D(X)$ mod N (use Berlekamp's algorithm); construct E so that $j(E) = j_0$,
    and choose among the family constructed an E such that $\#E = N+1-U$,
until one of the primality theorems can be applied.

4. Recent History

4.1. **Recent Improvements.** In this section we describe shortly the recent improvements included in the last version of the ECPP software.

First of all, the problem of whether the number of points on the CM-curve is $N+1-U$ or $N+1+U$ is now almost completely solved. For $D = 3, 4$, this follows from a theorem by Katre. For $h = 1$, see [14]. For $D = 20$, see [16]. A recent paper by Stark [19] settles the case $(D,6) = 1$. We have recently solved, using new invariants, the case $D \equiv 0 \bmod 3$, and partially solved the cases

$D \equiv \pm 1 \bmod 3$ [18]. As a consequence, one no more needs to compute $[p+1\pm t]P$ to find the exact cardinality of the curve.

Several implementation tricks have also be added: trial divisions steps have been improved, and I/O have been drastically reduced. The use of Montgomery's arithmetic has allowed a speedup by a factor of 2. Berlekamp's algorithm (which is used to factor the polynomial H_D over the field $\mathbb{F}_p$) has been adapted according to an idea of Atkin: Classically, one splits the polynomial P over $\mathbb{F}_p$ by computing $\gcd(P(X), X^{(p-1)/2} \pm 1)$. If small factors of $p-1$ are known, we can take a d-th root of unity ζ_d, and compute $\gcd(P(X), X^{(p-1)/d} - \zeta_d^i)$ for all $0 \leq i < d$. Instead of splitting the polynomial into two parts of degree roughly half of the initial polynomial, this should split it into several parts of smaller degree. Since our goal is just to find one linear factor, this should be much better, and indeed it is. This variant of Berlekamp's algorithm proved to be extremely efficient. Finally, backtrack was implemented at the request of E. Mayer, to allow one to restart interrupted computations. The current publicly available version of ECPP[1] is v.5.6.1 which, though newer than the one in MAGMA, for instance, does not include any of the improvements or the tricks described above. The up-to-date version is version 6.4.5, currently unstable.

4.2. **Records.** Large primes proved to be prime by using ECPP software include the following "world records":

- Cofactor of $2^{2^{11}}+1$ (564 digits, 458 hours on a Sun 3/60) (1988);
- Titanic $(2^{3539}+1)/3$ (1065 digits, 328 days on a Sun 3/60) (1988);
- $p(1840926)$ (1505 digits, 4 years of Sun 3/60) (1992);
- $(2^{7331}-1)/458072843161$ (2196 digits, 1 month on an Alpha 400 MHz, 6 hours to check the certificate) (1998, joint work with E. Mayer).

However, the record is now the property of P. Mihăilescu, using cyclotomy-based tests.

5. Conclusion

ECPP now seems to have reached a "stable" stage, where most of the theoretical problems with a real algorithmic pertinence have been solved, and the code has been cleaned and speeded up.

Perspectives include exploration of higher genus (à la Adleman-Huang). The main trouble is that the theory of complex multiplication is much more complicated in higher genus, and lots of practical problems arise when studying curves of genus ≥ 2.

Another direction of exploration which needs further development is to try to make the best two primality tests (ECPP and cyclotomy) interact with each other, for instance through the concept of "dual pairs", i.e., couple of integers (p,q) together with an elliptic curve E defined over $\mathbb{Z}$ such that $\#E(F_p) = q$ and $\#E(F_q) = p$.

Bibliography

[1] Adleman (L. M.) and Huang (M.-D. A.). – *Primality testing and Abelian varieties over finite fields.* – Springer-Verlag, 1992, *Lecture Notes in Mathematics*, vol. 1512.

[2] Adleman (L. M.), Pomerance (C.), and Rumely (R.). – On distinguishing prime numbers from composite numbers. *Annals of Mathematics*, vol. 117, n° 1, 1983, pp. 173–206.

[3] Arno (Steven). – A note on Perrin pseudoprimes. *Mathematics of Computation*, vol. 56, n° 193, January 1991, pp. 371–376.

[4] Atkin (A. O. L.) and Morain (F.). – Elliptic curves and primality proving. *Mathematics of Computation*, vol. 61, n° 203, July 1993, pp. 29–68.

[5] Atkin (A. O. L.) and Morain (F.). – Finding suitable curves for the elliptic curve method of factorization. *Mathematics of Computation*, vol. 60, n° 201, January 1993, pp. 399–405.

[1] Available from `http://www.lix.polytechnique.fr/Labo/Francois.Morain`

[6] Bosma (W.). – *Primality testing using elliptic curves.* – Technical Report n° 85-12, Math. Institut, Universiteit van Amsterdam, 1985.

[7] Chudnovsky (D. V.) and Chudnovsky (G. V.). – Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, vol. 7, 1986, pp. 385–434.

[8] Cohen (H.) and Lenstra, Jr. (H. W.). – Primality testing and Jacobi sums. *Mathematics of Computation*, vol. 42, n° 165, 1984, pp. 297–330.

[9] Cohen (Henri). – *A course in computational algebraic number theory.* – Springer-Verlag, Berlin, 1993, *Graduate Texts in Mathematics*, vol. 138, xii+534p.

[10] Goldwasser (S.) and Kilian (J.). – Almost all primes can be quickly certified. In *Proc. 18th STOC*. pp. 316–329. – ACM, 1986. May 28–30, Berkeley.

[11] Gordon (D. M.). – Pseudoprimes on elliptic curves. In Koninck (J.-M. De) and Levesque (Claude) (editors), *Théorie des nombres*. pp. 290–305. – Walter de Gruyter, 1989. Proceedings of the International Number Theory Conference held at Université de Laval, July 5–18, 1987.

[12] Grantham (J.). – Frobenius pseudoprimes. – May 1996. Preprint.

[13] Gurak (S.). – Pseudoprimes for higher-order linear recurrence sequences. *Mathematics of Computation*, vol. 55, n° 192, October 1990, pp. 783–813.

[14] Joux (A.) and Morain (F.). – Sur les sommes de caractères liées aux courbes elliptiques à multiplication complexe. *Journal of Number Theory*, vol. 55, n° 1, November 1995, pp. 108–128.

[15] Lenstra (H. W.). – Primality testing algorithms (after Adleman, Rumely and Williams). In *Bourbaki Seminar, Vol. 1980/81. Lecture Notes in Mathematics*, pp. 243–257. – Springer-Verlag, 1981.

[16] Leprévost (F.) and Morain (F.). – Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. *Journal of Number Theory*, vol. 64, 1997, pp. 165–182.

[17] Mihăilescu (P.). – Cyclotomy primality proving – recent developments. – March 1998. To appear in the Proceedings of ANTS-III.

[18] Morain (F.). – Primality proving using elliptic curves: an update. – January 1998. To appear in the Proceedings of ANTS-III.

[19] Stark (H. M.). – Counting points on *cm* elliptic curves. *Rocky Mountain Journal of Mathematics*, vol. 26, n° 3, 1996, pp. 1115–1138.

Cyclotomic Primality

Preda Mihailescu
ETH, Zürich

April 20, 1998

Abstract

The cyclotomic test was invented by Lenstra to combine the Jacobi sum test with Lucas-Lehmer tests. Although it has an odd asymptotic behaviour—$O(\log n \log\log\log n)$—and an "almost" deterministic approach, which makes certificates impossible, the cyclotomic test is robust and much faster than ECPP for numbers that can be proved with current computers. Also, in its central step, it is better understood, which does not leave much room for improvement.

This talk describes the general theory of cyclotomy of rings, the test and interesting relations with older tests of the Lucas-Lehmer type. In a second part, open problems related to primality tests are discussed. Although new records continually increase the size of numbers that can be proved prime, a general lack of knowledge will be uncovered.

Part 3

Analysis of Algorithms and Data Structures

On the Analysis of Linear Probing Hashing

Philippe Flajolet
INRIA, France

January 15, 1998

[summary by Hosam M. Mahmoud]

For uniform data, hashing is known to provide fast access schemes [12]. The idea in hashing is to maintain a table, of size m say, and map n keys to the locations of the table. In the absence of complications, later on we can retrieve the key by looking up its hash position in the table. A key x is associated with a hash address $h(x) \in \{1, \ldots, m\}$. In practice, data may collide: the chosen hash function may map two keys to the same location in the table. In this case we must resolve collisions. Standard mechanisms for collision resolution are chaining and linear probing, among other. For hashing a set of n keys to be successful, m must be at least as large as n. The ratio $\alpha = n/m \leq 1$ is called the load factor and plays an important role in the analysis. The special case $\alpha = 1$ corresponds to eventually filling the table at the end of hashing the entire data set; this case will be dubbed the title *full table*. A sparse table (small α) may be viewed as a collection of smaller full tables separated by empty locations. These smaller full tables are also figuratively called islands.

The situation is paralleled to balls-in-urns arguments. In this analogy, the n keys are emulated by n balls, and the m hash locations are emulated by m urns. The random allocation of balls unto urns is the parallel of a uniform hash function. Several results are mentioned to indicate some facts about random allocation of balls in urns and are related to classical theory:

- Collisions occur early (the Birthday Paradox);
- The probability of no collision in a full table is rather small (exponentially so);
- Empty cells disappear late (Coupon Collector's Problem);
- In a sparse table, the maximal share of a bucket is moderately high. For instance if the average share of an urn is $\alpha = n/m = 1/2$, still one of the shares grows on average as fast as $\log n / \log \log n$.

A proof is sketched to argue that when both $m, n \to \infty$, in such a way that $n/m \to \alpha$, the number of urns that receive exactly k (fixed) balls follows a Poisson law with parameter α:

$$P\{\text{an urn receives } k \text{ balls}\} = \frac{\alpha^k}{k!} e^{-\alpha}.$$

Noticeably, even when the number of balls and urns are the same ($\alpha = 1$) the proportion of empty urns ($k = 0$) approaches $e^{-\alpha} \approx 36\%$.

In passing, the analysis of Separate Chaining (when all keys hashed to the same location are linked in a linear chain) is mentioned. The main thrust of the talk, however, focused on Linear Probing Hashing. In this latter collision resolution method, when a key is hashed to an already occupied location, the resolution algorithm looks for the nearest unoccupied position above the hash position (wrapping around to the beginning of the table, if necessary). The distance a key travels till collision is resolved, the *displacement*, is a measure of efficiency for data insertion and retrieval.

Stochastically, the displacement increases as more keys are placed in the table. For example, stochastically the last key has the highest displacement. This last displacement is intuitively small for small α. If α is close to 1, "clotting" occurs and the average displacement is asymptotic to $m/2$.

The problem was first proposed by Knuth in 1962. Over the course of time connections to Abel identities and Ramanujan's function were discovered. "Generating functionology" is a key element in the analysis. A broad array of analytic constructions (a dictionary of formal operators so to speak) together with singularity analysis play a central rôle in the analysis. A starting point is the decomposition of an almost full table ($n = m - 1$) into two full tables:

$$\langle \text{full} \rangle \equiv \langle \text{full} \rangle \star \langle \text{full} \rangle,$$

with the $\star$ indicating an empty slot at any position. In the language of the enumeration generating function $F(z)$, this decomposition corresponds to an integral operator in the dictionary, giving

$$F = \int (zF)' F.$$

The substitution $T = zF$ gives an ordinary differential equation from which it is then demonstrated that $T(z)$ is the *tree function* that solves the equation

$$T = ze^T.$$

By Lagrange's inversion and methods of Eisenstein and Cayley, an explicit formal series is obtained:

$$T(z) = \sum_{n=0}^{\infty} n^{n-1} \frac{z^n}{n!}.$$

Trees also have a decomposition, discussed by Knuth as early as 1963. The number of almost-full tables for n keys is

$$F_n = (n+1)^{n-1}.$$

The talk then shifts focus from counting (the totality of the sample space) to distributional analysis of almost full tables. Conditioned on where the empty slot falls in an almost-full table, one obtains a convolution formula for the probability generating function of full tables:

$$F_n(q) = \sum_{k=0}^{n-1} \binom{n-1}{k} (1 + q + \cdots + q^k) F_k(q) F_{n-1-k}(q).$$

Let $F(z, q)$ be the bivariate generating function of the sequence $F_n(q)$. Via a number of differential operators on $F(z, q)$, moment generating functions are expressed by differential equations involving rational polynomials of the tree function. Let $d_{n,m}$ be the total displacement to place n uniform keys into a hash table of size m. Extraction of coefficients then yields the following result [7, 2].

Theorem 1.

$$E[d_{n,n}] = \frac{n}{2}\big(Q(n) - 1\big), \qquad E[d_{n,n}^2] = \frac{n}{12}\big(5n^2 + 4n - 1 - 8Q(n)\big),$$

where $Q(n)$ is a Ramanujan function.

Asymptotic analysis of the mean and variance gives a series expansion.

Theorem 2.

$$E[d_{n,n}] = \frac{\sqrt{2\pi}}{4} n^{3/2} - \frac{2}{3} n + \frac{\sqrt{2\pi}}{48} n^{1/2} - \frac{2}{135} + O\big(n^{-1}\big),$$
$$\operatorname{Var}[d_{n,n}] = \frac{10 - 3\pi}{24} n^3 + \frac{16 - 3\pi}{144} n^2 + \frac{\sqrt{2\pi}}{135} n^{3/2} - \cdots .$$

Higher moments are "pumped" from the functional equation on $F(z,q)$. Through the rth derivative, one gets a functional equation for the rth moment. The latter functional is solved either exactly or asymptotically. The method has been used before in various combinatorial analyses, such as Quicksort [4], path length in trees [17], Brownian excursions [11], in-situ permutations [9, 6].

The Airy distribution is introduced next. Its distribution function solves the differential equation

$$Y'' - zY = 0,$$

and is known to have the integral representation

$$Ai(z) = \frac{1}{\pi}\int_0^\infty \cos\Big(\frac{1}{3}t^3 + zt\Big)\,dt.$$

The Airy distribution is uniquely characterized by its moments, as its exponential moment generating function converges in a neighborhood of 0. By showing that all moments of the random total displacement converge to the moments of the Airy distribution, one main result of the investigation is obtained.

Theorem 3. *In an almost full table the random total displacement $d_{n,n-1}$ converges in distribution to A, a random variable having the Airy distribution, in the usual sense of convergence of distribution functions: for every real x,*

$$P\Big\{\frac{d_{n,n-1}}{(n/2)^{3/2}} \le x\Big\} \to P\{A \le x\}, \qquad \textit{as} \quad n \to \infty.$$

Full tables are building blocks of general hash tables. Generally, a table can be decomposed as

$$\langle\text{full}\rangle \equiv \langle\text{full}\rangle \star \cdots \star \langle\text{full}\rangle.$$

Given that there are k islands, the bivariate generating function becomes the convolution $F^k(z,q)$.

The whole analysis package outlined above can then be "recycled" to derive the result for a general load factor, as in [2, 8].

Theorem 4.

$$\begin{aligned} E[d_{m,n}] &= \frac{n}{2}\big(Q_0(m,n-1) - 1\big),\\ E[d_{m,n}^2] &= \frac{n}{12}\big[(m-n)^3 + (n+3)(m-n)^2 + (8n+1)(m-n) + 5n^2 + 4n - 1\\ &\qquad - \big((m-n)^3 + 4(m-n)^2 + (6n+3)(m-n) + 8n\big)Q_0(m,n-1)\big]. \end{aligned}$$

where $Q_0(m,n)$ is a Ramanujan function. Asymptotically, these expressions simplify to

$$\begin{aligned} E[d_{m,n}] &= \frac{\alpha}{2(1-\alpha)}n - \frac{\alpha}{(1-\alpha)^3} + O\big(n^{-1}\big),\\ \mathrm{Var}[d_{m,n}] &= \frac{6\alpha - 6\alpha^2 + 4\alpha^3 - \alpha^4}{12(1-\alpha)^4}n - \cdots . \end{aligned}$$

The convolution form of the generating function admits a Gaussian law.

Theorem 5. *The random total displacement is asymptotically normally distributed.*

This result is obtained by a delicate saddle point analysis on the integral

$$\frac{1}{2\pi i}\oint \frac{F^{m-n}(z,q)}{z^{n+1}}\,dz,$$

an expression for the coefficient (a probability generating function) of z^n in $F^{m-n}(z,q)$, the bivariate function for a table of m locations receiving n keys.

This general law for coefficients of functions that are large powers of generating functions has wide applicability and appears later in other contexts, like for example the analysis of Distributive Sort (a flavor of Bucket Sort) with a large number of buckets [13].

By no means the Airy distribution appears in hash tables as an isolated phenomenon. It seems to be a ubiquitous law in combinatorial analysis. We now know that it appears in full hash tables for Linear Probing with Hashing; inversions in trees; random walks; path length and Dyck or Catalan walks in random trees. These connections to the Airy distribution may be found in [10, 3, 8, 5, 16, 11, 17, 18, 14, 1, 15]. These works connect various areas of combinatorial analysis to each other and eventually to the Airy distribution. Although closed forms for bivariate functions for random variables with the Airy distribution are known, their moments are still hard to find.

Bibliography

[1] Flajolet (Philippe) and Noy (Marc). – *Analytic Combinatorics of Non-crossing Configurations.* – Research Report n° 3196, Institut National de Recherche en Informatique et en Automatique, June 1997.

[2] Flajolet (Philippe), Poblete (Patricio), and Viola (Alfredo). – *On the Analysis of Linear Probing Hashing.* – Research Report n° 3265, Institut National de Recherche en Informatique et en Automatique, September 1997. 22 pages. To appear in *Algorithmica*.

[3] Gessel (Ira) and Wang (Da Lun). – Depth-first search as a combinatorial correspondence. *Journal of Combinatorial Theory. Series A*, vol. 26, n° 3, 1979, pp. 308–313.

[4] Hennequin (Pascal). – Combinatorial analysis of quicksort algorithm. *RAIRO Theoretical Informatics and Applications*, vol. 23, n° 3, 1989, pp. 317–333.

[5] Janson (Svante), Knuth (Donald E.), Łuczak (Tomasz), and Pittel (Boris). – The birth of the giant component. *Random Structures & Algorithms*, vol. 4, n° 3, 1993, pp. 231–358.

[6] Kirschenhofer (P.), Prodinger (H.), and Tichy (R. F.). – A contribution to the analysis of in situ permutation. *Društvo Matematičara i Fizičara S. R. Hrvatske. Glasnik Matematički. Serija III*, vol. 22 (42), n° 2, 1987, pp. 269–278.

[7] Knuth (D. E.). – Notes on "open" addressing. – Unpublished memorandum, 1963. Memo dated July 22, 1963. With annotation *"My first analysis of an algorithm, originally done during Summer 1962 in Madison"*.

[8] Knuth (D. E.). – Linear probing and graphs. – Preprint, 1997.

[9] Knuth (Donald E.). – Mathematical analysis of algorithms. In *Information processing 71*. pp. 19–27. – Amsterdam, 1972. Proceedings IFIP, Ljubljana, 1971, Vol. 1: Foundations and systems.

[10] Kreweras (G.). – Une famille de polynômes ayant plusieurs propriétés énumeratives. *Periodica Mathematica Hungarica. Journal of the János Bolyai Mathematical Society*, vol. 11, n° 4, 1980, pp. 309–320.

[11] Louchard (G.). – The Brownian excursion area: a numerical analysis. *Computers & Mathematics with Applications*, vol. 10, n° 6, 1984, pp. 413–417.

[12] Lum (V. Y.), Yuen (P. S. T.), and Dodd (M.). – Key-to-address transform techniques: A fundamental performance study on large existing formatted files. *Communications of the ACM*, vol. 14, n° 4, April 1971, pp. 228–239.

[13] Mahmoud (Hosam), Flajolet (Philippe), Jacquet (Philippe), and Régnier (Mireille). – *Analytic Variations on Bucket Selection and Sorting.* – Research Report n° 3399, Institut National de Recherche en Informatique et en Automatique, 1998. 22 pages, submitted to *Acta Informatica*.

[14] Mallows (C. L.) and Riordan (John). – The inversion enumerator for labeled trees. *Bulletin of the American Mathematical Society*, vol. 74, 1968, pp. 92–94.

[15] Prellberg (T.). – Uniform q-series asymptotics for staircase polygons. *Journal of Physics. A. Mathematical and General*, vol. 28, n° 5, 1995, pp. 1289–1304.

[16] Spencer (Joel). – Enumerating graphs and Brownian motion. *Communications on Pure and Applied Mathematics*, vol. 50, n° 3, 1997, pp. 291–294.

[17] Takács (Lajos). – On the distribution of the number of vertices in layers of random trees. *Journal of Applied Mathematics and Stochastic Analysis*, vol. 4, n° 3, 1991, pp. 175–186.

[18] Wright (E. M.). – The number of connected sparsely edged graphs. *Journal of Graph Theory*, vol. 1, n° 4, 1977, pp. 317–330.

Smallest Components in Combinatorial Structures

Daniel Panario
University of Toronto

February 16, 1998

[summary by Philippe Flajolet]

Abstract

The smallest size of components in random decomposable combinatorial structures is studied in a general framework. The results apply to several combinatorial structures in both the labelled and the unlabelled case. Typical examples are the cycle decomposition of permutations and the factorization of polynomials over finite fields into irreducible factors.

1. Introduction

Many types of combinatorial objects decompose as *sets* of simpler basic objects diversely known as "prime", "irreducible", or "connected" components. For instance, a permutation decomposes as a set of cyclic permutations, a polynomial as a (multi)set of irreducible factors, and a graph as a set of connected components. Such situations are combinatorial analogues of the fact that natural numbers uniquely decompose as products of primes.

Let $\mathcal{I}$ be a class of basic objects, $\mathcal{F}$ the class of all sets of objects from $\mathcal{I}$, that is

$$\mathcal{F} = \texttt{Set}\,(\mathcal{I}).$$

As usual, this schema covers both the labelled case (L) where sets are built upon labelled products, and the unlabelled case (U) where multisets are intended. Enumeration is treated by generating functions [5]. The generating functions (gf's) $F(z), I(z)$ corresponding to $\mathcal{F}, \mathcal{I}$, are taken to be either the exponential generating function (egf) in the labelled case or the ordinary generating function in the unlabelled case,

$$(L): \qquad F(z) = \sum_n F_n \frac{z^n}{n!} \qquad I(z) = \sum_n I_n \frac{z^n}{n!}$$

$$(U): \qquad F(z) = \sum_n F_n z^n \qquad I(z) = \sum_n I_n z^n,$$

with F_n, I_n the number of objects of size n in $\mathcal{F}, \mathcal{I}$. Then, the fundamental relations between generating functions are given by the exponential formulæ:

$$(1) \qquad \begin{aligned} (L): &\quad F(z) = e^{I(z)} \\ (U): &\quad F(z) = \prod_{k=1}^{\infty} (1 - z^k)^{-I_k} = \exp\left(I(z) + \frac{1}{2} I(z^2) + \frac{1}{3} I(z^3) + \cdots \right). \end{aligned}$$

The construction covers a number of classical combinatorial structures like permutations (cyclic, general), monic polynomials over a finite field of cardinality q (irreducible, general), functional graphs (connected, general) in either the labelled or the unlabelled case. In fact, the examples just cited all belong to an interesting class called the "exp-log" class that was introduced in [4].

Definition 1. A pair $(\mathcal{I}, \mathcal{F})$ is said to have the exp-log property if $I(z)$ has a unique dominant singularity ρ of the logarithmic type,

$$I(z) \underset{z \to \rho}{\sim} a \log \frac{1}{1 - z/\rho} + c_0 + O((1 - z/\rho)^{\epsilon}), \tag{2}$$

for some $\epsilon > 0$, where a is called the multiplier. Accordingly, one has

$$F(z) \sim e^{I(z)} \sim c_1 (1 - z)^{-a}, \qquad c_1 = e^{c_0}. \tag{3}$$

It is understood that these expansions should hold in an indented disk of the type required by singularity analysis.

Based on the known facts for integers [12] and on specific combinatorial examples, the following properties are expected to hold true:

1. **Prime Number Theorem:** The *asymptotic density of irreducible objects* satisfies
$$\frac{I_n}{F_n} \sim (a e^{-c_0} \Gamma(a)) \frac{1}{n^a}.$$
2. **Gaussian law:** The *number of irreducible components* in a random $\mathcal{F}$-object of size n is asymptotically Gaussian with mean and variance each asymptotic to $a \log n$.
3. **Dickman's law:** The density of $\mathcal{F}$-object of size n whose *largest* $\mathcal{I}$-component is of size $m = n/u$ involves a function of which a prototype is the Dickman function $\rho(u)$ classically defined by the difference-differential equation
$$\rho(u) = 1 \ (0 \le u \le 1), \qquad u\rho'(u) + \rho(u-1) = 0 \ (u > 1).$$
4. **Buchstab's law:** The density of $\mathcal{F}$-object of size n whose *smallest* $\mathcal{I}$-component is of size $m = n/u$ involves a function of which a prototype is the Buchstab function $\omega(u)$ classically defined by the difference-differential equation
$$u\omega(u) = 1 \ (1 \le u \le 2), \qquad (u\omega(u))' = \omega(u-1) \ (u > 2).$$

The Prime Number Theorem for exp-log classes derives immediately from basic singularity analysis theorems. The Gaussian law was established in [4] by means of characteristic functions, thanks to the uniformity afforded by singularity analysis; it is an analogue of the classical Erdős-Kac theorem for the number of prime divisors of integers. The Dickman law is known originally from number theory [12] and it holds as well for the cycle decomposition of permutations [10], its extension to the general framework of exp-log classes being due to Gourdon [7]. The purpose of the talk is precisely to establish for exp-log structures the Buchstab law of smallest components by building upon Gourdon's analysis of largest components.

2. Cycles in Permutations

In its simplest terms the problems are well exemplified by the analysis of smallest and largest cycles in permutations. In an important paper, Shepp and Lloyd [10] established the Dickman law and the Buchstab law for permutations. Their approach is however based on an asymptotic-probabilistic model of permutations as sums of Poisson random variables of rates $1, \frac{1}{2}, \frac{1}{3}, \ldots$ relayed by nonconstructive Tauberian arguments. Gourdon [7] was instead able to push the analytic approach to its ultimate limits, thereby solving the long-standing Golomb-Knuth conjecture; see [6].

From standard methods of enumerative combinatorics the egf's of permutations with all their cycles of size at most m ($P^{[\le m]}(z)$) or at least $m+1$ ($P^{[>m]}(z)$) are given by

$$
\begin{aligned}
P^{[\le m]}(z) &= \exp\left(\frac{z}{1} + \frac{z^2}{2} + \cdots + \frac{z^m}{m}\right) \\
&= \frac{1}{1-z}\exp\left(-\frac{z^{m+1}}{m+1} - \frac{z^{m+2}}{m+2} - \cdots\right)
\end{aligned} \tag{4}
$$

$$
\begin{aligned}
P^{[>m]}(z) &= \exp\left(\frac{z^{m+1}}{m+1} + \frac{z^{m+2}}{m+2} + \cdots\right) \\
&= \frac{1}{1-z}\exp\left(-\frac{z}{1} - \frac{z^2}{2} - \cdots - \frac{z^m}{m}\right).
\end{aligned} \tag{5}
$$

Let L_n and S_n be the random variables that represent the largest cycle and the smallest cycle in a random permutation of size n. Equations (4) and (5) give access to probabilities, as

$$\Pr\{L_n \le m\} = [z^n]P^{[\le m]}(z), \qquad \Pr\{S_n > m\} = [z^n]P^{[>m]}(z).$$

In the analytic perspective, an important rôle is thus played by the decomposition of the logarithm into its partial sum and remainder,

$$\log\frac{1}{1-z} = s_m(z) + r_m(z), \qquad s_m(z) := \sum_{k=1}^{m}\frac{z^k}{k}, \qquad r_m(z) := \sum_{k>m}\frac{z^k}{k}.$$

Consider now smallest cycles. For any *fixed* m, singularity analysis at $z = 1$ immediately implies a formula for generalized derangements,

$$P_n^{[>m]} \equiv [z^n]P^{[>m]}(z) = e^{-H_m} + o(1), \tag{6}$$

where $H_m = 1 + \frac{1}{2} + \cdots + \frac{1}{m}$ is the harmonic number and the error term is exponentially small. There is no claim to uniformity, but this argument suggests for m tending to ∞ (at least sufficiently slowly) the approximate formula

$$P_n^{[>m]} \approx \frac{e^{-\gamma}}{m}. \tag{7}$$

Let S_n be length of the smallest cycle in a random permutation of size n. The estimate above suggests that the expectation of S_n satisfies

$$E[S_n] \equiv \sum_{m\ge 1} P_n^{[>m]} = e^{-\gamma}\log n(1 + o(1)),$$

where the asymptotic estimate matches what is otherwise known about the distribution of S_n. However, an approximation of the form (7) cannot hold all the way up to $m = n-1$ since

$$P_n^{[>(n-1)]} = \frac{1}{n}, \tag{8}$$

corresponding to cyclic permutations. A natural way to reconcile (7) and (8) is to look for a version that is of the form

$$P_n^{[>m]} \approx \frac{\omega(n/m)}{m}, \tag{9}$$

where one should have $\omega(1) = 1$ and $\omega(+\infty) = e^{-\gamma}$. It turns out that an amended form of (9) does hold true with $\omega(u)$ in (9) being precisely the Buchstab function.

3. The exp-log Class

The main theorem of the talk deals with the general exp-log case. We state it here in the case of a multiplier $a = 1$ where the standard Buchstab function appears. Also, we develop the main ideas in the representative case of the cycle structure of permutations.

Theorem 1. *For a random element of size n in an exp-log class $\mathcal{F}$ of multiplier $a = 1$, the probability that the smallest component S_n is of size greater than m satisfies*

$$\Pr\{S_n > m\} = \frac{1}{m}\omega\left(\frac{n}{m}\right) + O\left(\frac{1}{m^2} + \frac{\log n}{nm}\right),$$

uniformly over the range $\{0, \ldots, , n-1\}$.

The proof starts from Cauchy's coefficient formula

$$P_n^{[>m]} = \frac{1}{2i\pi}\int_C P^{[>m]}(z)\frac{dz}{z^{n+1}}. \tag{10}$$

With the purpose of "capturing the singularity", the integration contour is taken to be a circle of radius close to 1, namely $e^{-1/n}$. Set

$$z = e^{-t/n},$$

where t ranges from $1 - ni\pi$ to $1 + ni\pi$. Then z^{-n} normalizes to an exponential e^t. The form (5) of the gf $P^{[>m]}(z)$ involves $r_m(z)$ that is none other than a Riemann sum relative to the exponential integral,

$$E(v) := \int_v^{+\infty} e^{-w}\frac{dw}{w}.$$

Thus, everything rests on a uniform approximation of the Riemann sum $r_m(z)$ by the exponential integral. This is provided by the following key lemma of [6].

Lemma 1 (Gourdon). *One has uniformly for $\Re(h) > 0$ and $|\Im(h)| \le \pi$,*

$$r_m(e^{-h}) = E(mh) + O\left(\frac{e^{-mh}}{m}\right).$$

(The proof of the lemma is based on the integral formula

$$r_m(e^{-h}) = \frac{1}{m}\int_{mh}^{+\infty} e^{-s}\frac{1}{1 - e^{-s/m}}\,ds,$$

and the decomposition

$$\frac{1}{1-e^{-z}} = \left(\frac{1}{1-e^{-z}} - \frac{1}{z}\right) + \frac{1}{z},$$

where the first term is analytic near $z = 0$.)

Using Lemma 1, one can justify replacing the remainder logarithm in the expression of

$$[z^n](P^{[>m]}(z) - 1)$$

by an exponential integral. In this way, one establishes rigourously the chain of approximations

$$
\begin{aligned}
P_n^{[>m]} &= \frac{1}{2i\pi n}\int_{1-in\pi}^{1+in\pi}(e^{r_m(e^{-t/n})}-1)e^t\,dt \\
&\sim \frac{1}{2i\pi n}\int_{1-i\infty}^{1+i\infty}(e^{E(\mu t))}-1)e^t\,dt \\
&\sim \frac{1}{2i\pi m}\int_{1-i\infty}^{1+i\infty}(e^{E(t)}-1)e^{t/\mu}\,dt,
\end{aligned}
\tag{11}
$$

where $\mu = m/n$. (This is easier said than done!)

Now, the form (11) is an inverse Laplace integral evaluated at $1/\mu$. It can be matched against the Laplace transform of $\omega(u)$, itself directly derived from the defining difference-differential equation. Thus eventually, *the Buchstab law arises from Cauchy's coefficient integral upon using a contour close to the singularity $z = 1$ with a "renormalization" that leads to the appearance of a Laplace transform—the transform of Buchstab's function.*

The technique adapts gracefully to all exp-log structures with multiplier $a = 1$ since these behave analytically very nearly like permutations. For other multipliers $a \neq 1$, a function $\omega_a(u)$ closely related to the Buchstab function must be introduced (work in progress). Finally, like in Gourdon's treatment of largest components, other problems can be dealt with including: (i) local and central limit laws; (ii) distribution estimates for the rth largest component for small fixed r.

4. Applications

The analysis sketched here follows closely a preprint by Panario and Richmond [9] and the related works on largest components [6, 7]. It applies to all exp-log classes. In particular, it specializes to polynomials over finite fields and hence has consequences on the analysis of corresponding algorithms. We may cite here:

1. The comparative analysis of several halting rules for the Distinct Degree Factorization phase of univariate polynomial factorization in [3], which requires knowledge of the degrees of the two largest irreducible factors.
2. The analysis of the trial-and-error construction of irreducible polynomials by Ben-Or's algorithms [9], where only partial factorisations are attempted and a candidate polynomial is discarded as soon as its factor of smallest degree has been found.

More generally, the analogy between the prime decomposition of integers and exp-log structures is a striking fact that constitutes a valuable addition to the abstract theory of combinatorial schemas initiated by Soria [11]. (Other general approaches have been recently developed by a variety of authors in a stochastic perspective; see [1, 2, 8].)

Bibliography

[1] Arratia (Richard), Barbour (A. D.), and Tavaré (Simon). – Random combinatorial structures and prime factorizations. *Notices of the American Mathematical Society*, vol. 44, n° 8, 1997, pp. 903–910.

[2] Cameron (Peter J.). – On the probability of connectedness. *Discrete Mathematics*, vol. 167/168, 1997, pp. 175–187.

[3] Flajolet (Philippe), Gourdon (Xavier), and Panario (Daniel). – Random polynomials and polynomial factorization. In Meyer auf der Heide (F.) and Monien (B.) (editors), *Automata, Languages, and Programming*, *Lecture Notes in Computer Science*, pp. 232–243. – 1996. Proceedings of the 23rd ICALP Conference, Paderborn, July 1996. Journal version submitted to*SIAM J. Computing* and available as INRIA Res. Rep. 3370, 1998, 28 pages.

[4] Flajolet (Philippe) and Soria (Michèle). – Gaussian limiting distributions for the number of components in combinatorial structures. *Journal of Combinatorial Theory,* Series A, vol. 53, 1990, pp. 165–182.

[5] Goulden (Ian P.) and Jackson (David M.). – *Combinatorial Enumeration.* – John Wiley, New York, 1983.

[6] Gourdon (Xavier). – *Combinatoire, Algorithmique et Géométrie des Polynômes.* – PhD thesis, École polytechnique, June 1996.

[7] Gourdon (Xavier). – Largest component in random combinatorial structures. *Discrete Mathematics*, vol. 180, n° 1-3, 1998, pp. 185–209.

[8] Hansen (Jennie C.). – A functional central limit theorem for random mappings. *Annals of Probability*, vol. 17, n° 1, 1989.

[9] Panario (Daniel) and Richmond (Bruce). – Analysis of Ben-Or's polynomial irreducibility test. – Preprint, 1997. 16 pages. Submitted to *Random Structures and Algorithms.*

[10] Shepp (L. A.) and Lloyd (S. P.). – Ordered cycle lengths in a random permutation. *Transactions of the American Mathematical Society*, vol. 121, 1966, pp. 340–357.

[11] Soria-Cousineau (Michèle). – *Méthodes d'analyse pour les constructions combinatoires et les algorithmes.* – Doctorat ès Sciences, Université de Paris-Sud, Orsay, July 1990.

[12] Tenenbaum (Gérald). – *Introduction à la théorie analytique des nombres.* – Institut Élie Cartan, Nancy, France, 1990, vol. 13.

The Analysis of Hybrid Trie Structures

Julien Clément
Algorithms project, INRIA Rocquencourt

October 20, 1997

[summary by Frédéric Cazals]

1. Introduction

Tries are a general-purpose data structure of the dictionary type, that is supporting the three main operations Insert, Delete and Query. To see how they are defined, let $\mathcal{A} = \{a_j\}_{j=1}^r$ be an alphabet and S be a set of strings defined over $\mathcal{A}$. The trie associated to S is recursively defined by the rule

$$\operatorname{trie}(S) = \langle \operatorname{trie}(S\backslash a_1), \operatorname{trie}(S\backslash a_2), \ldots, \operatorname{trie}(S\backslash a_r)\rangle$$

where $S\backslash\alpha$ refers to the contents of S consisting of strings that start with α and stripped of their initial letter, and the recursion stops as soon as S contains one element.

Searching a trie T for a key w just requires tracing a path down the trie as follows: at depth i, the ith digit of w is used to orientate the branching. (Insertions and deletions are handled in the same way.) To complete the description, we need to specify which search structure is used to choose the correct sub-trie within a node. The main possibilities are:

1. the "array-trie" which uses an array of pointers to sub-tries. This solution is relevant for small alphabets only, otherwise too many empty pointers are created;
2. the "list-trie" that remedies the high-storage requirement of the "array-trie" by using a linked list of sub-tries instead. The drawback is a higher cost for the traversal;
3. the "bst-trie" which uses binary-search trees (bst) as a trade-off between the time efficiency of arrays and the space efficiency of lists.

In particular, the bst-trie can be represented as a ternary tree where the search on letters is conducted like in a standard binary search tree, while the tree descent is performed by following an escape pointer upon equality of letters. We shall refer to this data structure as a ternary search trie or tst. An example trie with its basic representation and the equivalent ternary search trie over the alphabet $\mathcal{A} = \{a, b, c\}$ is represented on fig. 1 and 2. As is well known, the performances

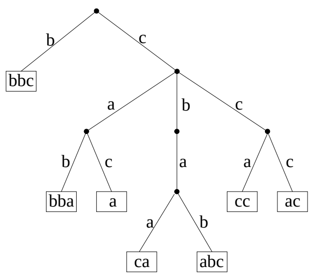


FIGURE 1. Basic trie

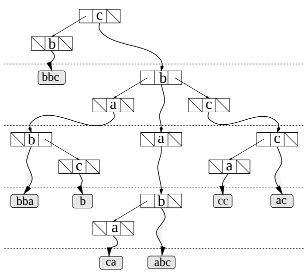


FIGURE 2. Its ternary search trie representation

of tries depend upon the probabilistic properties of the strings processed. More precisely, we shall work with two types of models:

- *The models for the infinite strings inserted in the tries.* These models depend upon the number of strings inserted—either a fixed number n or the output of a Poisson random variable $\mathcal{P}(n)$—and also on the way the characters are emitted after one another—either independently or with some memory scheme such as a Markov process or a continued fraction.
- *The models for the finite keys inserted in the tst nodes.* Examples of such models are the multiset model $\{a_1^{n_1}, a_2^{n_2}, \dots, a_r^{n_r}\}$, the Poisson model $\mathcal{P}(n, p_i)$ or the Bernoulli model $\mathcal{B}(n, p_i)$. It should be emphasized that since the infinite strings are drawn independently, their ith letters are also independent, which is matched by the previous models.

The quantities we are interested in to capture the tries performances are defined as follows:

Definition 1. The comparison path length of a tst t is defined as the sum of the distances from the root to the external nodes, expressed in number of comparison pointers. Similarly, for a string s, the search cost $R(s,t)$ is defined as the number of comparison pointers followed when accessing s in t. More precisely,

$$L(t) = l(\mathrm{root}(t)) + \sum_{i=1}^{r} L(t_i) \quad \text{and} \quad R(a_i s, t) = r_i(\mathrm{root}(t)) + R(s, t_i) \tag{1}$$

with $l()$ the number of external nodes in the sub-tries pointed at by comparison pointers and $r_i()$ the cost of searching a_i in the bst present at the root of t.

2. Tools Used to Perform the Analysis

2.1. Left-to-Right Maxima, Shuffle Product and Formal Laplace Transform.

Let w be a word of $\mathcal{A}^\star$. The ith letter of w denoted w_i is called a left-to-right maximum if $w_i \ge w_j, j = 1, \dots, i-1$. For example, the permutation $a_2 a_3 a_1 a_5 a_4$ has three left-to-right maxima, respectively a_2, a_3 and a_5. If one builds a bst from a permutation, the left-to-right maxima are naturally in bijection with the nodes located on the rightmost branch. For the analysis to be performed in section 3.1, we therefore investigate left-to-right maxima.

Clearly, all the possible decompositions of words by sets of left-to-right maxima are encoded by the regular expression

$$\mathcal{A}^\star = \prod_{j=1}^{r} (\varepsilon + a_j (a_1 + \cdots + a_j)^\star).$$

Marking a_i by the two variables $z x_i$ together with u if it is a left-to-right maximum yields the generating function

$$N_{\max}(z, u, x_1, x_2, \dots, x_r) = \prod_{j=1}^{r} \left(1 + \frac{z u x_j}{1 - z(x_1 + \cdots + x_j)}\right)$$

whose coefficient $[z^n u^k x_1^{n_1} \dots x_r^{n_r}]$ is the number of words of length n that have k maxima and n_j occurrences of the letter a_j. A similar formula holds for $N_{\min}$, the generating function of minima.

Another tool we shall use is the shuffle product $ш$ from which a word can be decomposed into words contained certain letters only:

$$(\mathcal{A} \backslash \{\alpha\})^\star = (a_1 + \cdots + a_{\alpha-1})^\star ш (a_{\alpha+1} + \cdots + a_r)^\star.$$

This product corresponds to the following operation on generating function

$$\left(\sum_n f_n z^n\right) ш \left(\sum_n g_n z^n\right) = \sum_n \left(\sum_{k=0}^{n} \binom{n}{k} f_k g_{n-k}\right) z^n.$$

A nice way to handle it is through the formal Laplace transform defined by $\mathcal{L}\left[\sum_n f_n \frac{z^n}{n!}\right] = \sum_n f_n z^n$. In particular we have $f(z) ш g(z) = \mathcal{L}\left[\mathcal{L}^{-1}[f(z)] \cdot \mathcal{L}^{-1}[g(z)]\right]$.

3. Main Results

3.1. **Search Costs in Bst.** We analyze the cost of searching a letter a_α in the bst $bst(w)$ built from the letters of a word w from $\mathcal{A}^\star$. More precisely: given a letter a_α and a word w, the search cost $c_\alpha(w)$ is defined as the number of edges on the branch corresponding to a_α in the bst built from the letters of w. In particular, we are interested in condensing the cost related informations in the formal sum

$$C_\alpha := \sum_{w \in \mathcal{A}^\star} u^{c_\alpha(w)} \cdot w \tag{2}$$

whose exponent of u refers to the search cost $c_\alpha(w)$. To see how $c_\alpha(w)$ can be evaluated, observe that $w = \text{prefix}(w) \quad a_\alpha? \quad \text{suffix}(w)$ where $a_\alpha?$ means that the letter a_α may be absent. The interest of this decomposition is to show that the cost of searching a_α in the bst built from w is chargeable to prefix(w). And since prefix(w) can be expressed as the shuffle product on the sets of letters $a_1, \ldots, a_{\alpha-1}$ with $a_{\alpha+1}, \ldots, a_r$, the formal sum (2) yields the value of $C_\alpha(z, u, x_1, \ldots, x_r)$:

$$(N_{\max}(z, u, x_1, \ldots, x_{\alpha-1}) ш N_{\min}(z, u, x_{\alpha+1}, \ldots, x_r)) \left(1 + \frac{z x_\alpha}{1 - z(x_1 + \cdots + x_r)}\right).$$

This form condenses all the information on costs. For example, the generating function of average costs is obtained by differentiating with respect to u and setting $u = 1$. For example:

Theorem 1. *The mean search cost of the letter a_α in a bst built from the Poisson model is*

$$\mathrm{E}[C_\alpha] = \sum_{\substack{\min(u,v) \le j \le \max(u,v) \\ j \ne \alpha}} \frac{n_j}{P_{[j,\alpha]}} \left(1 - e^{-zP_{[j,\alpha]}}\right), \qquad \textit{with} \quad P_{[u,v]} = \sum_j p_j.$$

3.2. **Exact Analysis.** In this section, we outline the analysis of the statistics introduced in def. 1. The crux of this analysis consists in using quantities that are independent from the source model the keys are generated by. To see how this works, consider the Poisson process of parameter z. The number N_h of strings that have a given prefix h obeys a Poisson law of parameter $p_h z$, with p_h the source dependent probability for a random string to start with the prefix h. Then, the probabilistic behavior of the tst that corresponds to the prefix h is described by a Poisson model of parameter $\{zp_h\}$ with individual letter probabilities $\{p_{i|h}\}$, with $p_{i|h}$ the conditional probability to have the prefix h followed by the letter a_i. Applying theorem 1 locally and unwinding the recurrences (1) yield

Theorem 2. *The comparison path length and the comparison cost of a random search in a ternary search trie made of n keys have expectations given by*

$$\mathrm{E}[L]_n = 2 \sum_{h \in \mathcal{A}^\star} \sum_{i<j} \frac{p_{h\cdot i} p_{h\cdot j}}{P_h[i,j]^2} [n P_h[i,j] - 1 + (1 - P_h[i,j])^n],$$

$$\mathrm{E}[R]_n = 2 \sum_{h \in \mathcal{A}^\star} \sum_{i<j} \frac{p_{h\cdot i} p_{h\cdot j}}{P_h[i,j]} [1 - (1 - P_h[i,j])^n]$$

	array-trie (standard)	list-trie	bst-trie (tst)
Pointers	$\dfrac{r}{H_S}n$	$\dfrac{2}{H_S}n$	$\dfrac{3}{H_S}n$
Path length	$\dfrac{1}{H_S}n\log n$	$\dfrac{C_S^\star}{H_S}n\log n$	$\dfrac{C_S}{H_S}n\log n$
Search	$\dfrac{1}{H_S}\log n$	$\dfrac{C_S^\star}{H_S}\log n$	$\dfrac{C_S}{H_S}\log n$

TABLE 1.

with $P_h[i,j] = \sum_{k=i}^{j} p_{k\cdot h}$ *and* $p_{h\cdot\alpha} = p_h p_{\alpha|h}$.

A noteworthy feature of this theorem is its independence from the source model since its derivation uses solely the independence of the digits processed. It can therefore be instantiated for the three models mentioned in section 1.

3.3. **Asymptotic Analysis.** We aim at finding asymptotic equivalents to the quantities of theorem 2. These quantities are harmonic sums amenable to a treatment with the Mellin transform [2].

The Mellin machinery applied to the formulae of theorem 2 requires evaluating the $p_{i|j}$ probabilities. This is done under two models: a memoryless (a.k.a. Bernoulli) source outputting infinite strings where the letter a_i has probability to appear independently of past history; and a Markov one producing letters with an initial distribution and with transition probabilities $p_{i|j}$. Singularity analysis on the Mellin transforms (combined with the so-called Dirichlet depoissonization) yields

Theorem 3. *The comparison external path length and random search cost for a ternary search tree built on n keys produced by a source S, either memoryless (m) or Markovian (M), have averages that satisfy*

$$\mathrm{E}[L]_n = \frac{C_S}{H_S} n\log n + O(n) \qquad \textit{and} \qquad \mathrm{E}[R]_n = \frac{C_S}{H_S}\log n + O(1)$$

where the entropy H_S and the quantity C_S are source-dependent constants.

3.4. **Comparative Studies.** Theorems 3 and 2 quantify precisely the access costs for tst. The same analysis can be carried out for the list-trie variant, while the parameters describing standard array-trie stem from Knuth's books. The results are summarized in table 1—with $C_m^\star$ and $C_M^\star$ constants known in closed forms—and show that the three structures have logarithmic costs and require linear space. In order to assess the relevance of these theoretical analyses, a simulation campaign was undertaken on Herman Melville's novel, *Moby Dick*. Its conclusions are [1]:

> *Ternary search tries are an efficient data structure from the information theoretic point of view since a search costs typically about* $\log n$ *comparisons. List-tries require about 3 times as many comparisons. For an alphabet of cardinality 26, the storage cost of ternary search tries is about 9 times smaller than standard array-tries.*

Bibliography

[1] Clément (Julien), Flajolet (Philippe), and Vallée (Brigitte). – The analysis of hybrid trie structures. In *Proceedings of the Ninth Annual ACM–SIAM Symposium on Discrete Algorithms*. pp. 531–539. – Philadelphia, 1998.

[2] Flajolet (Philippe), Gourdon (Xavier), and Dumas (Philippe). – Mellin transforms and asymptotics: harmonic sums. *Theoretical Computer Science*, vol. 144, n° 1-2, 1995, pp. 3–58. – Special volume on mathematical analysis of algorithms.

Pólya Urn Models in Random Trees

Hosam M. Mahmoud
The George Washington University

October 20, 1997

[summary by Marko R. Riedel]

1. Examples and previous results

Consider an urn that contains balls of k different colors $1, 2, \ldots, k$. There is a set of evolution rules: *(i)* a ball is chosen at random from the urn, where all balls are equally likely; *(ii)* that ball's color or type is noted, and the ball is returned to the urn; *(iii)* if the ball had color i, α_{ij} balls of color j are added to the urn.

Question of interest. What is the composition of the urn after n draws?

The model is encoded in the *addition matrix* $A = [\alpha_{ij}]$, $1 \leq i, j \leq k$. The α_{ij} may themselves be random, but this talk is concerned exclusively with deterministic α_{ij}, i.e., the case of a fixed addition matrix A.

Pólya and Eggenberger (1923) investigated the two-color problem, with $A = sI$ and s a positive integer. Suppose the two colors are red and blue, and let R_n and B_n be the number of red and blue balls after n picks.

Example. Set $s = 2$ and start with two red balls and one blue ball. One of eight possible length-3 runs is: Pick blue (probability 1/3), the composition of the urn is now $R_1 = 2$ and $B_1 = 3$; Pick blue (probability 3/5), $R_2 = 2$ and $B_2 = 5$; Pick red (probability 2/7), $R_3 = 4$ and $B_3 = 7$.

What is the typical behavior of R_n and B_n? Bernard Friedman (1949) studied a more general urn, the addition matrix now being $A = \left[\begin{smallmatrix} \alpha & \beta \\ \beta & \alpha \end{smallmatrix}\right]$. Freedman (1965) showed that

$$R_n^* \xrightarrow{D} N(0,1), \quad B_n^* \xrightarrow{D} N(0,1), \qquad \text{where} \qquad R_n^* = \frac{R_n - E[R_n]}{\sqrt{V[R_n]}}$$

and B_n^* is defined similarly.

2. The connection to random trees

Recall the random permutation model for binary trees, where n keys are inserted into a binary tree such that the root of any subtree is larger than all left and less than all right descendants. We have a uniform distribution on the $n!$ possible key orderings and wish to compute tree statistics associated to this model.

The Poblete-Munro (1985) heuristic suggests that we can obtain a more balanced tree with little extra work: we require that all subtrees on the fringe and of size at most three be balanced. This means that we rebalance size 3 subtrees on the fringe, if necessary. This process yields shorter trees; in fact $E[D_n] = (12/7) \ln n$ (compare with $2 \ln n$ for standard RBSTs).

2.1. **Balanced trees.** Work by Yao (1978) on 2-3 trees, Baeza-Yates, Gonnet and Ziviani on other tree statistics S_n shows that we can study $E[S_n]$ by studying fringe configurations of RBSTs, to obtain bounds of the type $f_1(n) \leq E[S_n] \leq f_2(n)$. Fringe analysis is based on exact counting of all (sub)trees less than or equal to a given height. The results improve in accuracy as the height is increased.

Mahmoud (1998) has used Pólya urn models to study the Poblete-Munro heuristic. We map fringe configurations to colors. The growth of the tree is modeled by a 3×3 urn. Suppose an incoming node is placed on one of the four leaves of a balanced subtree on three nodes. It is inserted without rebalancing the tree. Its sibling is a leaf. Suppose the next node is placed at that leaf. No rebalancing is required. Finally suppose that the next node is not placed at the sibling leaf, but rather at a leaf of the previous node. The tree must be rebalanced. We distinguish these three configurations by assigning different colors to the leaves concerned: color 1 to the leaves of any terminal node whose sibling is not a leaf, color 3 to the leaves of any terminal node whose sibling is a leaf, and color 2 to all such leaves. The leaves correspond to balls in a Pólya urn. The complexity measure of an insertion is the number of rotations, call it R_n. The addition matrix of the Pólya urn becomes

$$A = \begin{bmatrix} -2 & 1 & 2 \\ 4 & -1 & -2 \\ 4 & -1 & -2 \end{bmatrix}.$$

E.g., if we replace a leaf of color 1, we lose that leaf and recolor its sibling with color 2. The new leaves have color 3. R_n is therefore the number of picks of color 3. The row sums of the addition matrix A form the vector $S = [1, 1, 1]^T$, which reflects the fact that every BST on n nodes has $n+1$ leaves.

If an addition matrix A has the property that there exists an m such that all the entries of A^m are positive, we say that A is *regular*. In this particular example, A is not regular; nonetheless Mahmoud (1998) shows that

$$\frac{R_n - 2/7n}{\sqrt{n}} \xrightarrow{D} N\left(0, 66/637\right).$$

2.2. **m-ary search trees.** Under this model $m-1$ keys $k_1, k_2, \ldots, k_{m-1}$ are placed at the root of the tree. These keys partition the remaining keys into m intervals, $(-\infty, k_1), (k_1, k_2), \ldots, (k_{m-1}, +\infty)$, i.e., subtrees. The construction is recursive and the branch factor is m.

Example. Let $m = 3$ and consider the keys $9, 16, 4, 23, 11, 10, \ldots$ The first two keys are placed at the root, the key 4 is placed to the left of 9 and starts a new subtree, 23 is placed to the right of 16, also in a new subtree, and 11 and 10 fall between 9 and 16, starting a new subtree with root intervals $(9, 10)$, $(10, 11)$ and $(11, 16)$. There are three types of nodes (or *blocks* in a hardware-oriented setting): leaves, nodes that contain a single key, and nodes that contain two keys.

More generally, we ask about S_n, the number of nodes after n insertions, where $S_n = \sum_j X_n^j$ and X_n^j counts the number of nodes that contain j keys. We construct an urn model by mapping gaps between keys at a node to balls whose color indicates the number of gaps at that node. We can recover the number of nodes of each type from the number of gaps of the corresponding color. For instance, consider a leaf that contains i keys and hence $i+1$ gaps. We map these gaps to balls of color $i+1$. Now suppose that $i < m-1$ and we insert a key at this leaf. We lose $i+1$ gaps of color $i+1$ and gain $i+2$ gaps of color $i+2$. The addition matrix associated to this model has the following shape:

$$A = \begin{bmatrix} & \ddots & & & & & \\ & \cdots & -r & r+1 & & & \\ & \cdots & \cdots & -(r+1) & r+2 & & \\ & & & & & \ddots & \\ m & & & & & & -1 \end{bmatrix}.$$

The eigenvalues of the addition matrix A. Order the eigenvalues according to their real part, letting λ_1 be the eigenvalue whose real part is the largest. Athreya and Nay (1972) showed that if the real part of λ_2 is less than half the real part of λ_1, a condition guaranteed if A is regular, then the colors have a normal $N(0,1)$ distribution.

In the urn model associated to m-ary trees, this property holds for $m < 27$, even though the associated urn is not regular. (This suggests that regularity is too strong a precondition for the results of Athreya and Nay.) When $m = 27$, there are two conjugate eigenvalues whose real part is larger than half the real part of λ_1. More precisely, Lew and Mahmoud (1994) showed that for any sequence $c_1, c_2, \ldots, c_k$, where c_j is the cost of a node that contains j keys, the vector of random variables $\mathbf{X}_n = [X_n^1, X_n^2, \ldots, X_n^k]^T$ converges to a multivariate normal, i.e.,

$$\frac{\mathbf{X}_n - E[\mathbf{X}_n]}{\sqrt{n}} \xrightarrow{D} \mathrm{MVN}(0, \Lambda) \qquad \text{for} \qquad m = 2, 3, \ldots, 26.$$

2.3. **Paged binary trees.** In this model every external node stores at most b keys, while internal nodes store a single key. Overflow on external nodes is processed by splitting the node according to some splitting rule, say by selecting the median and adding two subtrees whose roots store $b/2$ keys. The corresponding counting problem leads to a differential equation in $F(x,y)$, the super exponential generating function of paged binary trees:

$$\frac{\partial^{b-1} F(x,y)}{\partial x^{b-1}} = \left(\frac{\partial F(x,y)}{\partial x}\right)^2.$$

PBSTs have been considered by Flajolet, Mahmoud and Martínez Parra. Results that are based on Pólya urn models indicate that there is a phase transition at $b = 118$, when the real part of the second eigenvalue of the addition matrix becomes larger than half the real part of the first eigenvalue. Work in progress by Flajolet *et al.* seeks to construct an interpretation of this fact in the context of generating functions.

3. Case study: plane-oriented recursive trees

This type of tree models a recruiting process where the recruiting probability of a recruiting officer increases with the number of recruits attracted so far, or more generally, where the probability of a node to receive a new node is proportional to its degree, a scenario that Mahmoud (1991) calls "success breeds success." We use plane-oriented recursive trees as the underlying model[1], as proposed by Bergeron, Flajolet and Salvy (1992). Every node has outdegree $2k+1$, for some $k \geq 0$; k of its children are plane-embedded nodes, and $k+1$ leaves are placed in the gaps between adjacent nodes.

[1]If we were using the terminology of combinatorial analysis, we would refer to these trees as increasing trees; more precisely, as R-enriched increasing trees, where R is the *list* structure.

Consider a chain letter scheme where the acquisition price of a letter is 100F, and copies of the letter are sold at 40F. Given that there are n participants in the scheme, we ask how many of them have just broken even, i.e., sold three letters. Let blue represent insertion slots at nodes that have bought, but not sold a single letter; red, nodes that bought and sold one copy of the letter, green, two copies, and white, three, i.e., broken even, and let B_n, R_n, G_n and W_n be the corresponding RVs. (We start with a single participant, i.e., $B_0 = 1$, $R_0 = G_0 = W_0 = 0$.) Finally, assume that the success probability of a participant is proportional to the number of letters sold (other models are possible and even reasonable). The addition matrix is easily seen to be

$$A = \begin{bmatrix} 0 & 2 & 0 & 0 \\ 1 & -2 & 3 & 0 \\ 1 & 0 & -3 & 4 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

E.g., if a participant has sold two letters and sells another, the three green insertion slots at the corresponding node are replaced by four white ones, and a new participant who has not sold any copy of his letter yet must be accounted for. Note that A is not regular. It can be shown that B_n is the number of leaves in a random tree of size $n + 1$.

Mahmoud, Smythe and Szymański (1993) show that

$$\mathrm{E}\begin{pmatrix} B_n \\ R_n \\ G_n \end{pmatrix} \sim \begin{pmatrix} 1/3 \\ 1/6 \\ 1/10 \end{pmatrix} (2n+1),$$

and that the covariance matrix is

$$\mathrm{Cov}(B_n, R_n, G_n) \sim \begin{pmatrix} 1/9 & -8/45 & -1/15 \\ -8/45 & 23/45 & -11/105 \\ -1/15 & -11/105 & -179/350 \end{pmatrix} n.$$

We sketch the proof of this result. Introduce the indicator variables $I_n^{(B)}, I_n^{(R)}, I_n^{(G)}$, $I_n^{(W)}$ so that $I_n^{(B)} + I_n^{(R)} + I_n^{(G)} + I_n^{(W)} = 1$. We now have e.g., $R_n = R_{n-1} + 2I_n^{(B)} - 2I_n^{(R)}$, and hence

$$E[R_n] = E[R_{n-1}] + 2E[I_n^{(B)}] - 2E[I_n^{(R)}].$$

The expectations of the indicator variables are obtained by conditioning on the $n-1$ picks that lead to a particular urn (call this σ-field T_{n-1}), so that

$$E[I_n^{(B)} \mid T_{n-1}] = \frac{B_{n-1}(T_{n-1})}{2n-1} \quad \text{and} \quad E[I_n^{(B)}] = \frac{E[B_n]}{2n-1}.$$

Substitute to get

$$E[R_n] = E[R_{n-1}] + 2\frac{E[B_n]}{2n-1} - 2\frac{E[R_n]}{2n-1}.$$

Similar computations for $E[B_n]$, $E[G_n]$ and $E[W_n]$ yield a system of recurrences of the form

$$[B_n, R_n, G_n, W_n]^T = F(n)[B_{n-1}, R_{n-1}, G_{n-1}, W_{n-1}]^T$$

where $F(n)$ is a matrix that depends on n. This system may be solved asymptotically. (Note that we have made critical use of the fact that the total number of balls in the urn is a function of n, namely $2n + 1$.)

The computation of the covariance is more involved. Start from $R_n = R_{n-1} + 2I_n^{(B)} - 2I_n^{(R)}$ as before, square both sides and use simple properties of mutually exclusive indicator variables to get

$$R_n^2 = R_{n-1}^2 + 4I_n^{(B)}R_{n-1} - 4I_n^{(R)}R_{n-1} + 4I_n^{(B)} + 4I_n^{(R)}.$$

Binary cross products of the four RVs appear on taking expectations, i.e., we develop recurrences for $E[R_n^2] = E[R_n R_n]$ and these recurrences involve terms like

$$\begin{aligned} E[I_n^{(B)} R_{n-1}] &= E\Big[E[I_n^{(B)} R_{n-1} \mid T_{n-1}]\Big] \\ &= E\Big[R_{n-1} E[I_n^{(B)} \mid T_{n-1}]\Big] = E\left[R_{n-1}\frac{B_{n-1}}{2n-1}\right] = \frac{E[R_{n-1}B_{n-1}]}{2n-1} \end{aligned}$$

The result is a system of recurrences in all binary cross products that yields the desired asymptotics.

Next consider the vector X_i of centered RVs;

$$X_i = \begin{pmatrix} B_i^* \\ R_i^* \\ G_i^* \end{pmatrix} = \begin{pmatrix} B_i \\ R_i \\ G_i \end{pmatrix} - (2i+1)\begin{pmatrix} 1/3 \\ 1/6 \\ 1/10 \end{pmatrix}$$

Mahmoud, Smythe and Szymanski (1993) show that

$$\frac{X_i}{\sqrt{n}} \xrightarrow{D} \mathrm{MVN}\left(0, \begin{pmatrix} 1/9 & -8/45 & -1/15 \\ -8/45 & 23/45 & -11/105 \\ -1/15 & -11/105 & -179/350 \end{pmatrix}\right).$$

The proof uses martingale techniques. Recall that a martingale is a sequence $Y_1, Y_2, Y_3, \ldots$ of random variables such that $E[Y_n \mid T_{n-1}] = Y_{n-1}$. E.g., consider a fair game ("win all or lose all with equal probability, i.e., 1/2"), which gives

$$E[Y_n \mid T_{n-1}] = 0 \cdot Y_{n-1}\frac{1}{2} + 2Y_{n-1}\frac{1}{2} = Y_{n-1}.$$

Note that $E[Y_n] = E[Y_{n-1}] = \cdots = E[Y_1] = 0$ in this example; this is known as the *martingale difference property*, because if $Y_1, Y_2, Y_3, \ldots$ is a martingale, then $E[Y_n - Y_{n-1} \mid T_{n-1}] = 0$. We can reconstruct the martingale from the sequence of first differences, i.e., via $\sum_{k=1}^{n} \triangle Y_k = Y_n$. More generally, we can construct a martingale from any sequence of random variables that has the martingale difference property; this was done e.g., by Régnier (1989) in the context of algorithms, who showed that the cost of Quicksort has a limit distribution.

If $E[\triangle Z_i \mid T_{i-1}] = 0$, then $A_n = \sum_{i=1}^{n} \triangle Z_i$ is a martingale, because

$$E[A_n \mid T_{n-1}] = E\left[\sum_{i=1}^{n} \triangle Z_i \mid T_{n-1}\right] = E\left[\triangle Z_n + \sum_{i=1}^{n-1} \triangle Z_i \mid T_{n-1}\right] = \sum_{i=1}^{n-1} \triangle Z_i = A_{n-1}.$$

By linearity, $E[\triangle Z_i \mid T_{i-1}] = 0$ implies $E[b_i \triangle Z_i \mid T_{i-1}] = 0$ for any sequence of constants $\{b_i\}$, and hence $\sum_{i=1}^{n} b_i \triangle Z_i$ is a martingale.

We return to the four-color urn of the chain letter scheme; consider the color blue.

$$E[B_i \mid T_{i-1}] = E\Big[B_{i-1} + \Big(1 - I_n^{(B)}\Big) \mid T_{i-1}\Big] = B_{i-1} + 1 - E[I_n^{(B)} \mid T_{i-1}] = B_{i-1} + 1 - \frac{1}{2i-1}B_{i-1}$$

Further manipulation yields

$$\begin{aligned} E[B_i - 1/3(2i+1) \mid T_{i-1}] &= (B_{i-1} - 1/3(2i-1)) + 1/3(2i-1) - 1/3(2i+1) \\ &\quad + 1 - \frac{1}{2i-1}(B_{i-1} - 1/3(2i-1)) - 1/3 \end{aligned}$$

and hence $E[B_i^* \mid T_{i-1}] = B_{i-1}^* - B_{i-1}^*/(2i-1)$. B_i^* is not a martingale but

$$B_i^* - B_{i-1}^* + \frac{1}{2i-1}B_{i-1}^*$$

is a *martingale difference*, because $E\left[\triangle \mathrm{M}_i^B \mid T_{n-1}\right]=0$, where we have set

$$\triangle \mathrm{M}_i^B = B_i^* - B_{i-1}^* + \frac{1}{2i-1} B_{i-1}^*.$$

We can construct a martingale from $\triangle \mathrm{M}_i^B$, since$\sum_{i=1}^n b_i \triangle \mathrm{M}_i^B$ is a martingale for any sequence $\{b_i\}$.

The *Cramér-Wold* device can be used to prove convergence to a multivariate normal. Suppose we seek $[X_n^{(1)}, X_n^{(2)}, X_n^{(3)}, \ldots, X_n^{(j)}]^T \xrightarrow{D} \mathrm{MVN}(0,\Lambda)$. It suffices to prove that any linear combination of the $X_n^{(\cdot)}$ converges to a normal distribution, i.e.,

$$\alpha_1 X_n^{(1)} + \alpha_2 X_n^{(2)} + \cdots + \alpha_j X_n^{(j)} \xrightarrow{D} N\left(0, \sigma_{\alpha_1,\ldots,\alpha_j}\right),$$

$\alpha_1, \alpha_2, \ldots, \alpha_j$ arbitrary. Here $j=3$ and we study $W_n = \alpha_1 B_n^* + \alpha_2 R_n^* + \alpha_3 G_n^*$. Centering the remaining two variables, we have

$$\begin{aligned}
E[B_i^* - B_{i-1}^* \mid T_{i-1}] &= -\frac{1}{2i-1} B_{i-1}^* \\
E[R_i^* - R_{i-1}^* \mid T_{i-1}] &= +\frac{2}{2i-1}(B_{i-1}^* - R_{i-1}^*) \\
E[G_i^* - G_{i-1}^* \mid T_{i-1}] &= +\frac{3}{2i-1}(R_{i-1}^* - G_{i-1}^*).
\end{aligned}$$

Introduce the martingale differences

$$\begin{aligned}
\triangle \mathrm{M}_i^B &= B_i^* - B_{i-1}^* + \frac{1}{2i-1} B_{i-1}^* \\
\triangle \mathrm{M}_i^R &= R_i^* - R_{i-1}^* - \frac{2}{2i-1}(B_{i-1}^* - R_{i-1}^*) \\
\triangle \mathrm{M}_i^G &= G_i^* - G_{i-1}^* - \frac{3}{2i-1}(R_{i-1}^* - G_{i-1}^*)
\end{aligned}$$

and set $V_{nk} = \sum_{i=1}^{k} \left(b_{in} \triangle \mathrm{M}_i^B + c_{in} \triangle \mathrm{M}_i^R + d_{in} \triangle \mathrm{M}_i^G\right)$ for arbitrary $\{b_{in}\}, \{c_{in}\}, \{d_{in}\}$. It remains to choose $\{b_{in}\}, \{c_{in}\}$ and $\{d_{in}\}$. Expand V_{nn} to get

$$V_{nn} = b_{nn}\left(B_n^* - B_{n-1}^* + \frac{1}{2n-1} B_{n-1}^*\right) + \cdots + \left(B_{n-1}^* - B_{n-2}^* + \frac{1}{2n-3} B_{n-3}^*\right) + \cdots$$

To obtain the particular linear combination $\alpha_1 B_n^* + \alpha_2 R_n^* + \alpha_3 G_n^*$ we set $b_{nn} = \alpha_1$, so that the term in B_n^* is preserved, and choose the remaining $b_{n,i}$ to cancel B_{n-1}^*, B_{n-2}^* etc. This technique can be used to show that given α_1, α_2 and α_3, we may choose constants $\{b_{in}\}, \{c_{in}\}$ and $\{d_{in}\}$, so that

$$V_{nn} = (\alpha_1 B_n^* + \alpha_2 R_n^* + \alpha_3 G_n^*) - 3/2 c_{1n} + 10/3 d_{1n},$$

which by a martingale central limit theorem yields

$$\frac{\alpha_1 B_n^* + \alpha_2 R_n^* + \alpha_3 G_n^*}{\sqrt{n}} \sim \frac{V_{nn}}{\sqrt{n}}, \qquad \text{hence} \qquad \frac{W_n}{\sqrt{n}} \xrightarrow{D} N\left(0, \sigma_{\alpha_1,\ldots,\alpha_j}\right), \quad \begin{pmatrix} B_n^* \\ R_n^* \\ G_n^* \end{pmatrix} \xrightarrow{D} \mathrm{MVN}(0,\Lambda).$$

Concluding remark

It should be obvious from the highly restricted class of addition matrices that have been considered that an abundance of combinatorial problems and possible addition matrices remain to be analyzed; e.g., apparently simple instances such as $\left[\begin{smallmatrix} 2 & 0 \\ 3 & 4 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$ have so far resisted attack.

A Top-Down Analysis of Fringe-Balanced Binary Search Trees

Helmut Prodinger

Technical University of Vienna

May 25, 1998

[summary by Michèle Soria]

Abstract

Fringe-balanced binary search trees are obtained by performing rotations only on subtrees of size three. The parameter "number of rotations" has recently been studied by Mahmoud [3], using a Pólya urn model. This talk, based on [5] proposes a top-down approach of the problem, that leads to a differential equation. The solution is related to the Weierstrass' $\wp$-function. This fact allows to derive the asymptotic normality of the parameter by means of Hwang's quasi-power theorem [2]. An alternative way of obtaining the exact expectation and variance, which relies on operator calculus, is also presented.

It is well-known that in a random binary search tree constructed by insertion at the leaves, the average depth of a node is logarithmic in the size of the tree, so that retrieval of the data stored in the nodes can be done efficiently. One simple way to improve the speed of retrieval even more is to compress the subtrees near the leaves by doing a *fringe-balanced rotation*: whenever a son is appended to a node that itself is a single son (its "brother" is an external node), a rotation of the three nodes is performed to place the median of the three elements as the root of the subtree and the other two elements as sons. Therefore all subtrees of size 3 in the tree are complete.

The distribution of the number of rotations that are made when constructing such a fringe-balanced binary tree under the random permutation model was recently analyzed by Mahmoud [3], using a Pólya urn model, and a central limit theorem for urn models by Smythe [6]. Here is presented an alternative way, based on analytic methods, of proving the Gaussian limiting distribution. This presentation follows [5].

1. Top-Down Approach

The recursive top-down analysis (see [4] for various uses of this approach) begins with a recurrence relation based on *splitting probabilities*. When constructing a fringe-balanced tree from a random permutation, the first three elements of the permutation determine the root of the final tree, as well as whether or not there is a rotation at the root (a rotation occurs in four cases out of six).

Hence the splitting probability $\pi_{n,k}$, which is the probability that in a tree of size n the root is the node k, is given by

$$\pi_{n,k} = \frac{(k-1)(n-k)}{\binom{n}{3}}$$

for $n \geq 3$ and $1 \leq k \leq n$, $\pi_{2,1} = \pi_{2,2} = 1/2$ and $\pi_{1,1} = 1$. And we also get a recurrence relation for the probability $F_{n,m}$, that the number of rotations is m, when generating a fringe balanced tree of size n, starting with an empty tree (the number of rotations to construct the root of the tree is 1 with probability 2/3, and 0 with probability 1/3). Thus for $n \geq 3$ and $1 \leq m \leq n$:

$$F_{n,m} = \frac{1}{3} \sum_{k=1}^{n} \pi_{n,k} \sum_{l=0}^{m} F_{k-1,l} F_{n-k,m-l} + \frac{2}{3} \sum_{k=1}^{n} \pi_{n,k} \sum_{l=0}^{m-1} F_{k-1,l} F_{n-k,m-1-l} \tag{1}$$

with initial values $F_{0,0} = 1$, $F_{1,0} = 1$, $F_{2,0} = 1$ and $F_{n,m} = 0$ otherwise.

Introducing the probability generating function $F(z,v) = \sum_{n,m \geq 0} F_{n,m} z^n v^m$ this recurrence leads to the differential equation $\frac{1}{6} \frac{\partial^3}{\partial z^3} F(z,v) = \left(\frac{1}{3} + \frac{2}{3} v\right) \left(\frac{\partial}{\partial z} F(z,v)\right)^2$, with initial conditions $F(0,v) = 1$, $\frac{\partial}{\partial z} F(z,v)\big|_{z=0} = 1$ and $\frac{\partial^2}{\partial z^2} F(z,v)\Big|_{z=0} = 2$.

Substituting $G(z,v) = \frac{\partial}{\partial z} F(z,v)$ this differential equation can be rewritten as

$$\frac{\partial^2}{\partial z^2} G(z,v) = (2+4v) G(z,v)^2 \tag{2}$$

with $G(0,v) = 1$ and $\frac{\partial}{\partial z} G(z,v)\big|_{z=0} = 2$.

1.1. **Moments.** The moments of the distribution are obtained by differentiating equation (2) with respect to v, and evaluating at $v = 1$. Let

$$M_1(z) = \frac{\partial}{\partial v} G(z,v)\Big|_{v=1} = \sum_{n \geq 0} n M_n^{(1)} z^{n-1}, \qquad \text{and} \qquad M_2(z) = \frac{\partial^2}{\partial v^2} G(z,v)\Big|_{v=1} = \sum_{n \geq 0} n M_n^{(2)} z^{n-1},$$

where $M_n^{(1)}$ and $M_n^{(2)}$ denote the first and second factorial moments of the number of rotations.

$M_1(z)$ and $M_2(z)$ both satisfy an Euler differential equation. Extracting the coefficients of the solutions $M_1(z)$ and $M_2(z)$ leads to exact values for the expectation $M_n = M_n^{(1)}$ and the variance $\mathrm{Var}_n = M_n^{(2)} + M_n^{(1)} - \left(M_n^{(1)}\right)^2$:

Theorem 1. *The expectation and the variance of the number of rotations when generating a fringe balanced binary search tree of size n are given by*

$$M_n = \frac{2}{7} n - \frac{8}{21} \quad (n \geq 6), \qquad \mathrm{Var}_n = \frac{66}{637} n - \frac{680}{5733} \quad (n \geq 12).$$

1.2. **Limiting Distribution.** Equation (2) transforms into

$$\frac{4}{3}(1+2v) G^3(z,v) + \frac{8}{3}(1-v) = \left(\frac{\partial}{\partial z} G(z,v)\right)^2,$$

from which we get the implicitly given solution of $G(z,v)$:

$$z = \int_1^{G(z,v)} dx \Big/ \sqrt{\frac{4}{3}(1+2v)x^3 + \frac{8}{3}(1-v)}.$$

This form shows a close relation between $G(z,v)$ and the Weierstrass' $\wp$-function, which can be characterized, within a simply connected domain of $\mathbb{C}_\infty$, which contains no zeros of the denominator, by the integral $\zeta = \int_{\wp(\zeta)}^{\infty} dx/\sqrt{4x^3 - g_2 x - g_3}$. Constants g_2 and g_3 are called the *invariants* of $\wp$.

Indeed, making the substitution

$$t = \sqrt{\frac{1+2v}{3}} \left(z - \int_1^{\infty} \frac{dx}{\sqrt{\frac{4}{3}(1+2v)x^3 + \frac{8}{3}(1-v)}} \right) \equiv \sqrt{\frac{1+2v}{3}} (z - s(v)),$$

it is shown in [5] that $W(t,v) = G(z(t),v)$ is a Weierstrass' $\wp$-function with invariants $g_2 = 0$ and $g_3 = -8(1-v)/(1+2v)$.

Since $\wp(\zeta)$ has a double pole at $\zeta = 0$, it follows that $G(z,v)$ has a double pole at $z = s(v)$, where it admits the local expansion $G(z,v) = \frac{3}{1+2v}\left(z - s(v)\right)^{-2} + \mathcal{O}\left(z - s(v)\right)^4$.

Integrating term by term, we obtain the expansion of $F(z,v)$:

$$F(z,v) = \frac{1}{\frac{1+2v}{3}s(v)\left(1 - \frac{z}{s(v)}\right)} + \mathcal{O}\left(z - s(v)\right)^5.$$

Singularity analysis leads immediately to the expansion of the coefficients:

$$[z^n]F(z,v) = \frac{1}{\frac{1+2v}{3}s(v)}s(v)^{-n} + \left(1 + \mathcal{O}\left(\frac{1}{n^4}\right)\right) \tag{3}$$

Performing a series expansion of the integrand, the integral $s(v)$ can be expressed in terms of a hypergeometric function:

$$\sqrt{\frac{1+2v}{3}}s(v) = {}_2F_1\left(\left.\begin{matrix}\frac{1}{2}, \frac{1}{6}\\ \frac{7}{6}\end{matrix}\right| -\frac{2(1-v)}{1+2v}\right).$$

In (3), the probability generating function of the number of rotations is given in a form that satisfies the hypothesis of Hwang's quasi-power theorem [2], so that we finally get the central limit theorem:

Theorem 2. *The distribution X_n of the number of rotations, when generating a fringe balanced binary search tree is asymptotically Gaussian:*

$$\Pr\left\{\frac{X_n - \frac{2}{7}n}{\sqrt{\frac{66}{637}n}} \leq x\right\} = \Phi(x) + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right).$$

2. Urn Model and Operator Calculus

Insertions in fringe-balanced binary search trees can be translated into an urn model of Pólya. The urn contains balls of three different colors, corresponding to the leaves of the tree: binary subtrees of size 3 (which are always complete) have four leaves of color 1; in subtrees of size 2, the two deepest leaves are colored by 3, and the third one is colored by 2. We start with an urn containing two balls of color 1, corresponding to a starting tree with one internal node. Inserting at a leaf of color 1, i.e. picking a ball of color 1, results in replacing two leaves of color 1 by one leaf of color 2 and two leaves of color 3. Inserting at a leaf of color 2 results in replacing this leaf and its two associated leaves of color 3 by four leaves of color 1. In the same manner, inserting at a leaf of color 3 results in replacing two leaves of color 3 and one leaf of color 2 by four leaves of color 1. Thus the process of insertion translates into the ball addition matrix A, whose (i,j) entry is the number of balls of type j to be added when a ball of color i is picked:

$$A = \begin{pmatrix} -2 & 1 & 2 \\ 4 & -1 & -2 \\ 4 & -1 & -2 \end{pmatrix}.$$

Working on the addition matrix, Mahmoud [3] obtains the exact averages and covariances for the number of balls in the urn after n picks, as well as the exact average and variance of the number of rotations after n random insertions in an empty fringe balanced tree.

These results can also be obtained by operator calculus [1]. Define the random variables $X_n^{(k)}$ to denote the number of balls of color k in the urn, when $n+1$ elements are in the urn altogether (after $n-1$ random picks). Only the values $\mathbb{E}\{X_n^{(2)}\}$ and $\mathbb{V}\{X_n^{(2)}\}$ must be calculated, since all other values follow by the relations $X_n^{(3)} = 2X_n^{(2)}$ and $X_n^{(1)} + X_n^{(2)} + X_n^{(3)} = n+1$. We denote by $p_{n,k}$ the probability $\mathbb{P}\{X_n^{(2)} = k\}$ and by $P_n(u)$ the generating function $\sum_{k\geq 0} p_{n,k}u^k$. The urn picking process leads to the recursion

$$P_{n+1}(u) = \sum_{k\geq 0} p_{n,k}\left[\frac{3k}{n+1}u^{k-1} + \left(1 - \frac{3k}{n+1}\right)u^{k+1}\right] = \sum_{k\geq 0}\left(u + \frac{3}{n+1}(1-u^2)D\right)p_{n,k}u^k$$

where D denotes the differential operator $\frac{d}{du}$. If evaluation at $u=1$ is denoted by operator U, we get then for $n \geq 6$:

$$\mathbb{E}\{X_{n+1}^{(2)}\} = UDP_{n+1}(u) = \left(U + \left(1 - \frac{6}{n+1}\right)UD\right)P_n(u) = 1 + \frac{n-5}{n+1}\mathbb{E}\{X_n^{(2)}\}$$

with $\mathbb{E}\{X_6^{(2)}\} = 1$. This linear recursion is easily solved and we get $\mathbb{E}\{X_n^{(2)}\} = \frac{1}{7}(n+1)$ for $n \geq 6$. A similar computation holds for the second factorial moment $\mathbb{E}\{X_{n+1}^{(2)}(X_{n+1}^{(2)} - 1)\} = UD^2P_{n+1}(u)$, from which the variance is obtained.

The average and variance of the number of rotations can also be treated in this way. Let the random variable R_n denote the number of rotations made when constructing a fringe balanced tree with n elements (or, in the urn model, the number of picks of elements with color 3 after $n-1$ random picks). Introduce the bivariate generating functions $R_n(u,v) = \sum_{k,l} p_{n,k,l}u^kv^l$, where $p_{n,k,l}$ denotes the probability, that after $n-1$ random picks k balls in the urn are of color 2 and l times a ball of color 3 was chosen. Following the picking process, the recursion for R_n is

$$R_{n+1}(u,v) = \sum_{k,l} p_{n,k,l}\left(\frac{k}{n+1}u^{k-1}v^l + \frac{2k}{n+1}u^{k-1}v^{l+1} + \left(1 - \frac{3k}{n+1}\right)u^{k+1}v^l\right).$$

Denoting by D_u and D_v the differential operator w.r.t. u resp. v and by U_u and U_v the evaluations at $u=1$ resp. $v=1$, we get for the expectation $\mathbb{E}\{R_{n+1}(u,v)\} = U_uU_vD_vR_{n+1}(u,v)$

$$\mathbb{E}\{R_{n+1}(u,v)\} = \left(\frac{2}{n+1}U_uU_vD_u + U_uU_vD_v\right)R_n(u,v) = \mathbb{E}\{R_n(u,v)\} + \frac{2}{n+1}\mathbb{E}\{X_n^{(2)}\}.$$

The average value of R_n is obtained by solving this recursion, and similar computations lead to the variance.

Bibliography

[1] Greene (D. H.) and Knuth (D. E.). – *Mathematics for the analysis of algorithms.* – Birkhäuser, Boston, 1982, second edition.

[2] Hwang (H.-K.). – *Théorèmes limites pour les structures combinatoires et les fonctions arithmetiques.* – PhD thesis, École Polytechnique, December 1994.

[3] Mahmoud (H.). – On rotations in fringe-balanced binary search trees. *Information Processing Letters*, vol. 65, 1998, pp. 41–46.

[4] Martinez (C.), Panholzer (A.), and Prodinger (H.). – On the number of descendants and ascendants in random search trees. *Electronic Journal of Combinatorics*, vol. 5(1):#R20, 1998.

[5] Panholzer (A.) and Prodinger (H.). – An analytic approach for the analysis of rotations in fringe-balanced binary search trees. – To appear in *Annals of Combinatorics*, 1998.

[6] Smythe (R.). – Central limit theorems for urn models. *Stochastic Processes and their Applications*, vol. 65, 1996, pp. 115–137.

Binary Search Tree and 1-dimensional Random Packing

Yoshiaki Itoh
Institute of Statistical Mathematics, Tokyo, Japan

September 22, 1997

[summary by Hosam M. Mahmoud]

This talk surveys some models of random trees underlying continuous partitioning processes:
1. One-dimensional random sequential packing;
2. Kakutani's interval splitting;
3. The random sequential bisection model;
4. The continuous binary search tree.

1. One-Dimensional Random Sequential Packing

The first model was introduced in [5]. In this model we place a unit interval I_1 at a random position in the interval $[0, x]$. We assume that the initial point ξ_1 of the interval I_1 is Uniform-$[0, x-1]$. The interval $(\xi_1, \xi_1 + 1)$ is removed and whichever among the remaining intervals $[0, \xi_1]$ and $[\xi_1 + 1, x]$ has length that permits further partitioning (i.e., greater than 1) is partitioned in a recursive fashion. The process continues as follows—if the intervals $I_1, I_2, \ldots, I_k$ have already been chosen, the next randomly chosen interval will be kept only if it does not intersect any of the intervals $I_1, I_2, \ldots, I_k$. In this case this interval will be denoted by I_{k+1}. If it intersects any of the intervals $I_1, I_2, \ldots, I_k$, we ignore it and choose a new interval. The procedure is continued until none of the lengths of gaps generated by the intervals placed in $[0, x]$ is greater than 1.

A parameter of interest is the number of intervals packed in $[0, x]$ by this procedure. We denote its mean value by $M(x)$. We can now formulate a differential equation (with delay) for $M(x)$. By conditioning on the initial point of the first interval and invoking its uniform distribution we obtain:

$$M(x+1) = \frac{2}{x} \int_0^x M(y)dy + 1;$$

for brevity many obvious boundary conditions are omitted in this overview of the talk. We can obtain the limiting behavior of this mean value via the Laplace transform and the method of undetermined coefficients. It then follows from a Tauberian theorem that, as $x \to \infty$,

$$\begin{aligned} \frac{M(x)}{x} &\to \int_0^\infty \exp\left(-2\int_0^t \frac{1-e^{-u}}{u} du\right) dt \\ &\doteq 0.748. \end{aligned}$$

Another parameter of interest is $L(x)$, the minimal gap length generated by the random packing. Again by conditioning on the position of the leftmost end of the first interval packed [2], we obtain an integral equation

$$P\left(L(x+1) \geq h\right) = \frac{1}{x} \int_0^x P\left(L(y) \geq h\right) P\left(L(x-y) \geq h\right) \, dy.$$

A similar integral equation can be obtained for the maximal gap length.

2. A Unified Model for Kakutani's Interval Splitting and Rényi's Random Packing

Rényi's partitioning process has an interpretation as a parking problem: One can park a car of length 1, if there is a space of length at least 1.

In a more general setting, one may consider parking cars (or packing intervals) of length ℓ, for a space of length at least 1. The expected number of cars is then

$$M(x+\ell) = \frac{1}{x}\int_0^x (M(y) + M(x-y) + 1)\ dy.$$

Rényi's problem is the case $\ell = 1$, whereas Kakutani considers the case $\ell = 0$. For this variation Komaki and Itoh [3] find the limiting behavior

$$\lim_{x\to\infty} \frac{M(x)}{x} = \int_0^\infty (1 + (1-\ell))\, e^{-(1-\ell)t} \exp\left(-2\int_0^t \frac{1-e^{-\ell u}}{u}\, du\right)\, dt.$$

For the probability distribution of the minimum of gaps, giving $f(x)$ for $0 \le x \le 1$, you get the functional form

$$f(x+\ell, h) = \frac{1}{x}\int_0^x f(x-y,h) f(y,h)\, dy.$$

3. The Height of a Continuous-Type Binary Search Tree

Consider a random permutation of $1, 2, \ldots, n$, with all $n!$ permutations equiprobable. Insert the elements of the permutation in a binary search tree. Let $H(n)$ be the height of the tree so obtained. This height satisfies the equation

$$P\left(H(n+1) \le h\right) = \frac{1}{n}\sum_{m=0}^{n} P\left(H(n-m) \le h-1\right) P\left(H(m) \le h-1\right).$$

Note that the continuous analogue

$$P\left(H(x+1) \le h\right) = \frac{1}{x}\int_0^x P\left(H(x-y) \le h-1\right) P\left(H(y) \le h-1\right) dy$$

is of the type we obtained in the continuous models considered earlier. Robson [6], Flajolet and Odlyzko [1], Mahmoud and Pittel [4] have considered heights of similar discrete-type random trees.

4. Random Sequential Bisection Model

Applying the idea for the analysis of random packing, a continuous model is studied as a random sequential bisection model [7].

Among the possible 2^d nodes at the d-th level, $1 \le d$, of the associated tree the proportions of the expected number of the internal and external nodes are the Poisson-like expressions

$$\frac{1}{x}\sum_{k=d}^{\infty} \frac{(\log x)^k}{k!},$$

and

$$\frac{1}{x}\frac{(\log x)^{d-1}}{(d-1)!},$$

respectively.

Let $N_i(x,d)$ and $N_e(x,d)$ denote the numbers of the internal and external nodes at the d-th level respectively. Let $m_i(x,d)$ and $m_e(x,d)$ denote their expected values respectively. Then

$$m_i(x,d) = \frac{1}{x}\int_0^x (m_i(x-y,d-1) + m_i(y,d-1))\,dy.$$

From this we have

$$m_i(x,d) = \frac{2^d}{x}\sum_{k=d}^{\infty}\frac{(\log x)^k}{k!}, \qquad \text{for} \quad 1 \le x,$$

for $d = 0,1,2,\ldots$.

In any binary tree $N_i(x,d-1)$ internal nodes have $2N_i(x,d-1)$ son nodes, among which $N_i(x,d)$ are internal, therefore $N_e(x,d) = 2N_i(x,d-1) - N_i(x,d)$, for $d = 1,2,\ldots$. The expectation of this equality shows that for $d = 1,2,\ldots$, $m_e(x,d) = 2m_i(x,d-1) - m_i(x,d)$. As x and d increase to infinity in such a way that $d = c\log x$, we find

$$m_i(x,d) = \frac{1}{\sqrt{2\pi d}}e^{-d\gamma(c)} + O(1/d),$$

if $c > 1$. If $c < 1$,

$$m_i(x,d) = 2^d - \frac{1}{\sqrt{2\pi d}}e^{-d\gamma(c)} + O(1/d),$$

where $\gamma(c) = 1/c + \log(c/2) - 1$. It follows that

$$\lim_{x\to\infty} m_e(x,d) = \lim_{x\to\infty} m_i(x,d) = \begin{cases} 0, & \text{for } \hat{c} \le c < \infty; \\ \infty, & \text{for } 1 \le c < \hat{c}, \end{cases}$$

and, on the other hand,

$$\lim_{x\to\infty} m_e(x,d) = \lim_{x\to\infty}\{2^d - m_i(x,d)\} = \begin{cases} 0, & \text{for } 0 \le c < \check{c}; \\ \infty, & \text{for } \check{c} \le c < 1, \end{cases}$$

where $\hat{c} \doteq 4.311$ and $\check{c} \doteq 0.3734$ are the positive solutions of $\gamma(c) = 1/c + \log(c/2) - 1 = 0$.

Bibliography

[1] Flajolet (P.) and Odlyzko (A.). – The average height of binary trees and other simple trees. *Journal of Computer and System Sciences*, vol. 25, 1982, pp. 171–213.

[2] Itoh (Yoshiaki). – On the minimum of gaps generated by one-dimensional random packing. *Journal of Applied Probability*, vol. 17, n° 1, 1980, pp. 134–144.

[3] Komaki (Fumiyasu) and Itoh (Yoshiaki). – A unified model for Kakutani's interval splitting and Rényi's random packing. *Advances in Applied Probability*, vol. 24, n° 2, 1992, pp. 502–505.

[4] Mahmoud (Hosam) and Pittel (Boris). – On the most probable shape of a search tree grown from a random permutation. *SIAM Journal on Algebraic and Discrete Methods*, vol. 5, n° 1, 1984, pp. 69–81.

[5] Rényi (Alfréd). – On a one-dimensional problem concerning random space filling. *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, vol. 3, n° 1/2, 1958, pp. 109–127.

[6] Robson (J. M.). – The height of binary search trees. *The Australian Computer Journal*, vol. 11, n° 4, 1979, pp. 151–153.

[7] Sibuya (Masaaki) and Itoh (Yoshiaki). – Random sequential bisection and its associated binary tree. *Annals of the Institute of Statistical Mathematics*, vol. 39, n° 1, 1987, pp. 69–84.

On Tree-Growing Search Strategies

Hosam M. Mahmoud
Algorithms Project, INRIA Rocquencourt and The George Washington University

January 5, 1998

[summary by Michèle Soria]

Abstract

A search algorithm that adds a key to a sorted file can be represented by a *deterministic* tree whose external nodes are equally likely targets for insertion. The collection of algorithms that one uses throughout the stages of insertion sort is called a *search strategy.* Using the concept of "tree-growing" strategy, we demonstrate that most practical algorithm have a normal behavior. We present a sufficient condition for normality of tree-growing strategies. The sufficient condition specifies a relationship between the overall variance and the rate of growth in height of the sequence of trees that the search strategy "grows".

Insertion sort is a well-known on-line sorting algorithm: at each stage of the sorting, the elements obtained so far make up a sorted array; when reading a new element, the algorithm searches for its proper position in the array and inserts it. The searching may be done by any method (linear, binary, etc) and the methods may be different from one stage to another. At each stage, given a searching strategy, the positions of *probes* (positions for comparisons between the new element to be inserted and elements of the current array) is represented by a binary decision tree. The first probe is the root of the decision tree, the two positions of the second probe, at most one on each side of the first probe, become the children of the root and all internal nodes are constructed so forth. The leaves of the tree correspond to the places where new elements are to be inserted. The root-to-leaf paths of the tree thus represent the possible probe sequences of the searching algorithm.

1. Tree-growing and normal strategies

Let S_i denote the searching algorithm at stage i, with corresponding decision tree T_i; the collection of searching algorithms $\mathcal{S} = \{S_i\}_{i=1}^{\infty}$, or equivalently the collection of corresponding decision trees $\mathcal{T} = \{T_i\}_{i=1}^{\infty}$, will be called a *search strategy.* A search strategy is *tree-growing* if, for each positive integer i, the shape of T_{i+1} is obtained by replacing a leaf of T_i by an internal node (with two hanging leaves).

We analyse tree-growing search strategies under the assumption of uniform distribution of the leaves at each stage. Let the random variable C_n be the total number of times $\mathcal{S}$ compares a new element to a probe during the sorting of the first n elements. The class of *normal search strategies* is composed of the strategies for which C_n, once normalized, converges in distribution to the normal law, i.e.

$$\frac{C_n - \mathrm{E}[C_n]}{\sqrt{\mathrm{Var}[C_n]}} \to_{\mathcal{D}} \mathcal{N}(0,1).$$

The following lemma gives a sufficient condition for a tree-growing strategy to be normal. This condition relates the variance of C_n to the height of the decision trees of the search strategy. We denote by h_n the height of tree T_n, and by s_n^2 the variance of C_n.

Lemma 1. *If $h_n = o(s_n)$ then $\mathcal{S}$ is a normal strategy.*

Proof. C_n is the sum of n random variables $(X_i)_{i=1,\ldots,n}$, where X_i denotes the number of comparisons made by S_i. Since each insertion is performed independently of all others, we assume the X_i's to be independent random variables. The proof of Lemma 1 is a technical verification of Lindeberg's condition, which ensures normality:

$$\forall \epsilon > 0, \quad \lim_{n\to\infty} \frac{1}{s_n^2} \sum_{i=1}^{n-1} \int_{|X_i|>\epsilon s_n} X_i^2 \, dF_{X_i} = 0.$$

□

Practically for a given strategy, the difficulty lies in computing the variance of C_n, which is the sum of the variances of the X_i's. The most commonly used strategies, linear search and binary search, satisfy the condition of Lemma 1. When linear search is used at every stage, it is easy to show that C_n has average value asymptotic to $n^2/4$, and variance asymptotic to $n^3/36$, whereas h_n equals $n-1$. For binary repeated search strategies, one can easily show that h_n is asymptotic to $\log n$ and the average value of C_n is equivalent to $n \log_2 n$, but the computation of the variance is more intricate and finally leads to $s_n^2 = nA(n) + \mathcal{O}(\log n)$, where $A(n)$ is an oscillating function of bounded magnitude.

There exists tree-growing search strategies which are not normal. In [2], the authors exhibit a strategy that does not satisfy the condition of Lemma 1, and can be shown to be non normal by Feller-Lindeberg condition (see [1, vol. 2, §XV.6]). To ensure normality, some further conditions, which are presented in the next section, are required on the decision trees of the search strategy.

2. Normality of consistent strategies

This section identifies a subclass of tree-growing strategies, the consistent strategies, which are proved to be normal.

Let $\mathcal{T} = \{T_i\}_{i=1}^{\infty}$ be the collection of decision trees corresponding to a search strategy $\mathcal{S}$. For each T_i, we denote by T_{L_i} its left subtree (with size n_{L_i}) and T_{R_i} its right subtree (with size n_{R_i}). The size of the smaller subtree is noted by $g(i) = \min(n_{L_i}, n_{R_i})$. A search strategy $\mathcal{S}$ is said to be *self-similar* if for each decision tree, its left and right subtrees belong to $\mathcal{T}$, that is $T_{L_i} = T_{n_{L_i}}$ and $T_{R_i} = T_{n_{R_i}}$ (where trees are considered as equal if they have the same shape). And $\mathcal{S}$ is said to be *well-proportioned* if the proportion of nodes belonging to the smaller subtree approaches a limit as i tends to infinity, that is $\lim_{i\to\infty} g(i)/i$ exists. Finally we call *consistent* a strategy which is tree-growing, self-similar and well proportioned. Many usual strategies, such as linear search ($g(i)/i \to 0$) or binary search ($g(i)/i \to 1/2$), are consistent.

Theorem 1. *All consistent strategies are normal.*

The proof of this theorem relies on three properties of search strategies decision trees that ensure the sufficient condition for normality stated in Lemma 1.

Property 1. *For each positive integer i, the decision tree T_i has at least one external node on each unsaturated level.*

Property 2. *Let m_k be the number of decision trees with height k, the sequence $\{m_k\}_{k=1}^{\infty}$ is non-decreasing in k.*

For consistent strategies, these two properties result from self-similarity and tree-growing of the decision trees.

Property 3. *The variance of* C_n *satisfies* $s_n^2 = \Omega(n)$.

This property holds true for any decision tree, the intuition being that the tree with smallest variance is the complete binary tree (all levels saturated, except possibly the last one), which is the decision tree associated with binary search.

The proof of Theorem 1 considers two cases, $g(i)/i \to 1/2$ and $\lim g(i)/i \in [0, 1/2)$. In the first case the strategy is similar to binary search, $h_n = o(s_n)$ and the result follows from Property 3. In the second case Properties 1 and 2 are used to show that $h_n = o(s_n)$.

3. Relaxed conditions for normality

The sufficient condition for normality stated in Lemma 1 holds true for some families of tree-growing search strategies that are not consistent. For example, Fibonaccian search, where Fibonacci numbers are used to indicate the next probe, is not consistent since $\lim g(i)/i$ does not exist; but it can be shown to be normal with a proof similar to the one of Theorem 1, since $\liminf_{n\to\infty} g(n)/n$ as well as $\limsup_{n\to\infty} g(n)/n$ stand in $(0, 1/2)$.

More generally, one can exhibit different conditions on search strategies, that lead to normality by showing that the heights of the decision trees grow at a steady rate. For example

Proposition 1. *Any tree-growing search strategy* $\mathcal{S}$ *for which* $\liminf_{n\to\infty} g(n)/n$ *belongs to* $(0, 1/2)$ *is normal.*

Proposition 2. *If* $m_k = \Omega(k^{1+\epsilon})$ *for some* $\epsilon > 0$, *and* $\mathrm{Var}[X_n] = \Omega(1)$, *then the corresponding tree-growing search strategy is normal.*

Bibliography

[1] Feller (William). – *An introduction to probability theory and its applications.* – John Wiley & Sons Inc., New York, 1971, second edition, vol. II, xxiv+669p.

[2] Lent (Janice) and Mahmoud (Hosam M.). – On tree-growing search strategies. *The Annals of Applied Probability*, vol. 6, n° 4, 1996, pp. 1284–1302.

Complete Analysis of the Binary GCD Algorithm

Brigitte Vallée
Université de Caen

April 27, 1998

[summary by Cyril Banderier]

1. Introduction

The analysis of the *classical* Euclidean algorithm has been performed by Heilbronn [4] and Dixon [3], using different approaches. For a random pair of rational numbers, the average number of divisions is

$$D_n \sim \frac{12\log 2}{\pi^2}\log n.$$

Here, we will analyse the *binary* Euclidean algorithm, which uses only subtractions and right binary shifts. This "binary GCD algorithm" takes as input a pair of odd integers (u, v) from the set $\Omega = \{(u, v) \text{ odd}, 0 < u \le v\}$. Then the GCD is recursively defined by

$$\begin{cases} \gcd(u, v) = \gcd\left(\frac{v-u}{2^{\mathrm{Val}_2(v-u)}}, v\right) \\ \gcd(u, v) = \gcd(v, u) \end{cases}$$

where $\mathrm{Val}_2(n)$ is the greatest integer b such 2^b divides n, i.e., the dyadic valuation of n. The corresponding binary GCD algorithm is as follows:

```
while u ≠ v do
    while u < v do
        b := Val_2(v − u);
        v := (v − u)/2^b;
    end;
    exchange u and v;
end;
return u.
```

Example. If the input is $(u, v) := (7, 61)$ then $b := \mathrm{Val}_2(61 - 7) = 1$. Thus $v := 54/2^1 = 27$, and the algorithm continues because $u < v$. Now $b := \mathrm{Val}_2(27 - 7) = 2$. Thus $v := 20/2^2 = 5$. Now the algorithm restarts with $(u, v) := (5, 7)$. It leads to $v := (7 - 5)/2^1 = 1$ and therefore one restarts with $(u, v) := (1, 5)$ which leads to $v = 1 = u$ so the algorithm stops and returns u, namely 1 (as expected since 7 and 61 are coprime). One can write:

$$\frac{7}{61} = \cfrac{1}{3 + \cfrac{2^3}{1 + \cfrac{2^1}{1 + 2^2}}}.$$

In general, for each "inner while loop", one has

$$x_i = \frac{1}{a_i + 2^{k_i} x_{i+1}}$$

where $x_i := u/v$ (with (u,v) as in the beginning of the loop), $x_{i+1} := u/v$ (with (u,v) as after the exchange), where $a_i := 1 + 2^{b_1} + 2^{b_1+b_2} + \cdots + 2^{b_1+\cdots+b_{l-1}}$ and $k_i := b_1 + \cdots + b_{l-1} + b_l$ (the sum of all the b's obtained during the i-th inner while loop). The algorithm thus produces the following binary continued fraction expansion

$$\frac{u}{v} = \cfrac{1}{a_1 + \cfrac{2^{k_1}}{\cdots + \cfrac{2^{k_{r-1}}}{a_r + 2^{k_r}}}}.$$

Three interesting parameters are:

- r, the depth of the continued fraction or equivalently the number of outer loops performed;
- $\sum_{i=1}^{r} \nu(a_i)$, the number of subtractions (where $\nu(w)$ is the number of 1's in the binary expansion of the integer w);
- $\sum_{i=1}^{r} k_i$, number of rights shifts performed or equivalently inner loop executions.

Their average values on the set $\Omega_n = \{(u,v) \text{ odd}, 0 < u \le v \le n\}$ are respectively noted E_n, P_n and S_n. Note that E_n is also the average number of exchanges in the algorithm, and that P_n is the average number of operations that are necessary to obtain the expansion.

2. A Ruelle Operator for a Tauberian Theorem

In order to establish that these three parameters have averages that are asymptotic to $\log n$, we introduce the following Ruelle operator:

$$V_s[f](x) := \sum_{k \ge 1} \sum_{\substack{a \text{ odd} \\ 1 \le a \le 2^k}} \frac{1}{(a + 2^k x)^s} f\left(\frac{1}{a + 2^k x}\right).$$

The average E_n is easily expressed in term of V_s, with the help of the following definitions:

$$F(s) := (\mathrm{Id} - V_s)^{-1}[\mathrm{Id}](1), \quad G(s) := (\mathrm{Id} - V_s)^{-2} \circ V_s[\mathrm{Id}](1), \qquad \tilde{\zeta}(s) := \sum_{k \text{ odd}} \frac{1}{k^s} = \left(1 - \frac{1}{2^s}\right)\zeta(s).$$

Proposition 1. *E_n is a ratio of partial sums of the two Dirichlet series $\tilde{\zeta}(s)F(s)$ and $\tilde{\zeta}(s)G(s)$.*

Proof. Let $\Omega^{[l]}$ be the subset of Ω for which the algorithm performs exactly l exchanges. Then,

$$V_s^l[f](1) = \frac{1}{\tilde{\zeta}(s)} \sum_{(u,v) \in \Omega^{[l]}} \frac{1}{v^s} f\left(\frac{u}{v}\right).$$

Summing over all the possible heights ($l \ge 0$) yields:

$$(\mathrm{Id} - wV_s)^{-1}[f](1) = \sum_{l \ge 0} w^l V_s^l[f](1) = \frac{1}{\tilde{\zeta}(s)} \sum_{(u,v) \in \Omega^{[l]}} \frac{1}{v^s} f\left(\frac{u}{v}\right).$$

Differentiating with respect to w, and then choosing $f = 1$ and $w = 1$ yields

$$E_n = \frac{1}{|\Omega_n|} \sum_{l \ge 0} l |\Omega_n^{[l]}| = \frac{\sum_{l \ge 0} l \sum_{k \le n} v_k^{[l]}}{\sum_{l \ge 0} \sum_{k \le n} v_k^{[l]}}.$$

The proof is completed by observing that

$$F(s) = \frac{1}{\tilde{\zeta}(s)} \sum_{k\geq 1} \frac{1}{v^s} \sum_{l\geq 0} v_k^{[l]}, \qquad G(s) = \frac{1}{\tilde{\zeta}(s)} \sum_{k\geq 1} \frac{1}{v^s} \sum_{l\geq 0} l v_k^{[l]}.$$

□

The key is now to prove that the following theorem may be used:

Theorem 1 (Tauberian theorem). *If $F(s)$ is a Dirichlet series with non-negative coefficients that is convergent for $\Re(s) > \sigma > 0$ and if*

1. *F is analytic on the line $\Re(s) = \sigma$ except at $s = \sigma$;*
2. *$F(s) = \frac{A(s)}{(s-\sigma)^{\gamma+1}} + C(s)$ where A, C are analytic at σ (with $A(\sigma) \neq 0$);*

then one has, as $n \to \infty$,

$$\sum_{k\leq n} a_k = \frac{A(\sigma)}{\sigma\Gamma(\gamma+1)} n^\sigma \log^\gamma n(1+\epsilon(n)),$$

where $\epsilon(n) \to 0$.

Proof. See Delange [2]. □

Lemma 1. *The Tauberian theorem applies to F with $\sigma = 2$ and $\gamma = 0$.*

Proof. Indeed

$$F(s) := (\mathrm{Id} - V_s)^{-1}[\mathrm{Id}](1) = 1 + \frac{1}{2\tilde{\zeta}(s)} \sum_{v \text{ odd}} \frac{v-1}{v^s} = \frac{1}{2}\left(\frac{\tilde{\zeta}(s-1)}{\tilde{\zeta}(s)} + 1\right).$$

The last member of the equality clearly satisfies the conditions of the Tauberian theorem, and the same holds for $\tilde{\zeta} F$ with $\sigma = 2$ and $\gamma = 0$. □

Lemma 2. *The Tauberian theorem applies to G with $\sigma = 2$ and $\gamma = 1$.*

Proof. Here lies the complex part of Brigitte Vallée's proof. It is impossible to conclude as quickly as in lemma 1, indeed, this time we need to find an appropriate functional space on which V_s is a compact operator. A mixture of various functional analysis theorems (Fejer-Riesz' inequality, Gabriel's inequality, Krasnoselsky's theorem and other works by Shapiro and Grothendieck) show that it is the case on the Hardy space $H^2(D)$, where D is an open disk containing $]0,1]$. This leads to the fact that for $s > 3/2$, V_s has a unique positive dominant eigenvalue, equal to 1 when $s = 2$. In addition V_s has a spectral radius < 1 on $\Re(s) \geq 2, s \neq 2$. Thus $(\mathrm{Id} - V_s)^{-1}$ is regular on the domain D and condition 1 of the Tauberian theorem is fulfilled. Condition 2 is proved by means of perturbation theory applied to $V_s = P_s + N_s$ (P_s is the projection of V_s on the dominant eigensubspace), in a neighbourhood of $s = 2$. See [7] for a detailed proof. □

This implies the following fundamental result:

Theorem 2. *The average number of exchanges of the binary Euclidean algorithm on Ω_n is*

$$E_n \sim \frac{2}{\pi^2 f_2(1)} \log n,$$

where f_2 is the fixed point of the operator V_2 that is normalised by $\int_0^1 f_2(t)dt = 1$.

3. The Other Two Parameters

In order to study the other two parameters (total number of subtractions, total number of shifts) one still uses the Tauberian theorem but with a more intricate Ruelle operator, see Vallée [7]. This leads to the following two results.

Theorem 3. *The average number of total iterations is*

$$P_n \sim A \log n \qquad \textit{with} \quad A := \frac{2}{\pi^2 f_2(1)} \sum_{a \ odd} \frac{1}{2^{k_a}} F_2\left(\frac{1}{a}\right)$$

where f_2 is defined as above, $F_2(x) := \int_0^x f_2(t)dt$, $F_2(1) = 1$ (where k_a is the integer part of $\log_2 a$).

Theorem 4. *The average number of the sum of exponents of 2 used in the numerators of the binary continued fraction expansions, i.e., average total number of right shifts is*

$$S_n \sim \frac{2}{\pi^2 f_2(1)} \left(2 \sum_{a \ odd} \frac{1}{2^{k_a}} F_2\left(\frac{1}{a}\right)\right) \log n.$$

4. All Roads Lead to Rome

In Brent's paper [1], one can find a different approach which suggests that

$$P_n \sim \frac{1}{M} \log n \qquad \text{where} \quad M = \log 2 - \frac{1}{2} \int_0^1 \log(1-x) g_2(x) dx$$

and where g_2 is the fixed point (and normalised as f_2) of

$$B_2[f](x) := \sum_{b \geq 1} \left(\frac{1}{1+2^b x}\right)^2 f\left(\frac{1}{1+2^b x}\right) + \sum_{b \geq 1} \left(\frac{1}{x+2^b}\right)^2 f\left(\frac{x}{x+2^b}\right).$$

Unfortunately, this approach is based on a heuristic hypothesis (exercise 36, section 4.5.2, rated HM49 by Knuth in [5]). Brigitte Vallée explored this approach with a Brent operator B_s, without heuristic arguments but providing a spectral conjecture holds, this leads to the following result:

$$P_n \sim B \log n \qquad \text{where} \quad B := \frac{4}{\pi^2 g_2(1)}.$$

The miracle holds and, after numerical experiments, $A = \frac{1}{M} = B = 1.0185\ldots$. But nobody has proved these equalities. We can also note that a similar method was used by Brigitte Vallée and one of her students to analyse the Jacobi symbol algorithm [6]. Finally, the binary Euclidian algorithm is only a slight variation on one of the oldest known algorithms but there is still some unknown territories in its "complete" analysis!

Bibliography

[1] Brent (Richard P.). – Analysis of the binary Euclidean algorithm. In *Algorithms and complexity*, pp. 321–355. – Academic Press, New York, 1976. Proceedings of a Symposium held at Carnegie-Mellon University, 1976.

[2] Delange (Hubert). – Généralisation du théorème de Ikehara. *Annales Scientifiques de l'École Normale Supérieure*, vol. 71, n° 3, 1954, pp. 213–242.

[3] Dixon (John D.). – The number of steps in the Euclidean algorithm. *Journal of Number Theory*, vol. 2, 1970.

[4] Heilbronn (H.). – On the average length of a class of finite continued fractions. In *Number Theory and Analysis (Papers in Honor of Edmund Landau)*, pp. 87–96. – Plenum, New York, 1969.

[5] Knuth (Donald E.). – *The Art of Computer Programming*. – Addison-Wesley, 1997, third edition, vol. 2.

[6] Lemée (Charlie) and Vallée (Brigitte). – Analyse des algorithmes du symbole de Jacobi. *GREYC*, 1998.

[7] Vallée (Brigitte). – The complete analysis of the binary Euclidean algorithm. In *Proceedings ANTS'98*. – 1998.

A Probabilistic Algorithm for Molecular Clustering

Frédéric Cazals
Algorithm Project, Inria

December 15, 1997

[summary by Bruno Salvy]

In order to design a drug curing a given pathology, an approach which is commonly used consists in first selecting those that work best among molecules known to treat similar symptoms. In view of the number of known molecules, an exhaustive approach is often impossible. Instead, it is a common strategy to pick at random a number of molecules in a large database; and then concentrate on those that are chemically close to the ones that performed well. It is therefore important to be able to find those molecules in such a database. The aim of this work is to present a probabilistic algorithm for this task.

1. Molecules and similarity

The database is represented as an array of $n \simeq 10,000$ molecules, each molecule being characterized by the presence or absence of $d \simeq 1,500$ molecular fragments. Molecules are close when they differ by few molecular fragments. More precisely, one defines the *size* $s(m)$ of a molecule m as the number of its fragments and the *similarity* $\operatorname{sim}(m, M)$ between two molecules as the number of common fragments. Finally, two molecules m and M are called (α, β)-similar for $\alpha \in [0, 1]$ and $\beta \geq 1$ when

$$\operatorname{sim}(m, M) \geq \alpha \min(s(m), s(M)), \qquad \max(s(m), s(M)) \leq \beta \min(s(m), s(M)). \tag{1}$$

Note that this is not an equivalence relation. Other measures of similarity might also be of interest in practice.

2. Algorithm

The aim of this work is to find efficiently as many (α, β)-similar pairs in the database as possible. Obviously, an exhaustive search in $n(n-1)/2$ operations is possible, but expensive. The idea instead is to use a divide-and-conquer partitioning process. A fragment is selected at random and the database is partitioned into two subsets according to the presence or absence of this fragment. When such a subset has less than a fixed number K of elements an exhaustive search is performed; otherwise, the same process is applied recursively.

This technique finds a proportion τN of the number N of (α, β)-similar pairs. Heuristically, repeating the same process from scratch yields $\tau(1-\tau)^{i-1}N$ new pairs at the ith iteration. Thus a few iterations of this idea yield a very large proportion of N.

3. Implementation

The parameter K plays an important part in the efficiency of the algorithm. When K is small the search is faster but finds less pairs, so that the number of times it has to be repeated to obtain the same number of pairs can be larger than for higher values of K. The optimal value of K also depends on the efficiency of the different stages of the algorithm. Any improvement on the partitioning and exhaustive search part shift the optimum to larger values of K, while a good data-structure for checking whether a pair has already been found shifts it in the other direction. Here are implementation ideas that lead to an efficient program:

- The database is stored as an array of bits;
- the entries in the database are accessed by chunks (bytes or words), a constant array making it fast to count the number of bits equal to 1 in a chunk;
- computing the similarity between to molecules is then performed by bitwise and;
- the sizes of the molecules are computed once at the beginning;
- the partitioning is done like in Quicksort, on an array of pointers to the molecules;
- the set of pairs is stored as an array of binary search trees (a hash table would also do).

In practice, with this implementation and K around 150, then 4 or 5 runs of the partitioning yield more than 90% of the pairs in a matter of minutes. The exhaustive search would take several hours.

Conclusion

It would be nice to find the optimal value of K by a complexity analysis. However, the Bernoulli distribution for the bits in the database does not give a good model. It is necessary to take into account the fact that the database was arrived at by a historical process where many of the molecules are variants of each other.

Bibliography

[1] Cazals (Frédéric). – Effective nearest neighbours searching on the hyper-cube, with applications to molecular clustering. In *ACM Symposium on Computational Geometry.* pp. 222–230. – ACM Press, 1998. Also available at the url `http://www.inria.fr/prisme/personnel/cazals/xfc_research.html`.

Greedy Algorithms for the Shortest Common Superstring that are Asymptotically Optimal

Wojciech Szpankowski
Purdue University

March 9, 1998

Abstract

There has recently been a resurgence of interest in the shortest common superstring problem due to its important applications in molecular biology (e.g., recombination of DNA) and data compression. The problem is NP-hard, but it has been known for some time that greedy algorithms work well for this problem. More precisely, it was proved in a recent sequence of papers that in the worst case a greedy algorithm produces a superstring that is at most B times $(2 < B < 4)$ worse than optimal. We analyze the problem in a probabilistic framework, and consider the optimal total overlap and the overlap produced by various greedy algorithms. These turn out to be asymptotically equivalent. We show that with high probability the ratio of these overlaps tends to one as the number of strings goes to infinity. Our results hold under a condition that the lengths of all strings are not too short.

The results presented in this talk were obtained jointly with A. Frieze.

Two Not-That-Dull Functional Equations Arising in the Analysis of Algorithms

Wojciech Szpankowski
Purdue University

June 15, 1998

[summary by Philippe Jacquet]

1. Introduction

The talk addresses two functional equations arising in the analysis of algorithms, namely, in the performance evaluation of the generalized digital search trees and the asymmetric leader election algorithm. These functional equations deal with Poisson transforms of the general recurrence

$$x_{n+b} = a_n + cp^n x_n + u \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} (x_k + x_{n-k}),$$

where u and c are constants, a_n is a given sequence, and $b \geq 1$ is a parameter. Together with suitable initial condition, this recurrence describes both algorithms. It was extensively investigated either for $b = 1$ or $c = 0$. The speaker presents asymptotic expansions of x_n up to $O(1)$ term. Interestingly enough, for both algorithms there appears a constant that must be evaluated numerically from the original recurrence. Analytic techniques of (precise) analysis of algorithms are used to establish these conclusions. In particular, the author uses analytic poissonization/depoissonization, Mellin transform and singularity analysis.

The results presented in this talk were obtained jointly with S. Janson, G. Louchard and J. Tang.

2. The Generalized Digital Search Tree Algorithm

The basic Digital Search Tree (DST) is a tree-like data structure. Each node in the tree contains one data. We assume that all data are encoded over a common finite alphabet of size, say V. Each one of the edges pending from a node is in correspondence with one symbol of the alphabet. Consequently the branching degree of each node cannot exceed V.

The insertion of a new data X in the DST proceeds as follows:

1. Scan the first characters of data X in order to create a path in the DST with the symbol-edge correspondence;
2. use the character after the last scanned character of X to create a new edge in the DST pending from the last node visited, and create a new node to store X.

The basic DST can be used to implement Lempel-Ziv compression algorithms. The successive data inserted in the DST are phrases scanned on the text to be compressed. Therefore the original text is divided into phrases, and since each phrase points to another phrase via a symbol-edge in the DST structure, the compressed code replaces each phrase by a pair (pointer, symbol).

In the following we consider data generated from a Bernoulli binary source over a probability vector (p, q).

The average depth of insertion ED_n in the binary DST satisfies the following recursion valid for $n > 0$:

$$(n+1)ED_{n+1} = n + 1\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} (kED_k + (n-k)ED_{n-k}).$$

The probability generating function $D_n(u)$ of the depth of insertion satisfies:

$$(n+1)D_{n+1}(u) = 1 + u\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} (kD_k(u) + (n-k)D_{n-k}(u)).$$

The general case for data generated from Bernoulli source over V-ary alphabet (with probability vector $(p_1, \ldots, p_V)$):

$$(n+1)D_{n+1}(u) = 1 + u\sum_{k_1,\ldots,k_V} \binom{n}{k_1 \cdots k_V} p_1^{k_1} \cdots p_V^{k_V} (k_1 D_{k_1}(u) + \cdots + k_V D_{k_V}(u)).$$

The generalized DST assume a capacity b for each node of the DST, *i.e.,* each can store up to b data. The insertion algorithm is the same excepted that if the last visited node contains less than b data, then data X is stored in this node and no new node is created.

The functional recursion of p.g.f. $D_n(u)$ is now the following:

$$(n+b)D_{n+b}(u) = b + u\sum_{k} \binom{n}{k} p^k (1-p)^{n-k} (kD_k(u) + (n-k)D_{n-k}(u)).$$

The generating function of $D(z) = \sum_n ED_n \frac{z^n}{n!} e^{-z}$ satisfies the functional equation:

$$\sum_{i=0}^{b} \binom{b}{i} \frac{\partial^i}{\partial z^i} D(z) = z + D(pz) + D(qz).$$

The aim is to find an accurate asymptotic expansion of ED_n. Via depoissonization argument it is equivalent to find an asymptotic expansion of $D(n) = ED_n + O(\log n)$. To this end one makes use of the Mellin transform $d(s)\Gamma(s) = \int_0^\infty D(x)x^{s-1}dx$ satisfies:

$$\sum_{i=0}^{b} \binom{b}{i} (-1)^i d(s-i) = (p^{-s} + q^{-s}) d(s).$$

In other words $(1 - p^{-s} - q^{-s})d(s)$ is a linear combination of $d(s-i)$, i varying from 1 to b:

$$d(s) = \frac{1}{1 - p^{-s} - q^{-s}} \sum_{i=0}^{b} \binom{b}{i} (-1)^{i+1} d(s-i).$$

It comes that $d(s)$ is defined for $-b-1 < \Re(s) < -1$. The inverse Mellin transform expresses $D(z)$ via an integration formula:

$$D(z) = \frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} d(s)\Gamma(s)z^{-s}ds$$

for $c \in]-b-1, -1[$. The asymptotic expansion of $D(z)$ when $z \to \infty$ comes from the poles of $d(s)$ and $\Gamma(s)$ via application of the residue theorem. The poles of $d(s)$ are the roots of $1 - p^{-s} - q^{-s}$, and the same roots repeat when translated on the right by integer values because of the identities between $d(s)$ and $d(s-i)$. The main singularity is at $s = -1$ which doubles the pole of $\Gamma(s)$ and will contribute in a $z \log z$ term in $D(z)$'s expansion.

Application of the residue theorem finally gives:

$$D(z) = \frac{1}{h} z \log z + \left(\frac{h_2 - h}{h^2} + \gamma - \frac{f'(-1)}{h} \right) z + z P_1(\log z) + O(\log z),$$

with $h = -p \log p - q \log q$ and $h_2 = p \log^2 p + q \log^2 q$. Quantity $P_1(z)$ is periodic with small amplitude when $\log p / \log q$ is rational (when the roots of $1 - p^{-s} - q^{-s}$ are regularly spaced on the vertical axis $\Re(s) = -1$), and $o(z)$ otherwise. Quantity $f'(-1)$ denotes the derivative of $\sum_{i=1}^{b} \binom{b}{i} (-1)^{i+1} d(s-i)$ at $s = -1$.

The question remains on how to compute a numerical evaluation of constant $f'(-1)$. To this end one computes a numerically tractable expression of $d(s)$ via the Mellin transform:

$$d(s) = \frac{1}{\Gamma(s)} \int_0^\infty z^{s-1} \sum_n ED_n \frac{z^n}{n!} e^{-z} dz = \sum_n \frac{ED_n}{n!} \frac{\Gamma(s+n)}{\Gamma(s)}.$$

Therefore

$$d(s) = \sum_n \frac{ED_n}{n!} s(s+1) \cdots (s+n-1).$$

Using this formula and truncating it up to certain rank N gives a numerical evaluation of $f'(-1)$. Unfortunately the error term can be proven to be of order $O(\log N/N)$. There are probably better estimates which converge geometrically.

3. **Leader Election**

We don't give details on the problem of leader election. Via successive Bernoulli splits over a group of n people, one randomly selects a leader. We denote X_n the average number of steps needed to achieve this election over a population of n people. When the Bernoulli splits are all done over the same probability vector (p, q), one obtains the recursion for $n \geq 2$:

$$X_n = 1 + q^n X_n + \sum_k \binom{n}{k} p^k q^{n-k} X_k$$

which translates into a functional equation for the generating function $L(z) = \sum_n X_n e^{-z} z^n / n!$:

$$L(z) = 1 - (1+z)e^{-z} + L(pz) + L(qz)e^{-pz}.$$

Using again the Mellin approach, $L^*(s)$ the Mellin transform of $L(z)$ satisfies the identity:

$$L^*(s) = \frac{f^*(s) - (1+s)\Gamma(s)}{1 - p^{-s}},$$

where $f^*(s)$ is the Mellin transform of $f(z) = L(qz)e^{-pz}$. Since $L(0) = 0$, $L^*(s)$ is defined for $-1 < \Re(s) < 0$, and thanks to the exponential decrease of $f(z)$, $f^*(s)$ is defined for all $\Re(s) > -1$. There is a sequence of poles on the axis $\Re(s) = 0$ regularly spaced: $s_k = 2i\pi k / \log p$, for k integer. The poles are simple for $k \neq 0$, the pole is double at $s = 0$ due to the contribution of the pole of $\Gamma(s)$. The double pole contributes in a $-\log z / \log p$ term in the residue theorem applied to reverse Mellin transform. The other poles contribute to a periodic function which depends on $f^{(s)}$ at $s = s_k$.

In summary for any $M > 0$:

$$L(z) = -\frac{\log z}{\log p} + \frac{1}{2} + \frac{1 - \gamma - f^*(0)}{\log p} + P_2(\log z) + O\left(\frac{1}{z^M}\right).$$

$P_2(x)$ is a periodic function of period $\log p$ and small amplitude. Using again depoissonization theorems one gets $X_n = L(n) + O(1/n)$.

As with the generalized DST, the numerical evaluation of constant $f^*(0)$ remains. In this case we are luckier than with DST since $f^*(0) = \sum_n X_n q^n / n$ which converges exponentially.

Part 4

Probabilistic Methods

Birth-Death Processes, Lattice Path Combinatorics, Continued Fractions, and Orthogonal Polynomials

Fabrice Guillemin
France Telecom, CNET, Lannuon, Breizh

February 2, 1998

[summary by Philippe Flajolet and Fabrice Guillemin]

Abstract

Classic works of Karlin-McGregor and Jones-Magnus have established a fully general correspondence between birth-death processes and continued fractions of the Stieltjes-Jacobi type together with their associated orthogonal polynomials. This fundamental correspondence can be revisited in the light of the otherwise known combinatorial correspondence between weighted lattice paths and continued fractions. For birth-death processes, this approach separates clearly the formal apparatus from the analytic-probabilistic machinery and neatly delineates those parameters that are amenable to a treatment by means of continued fractions and orthogonal polynomials.

1. Birth-Death Processes

Consider a particle initially in state 0 that, at any given time, may change to another state 1 (where it stays), with rate λ. This means that the probability of a state change in an interval of time of length dt is λdt. Then, the probability $p_0(t)$ that the particle is still in state 0 at time t satisfies

$$p_0(t + dt) - p_0(t) = -\lambda p_0(t)dt$$

or $p_0'(t) = -\lambda p_0(t)$, whose solution is an exponential distribution,

$$p_0(t) = e^{-\lambda t}.$$

Similarly, a particle initially in state 0 that may change either to state 1 with rate λ or to state -1 with rate μ will satisfy ($p_j(t)$ is the probability of being in state j at time t)

$$p_0(t) = e^{-(\lambda+\mu)t}, \qquad p_1(t) = \frac{\lambda}{\lambda+\mu}(1 - e^{-(\lambda+\mu)t}), \qquad p_{-1}(t) = \frac{\mu}{\lambda+\mu}(1 - e^{-(\lambda+\mu)t}).$$

The interpretation is obvious: the particle stays in state 0 for a random amount of time with an exponential distribution of rate $\lambda + \mu$ and then changes to states $-1, +1$ with probabilities equal to to $\lambda/(\lambda + \mu)$ and $\mu(\lambda + \mu)$.

In a general *birth-death* process a particle can be in any state in $\{0, 1, 2, \dots\}$ and when in state j, it can only change to state $j + 1$ at rate λ_j or to state $j - 1$ at rate μ_j. By analogy with the model of an evolving population (whose size is represented by the state), the λ_j are called birth rates and the μ_j death rates. The general problem is to understand the evolution of a process given values (or properties) of its birth and death rates; see [12, Ch. 4] for an excellent introduction.

Let $p_n(t)$ be the probability of being in state n at time t. An essential rôle is played by the coefficients

$$\pi_n = \frac{\lambda_0 \lambda_1 \cdots \lambda_{n-1}}{\mu_1 \mu_2 \cdots \mu_n}.$$

Indeed, a classical result asserts that the process is ergodic (the expected time to return from each state to itself is finite) if and only if

$$\sum_{n \geq 1} \pi_n < \infty, \qquad \sum_{n \geq 0} \frac{1}{\lambda_n \pi_n} = +\infty.$$

(The first condition ensures the existence of an invariant measure for the embedded discrete-time Markov chain; the second one guarantees that, in the continuous-time process, the particle is not absorbed at infinity in finite time.) In that case, one has

$$p_n := \lim_{t \to \infty} p_n(t) = \frac{\pi_n}{\sum_{n \geq 1} \pi_n},$$

where these quantities represent the long run probability of being in state n.

More puzzling is the nonstationary behaviour of the process that is described by the *infinite-dimensional* differential system

$$p_j'(t) = \lambda_{j-1} p_{j-1}(t) - (\lambda_j + \mu_j) p_j(t) + \mu_{j+1} p_{j+1}(t), \qquad p_j(0) = \delta_{j,0}. \tag{1}$$

Although finite-dimensional versions are "easy" and reduce to combinations of exponentials, it is precisely the infinite-dimensional character of the system that renders its analysis interesting.

In a series of important papers, Karlin and McGregor [10, 11] have developed a general connection between the fundamental system (1) and an associated family of orthogonal polynomials. Later, Jones and Magnus constructed a direct continued fraction representation; see [8, 9].

This summary is an account of Guillemin's lecture (see [5, 6]), as well as of later developments. The point of view that is adopted here consists in relating the combinatorial theory of lattice paths to birth-death processes in the following way: (i) trajectories of birth-death processes are precisely lattice paths; (ii) lattice paths have generating functions expressed as continued fractions; (iii) the Laplace transform expresses the main parameters of birth-death processes as weighted lattice paths to which the combinatorial theory applies.

2. Lattice Paths and Continued Fractions

It is known that the formal theory of continued fraction expansions for power series is identical to the combinatorial theory of weighted lattice paths; see [1, 2, 4]. Define a path $v = (U_0, U_1, \ldots, U_n)$ to be a sequence of points in the lattice $\mathbb{N} \times \mathbb{N}$ such that if $U_j = (x_j, y_j)$, then $x_j = j$ and $|y_{j+1} - y_j| = 1$. If successive points are connected by edges, then an edge can only be an *ascent* ($\underline{a}$: $y_{j+1} - y_j = +1$), a *descent* ($\underline{b}$: $y_{j+1} - y_j = -1$), or a *level step* ($\underline{c}$: $y_{j+1} - y_j = 0$). Thus a path is always nonnegative and by a horizontal translation, one may always assume that $x_0 = 0$. A path can be encoded by a word with a, b, c representing the three types of steps. What we call the *standard encoding* is such a word in which each step a, b, c is subscripted by the value of the y-coordinate of its associated point. For instance,

$$w = a_0 a_1 a_2 b_3 c_2 c_2 a_2 b_3 b_2 b_1 a_0 c_1$$

encodes a path that connects the source $U_0 = (0,0)$ to the destination $U_{12} = (12, 1)$. We freely identify a path v defined as a sequence of points, its word encoding w, and the corresponding monomial.

We consider various geometric conditions that may be imposed on paths: $\mathcal{H}_{k,l}$ is the collection of all paths that connect a source at altitude k to a destination at altitude l, $\mathcal{H}^{[\le h]}$ denotes paths of height (maximal altitude) at most h, etc.

Theorem 1. *The collection $\mathcal{H}_{0,0}$ of all paths has generating function*

$$H_{0,0} = \cfrac{1}{1 - c_0 - \cfrac{a_0 b_1}{1 - c_1 - \cfrac{a_1 b_2}{1 - c_2 - \cfrac{a_2 b_3}{\ddots}}}}$$

Proof. It suffices to observe that $(1-f)^{-1} = 1+f+f^2+\cdots$ generates symbolically all the sequences with components f. For instance, in $\mathcal{H}_{0,0}$, the expressions

$$(2) \qquad \frac{1}{1-c_0}, \qquad \frac{1}{1-c_0-a_0b_1}, \qquad \cfrac{1}{1-c_0-\cfrac{a_0b_1}{1-c_1}}$$

generate successively paths composed from c_0 level steps only, paths of height at most 1 without c_1 steps, all paths of height at most 1. The complete continued fraction representation is easily built by stages in a similar fashion. $\square$

In particular, the collection of all paths from level 0 to level 0 with height at most h is

$$(3) \qquad H_{0,0}^{[<h]} = \frac{P_h}{Q_h},$$

a rational fraction, whose numerators and denominators, P_h, Q_h, each satisfy the recurrence

$$y_{h+1} = (1-c_h)y_h - a_{h-1}b_h y_{h-1},$$

with $Q_{-1} = P_0 = 0$, $Q_0 = P_1 = 1$. (Linear fractional transformations are 2×2 matrices in disguise!)

Well-known path decompositions, like those based on first or last time at which levels are reached, can then be used provided they are combinatorially "unambiguous". This and simple manipulations on linear fractional transformations give access to many geometric constraints in addition to (2) and (3). We cite here some representative identities from [1, 2],

$$(4) \qquad H_{0,h-1}^{[<h]} = \frac{a_0a_1\cdots a_{h-1}}{Q_h}, \qquad H_{0,k} = \frac{1}{b_1b_2\cdots b_k}\left(Q_kH_{0,0} - P_k\right),$$

$$(5) \qquad H_{k,l} = \frac{Q_k}{a_0\cdots a_{k-1}b_1\cdots b_l}\left(Q_lH_{0,0} - P_l\right),$$

where the latter holds provided $k \le l$.

The forms (2), (3) (4), (5) can be converted into *bona fide* counting generating functions of paths weighted multiplicatively by means of the *combinatorial morphism*,

$$\chi(a_k) = \alpha_k z, \qquad \chi(b_k) = \beta_k z, \qquad \chi(c_k) = \gamma_k z.$$

In that case, the continued fraction (2) becomes the general fraction of the J-type (for Jacobi); see [7, 9, 13].

3. The Connection

We illustrate here in its simplest form the many-faceted connection between birth-death processes and continued fractions. It was apparently first stated explicitly by Jones and Magnus but it is implicit in earlier works of Karlin and McGregor. The connection goes through the probabilities $p_{i,j}(t)$ of being in state j at time t starting from state i and the Laplace transforms,

$$P_{i,j}(s) = \int_0^\infty p_{i,j}(t) e^{-st}\, dt.$$

Theorem 2. *The Laplace transform of the probability of return to the origin satisfies*

$$P_{0,0}(s) = \cfrac{1}{\lambda_0 + s - \cfrac{\lambda_0\mu_1}{\lambda_1 + \mu_1 + s - \cfrac{\lambda_1\mu_2}{\ddots}}}.$$

We offer here two proofs. A third proof that is based on "uniformization of time" can also be given but is omitted in this note.

Proof 1. Take the Laplace transform of the fundamental system (1) (so that $p_j(t) = p_{0,j}(t)$) and use the induced relations on the ratios $P_{0,r}/P_{0,r+1}$. This proof is the most direct but the least illuminating from a structural standpoint. In particular, this proof does not provide an immediate grasp on the question of deciding which parameters are amenable to continued fraction representations. □

Proof 2. Examine the times at which the (continuous time) birth-death process $\{\Lambda_t\}$ changes states. This defines an embedded (discrete time) Markov chain $\{Y_n\}$. Then the set of trajectories of the chain $\{Y_n\}$ is exactly the family of lattice paths of Section 2. The method consists in splitting the probabilities by conditioning according to all legal trajectories.

- The first observation is that, given a lattice path $w = w_1 w_2 \cdots w_n$, the probability $p_{0,0}(t \mid w)$ of being back to 0 at time t having followed the path w is

  $$\Pr\{\Lambda_t = 0 \mid w\} = \Pr\left\{S_{q_1} + S_{q_2} + \cdots + S_{q_n} \le t,\ S_{q_1} + S_{q_2} + \cdots + S_{q_n} + S_{q_{n+1}} > t\right\},$$

  where S_{q_j} is the random variable that represents the sojourn time at the state q_j determined by $w_1 \cdots w_j$, while the right-hand side involves q_{n+1} that ranges over all legal "continuations" of w (in the case of $\mathcal{H}_{0,0}$, one has $w_{n+1} = a_0$ and $q_{n+1} = 0$). As seen already, the sojourn time at some state e is exponential with parameter $(\lambda_e + \mu_e)$ so that its Laplace transform is $(\lambda_e + \mu_e)/(s + \mu_e + \lambda_e)$.
- The second observation is that the probability of a path in the embedded chain is the product of the individual transition probabilities, namely $\lambda_j/(\lambda_j + \mu_j)$ and $\mu_j/(\lambda_j + \mu_j)$.

The different sojourn times are independent by the nature of the process (the strong Markov property satisfied by $\{\Lambda_t\}$). Also, sums of independent random variables correspond to products of Laplace transforms. Thus, the Laplace transform of the probability in the continuous model of following a path w has a product form; for instance, to $w = a_0 a_1 b_2 a_1$, there corresponds the transform

$$\left(\frac{\lambda_0}{\lambda_0 + \mu_0}\frac{\lambda_1}{\lambda_1 + \mu_1}\frac{\mu_2}{\lambda_2 + \mu_2}\frac{\lambda_1}{\lambda_1 + \mu_1}\right) \cdot \left(\frac{\lambda_0 + \mu_0}{s + \lambda_0 + \mu_0}\frac{\lambda_1 + \mu_1}{s + \lambda_1 + \mu_1}\frac{\lambda_2 + \mu_2}{s + \lambda_2 + \mu_2}\frac{\lambda_1 + \mu_1}{s + \lambda_1 + \mu_1}\right).$$

Thus, the Laplace transform $P_{0,0}(s)$ is, apart from a fudge factor of $1/(s+\lambda_0)$, a sum over all paths lattice from zero to zero weighted multiplicatively by the *probabilistic morphism*,

$$\chi'(a_j) = \frac{\lambda_j}{s+\lambda_j+\mu_j}, \qquad \chi'(b_j) = \frac{\mu_j}{s+\lambda_j+\mu_j}, \tag{6}$$

with $\chi'(c_j) = 0$. In other words, one has $P_{0,0}(s) = \chi'(H_{0,0})\frac{1}{s+\lambda_0}$, and the statement follows. □

The same method applies to the computation of transition probabilities, the analysis of maximum height, and so on. For instance, the probability of reaching state k has

$$P_{0,k}(s) = \frac{1}{\mu_1\mu_2\cdots\mu_k}\left(A_k(s)P_{0,0}(s) - B_k(s)\right),$$

where A_k/B_k is the kth convergent of the continued fraction that represents $P_{0,0}$, so that A_k, B_k are simple variants of $\chi'(P_k), \chi'(Q_k)$.

Orthogonality. In the case of paths, the reciprocals of the Q_h polynomials, $\overline{Q}_h(z) = z^h\chi(Q)(z^{-1})$ are *formally orthogonal* with respect to a measure defined its moments,

$$\mathcal{L}[z^n] \equiv \int z^n\, d\mu(z) = H_{0,0,n}. \tag{7}$$

Formal aspects of paths and orthogonality are detailed in Godsil's book [3].

A similar orthogonality property then holds for the probabilistic counterparts A_h, B_h of the P_k, Q_k polynomials. This provides alternative expressions of various probabilistic quantities in terms of scalar products involving the measure μ of (7). One can rederive in this way, via the combinatorial theory, a number of formulæ originally discovered by Karlin and McGregor. For instance, one has

$$p_{m,n}(t) = \pi_n \int_0^\infty e^{-tx}\theta_m(x)\theta_n(x)\, d\mu(x),$$

where the θ_k polynomials (closely related to the B_k and Q_k) satisfy the recurrence $\lambda_n\theta_{n+1} + (x - \lambda_n - \mu_n)\theta_n + \mu_n\theta_{n-1} = 0$.

4. So What?

The original motivation for the talk comes from the need to elucidate the behaviour of certain *queueing systems* in the context of telecommunication applications. For instance, the single server queue ($M/M/1$) is modelled by $\lambda_j = \rho$, $\mu_j = 1$, while the infinite server queue ($M/M/\infty$) corresponds to $\lambda_j = \rho$, $\mu_j = j$. (Models of population growth lead to considering different types of weights, like $\lambda_j = (j+1)\rho$, $\mu_j = j$.) More specifically, the problem is to quantify parameters of some simple statistical multiplexing scheme that describe the quality of service on an ATM link. The relevant model is that of the $M/M/\infty$ queue and parameters are to be analysed, like the duration θ of an excursion above some level c, the volume V of lost information, or the number of bursts C in a busy period.

Each parameter leads to a specific continued fraction representation. By Theorem 2, the basic continued fraction of the $M/M/\infty$ process is

$$\cfrac{1}{s+\rho-\cfrac{1\rho}{s+1+\rho-\cfrac{2\rho}{\ddots}}}.$$

This is recognizable as an instance of Gauß's continued fraction associated to a quotient of *contiguous hypergeometric functions*. The numerator and denominator polynomials are the Poisson-Charlier polynomials that are orthogonal with respect to the Poisson measure.

The quantity V (area) leads to challenging asymptotics questions both for the $M/M/\infty$ queue and for the $M/M/1$ queue. A simple modification of the basic techniques of this note shows that the bivariate Laplace transform with (s,u) "marking" (t,V) is obtained by the modified morphism,

$$\chi''(a_j) = \frac{\lambda_j}{s + ju + \lambda_j + \mu_j}, \qquad \chi''(b_j) = \frac{\mu_j}{s + ju + \lambda_j + \mu_j}.$$

In the case of area under the $M/M/1$ queue, quotients of continuous Bessel functions make an appearance. Stripped of its probabilistic context, the corresponding problem of tail estimation then admits a purely analytic formulation:

Problem. *Let $A(x)$ be a function whose Laplace transform is*

$$\widetilde{A}(s) = \frac{1}{\sqrt{s}} \frac{J_{\nu(s)+1}\left(\frac{2\sqrt{\rho}}{s}\right)}{J_{\nu(s)}\left(\frac{2\sqrt{\rho}}{s}\right)}, \qquad \nu(s) = (1+\rho)/s,$$

with J_ν a Bessel function, and $\rho > 0$ a parameter. Show that, for some constants c_1, c_2, one has

$$\int_x^\infty A(y)\,dy \sim c_1 x^{-1/4} e^{-c_2\sqrt{x}}, \qquad (x \to +\infty).$$

Under plausible analytic or probabilistic conjectures, precise (and useful!) quantitative conclusions can be drawn. See the papers by Guillemin and Pinchon [5, 6] for full developments.

Bibliography

[1] Flajolet (P.). – Combinatorial aspects of continued fractions. *Discrete Mathematics*, vol. 32, 1980, pp. 125–161.

[2] Flajolet (P.), Françon (J.), and Vuillemin (J.). – Sequence of operations analysis for dynamic data structures. *Journal of Algorithms*, vol. 1, 1980, pp. 111–141.

[3] Godsil (C. D.). – *Algebraic Combinatorics*. – Chapman and Hall, 1993.

[4] Goulden (Ian P.) and Jackson (David M.). – *Combinatorial Enumeration*. – John Wiley, New York, 1983.

[5] Guillemin (Fabrice) and Pinchon (Didier). – Continued fraction analysis of the duration of an excursion in an $M/M/\infty$ system. *Journal of Applied Probability*, vol. 35, n° 1, 1998, pp. 165–183.

[6] Guillemin (Fabrice) and Pinchon (Didier). – Excursions of birth and death processes, orthogonal polynomials, and continued fractions. – Preprint, 1998. To appear in *Journal of Applied Probability*. 21 pages.

[7] Henrici (Peter). – *Applied and Computational Complex Analysis*. – John Wiley, New York, 1977. 3 volumes.

[8] Jones (William B.) and Magnus (Arne). – Application of Stieltjes fractions to birth-death processes. In Saff (E. B.) and Varga (Richard S.) (editors), *Padé and rational approximation*. pp. 173–179. – New York, 1977. Proceedings of an International Symposium held at the University of South Florida, Tampa, Fla., December 15-17, 1976.

[9] Jones (William B.) and Thron (W. J.). – *Continued Fractions: Analytic Theory and Applications*. – Addison–Wesley, 1990, *Encyclopedia of Mathematics and its Applications*, vol. 11.

[10] Karlin (S.) and McGregor (J. L.). – The differential equations of birth-and-death processes, and the Stieltjes moment problem. *Transactions of the American Mathematical Society*, vol. 85, 1957, pp. 489–546.

[11] Karlin (Samuel) and McGregor (James). – The classification of birth and death processes. *Transactions of the American Mathematical Society*, vol. 86, 1957, pp. 366–400.

[12] Karlin (Samuel) and Taylor (Howard). – *A First Course in Stochastic Processes*. – Academic Press, 1975, second edition.

[13] Perron (Oskar). – *Die Lehre von der Kettenbrüchen*. – Teubner, 1954, vol. 2.

Trees and Branching Processes

Brigitte Chauvin
Université de Versailles-St Quentin

January 5, 1998

[summary by Philippe Robert]

Abstract

A random tree is defined as an elementary event ω of a probability space $(\Omega, \mathcal{F}, P)$. The probability P depends on the random model of trees which is analyzed. The main results concerning the Galton-Watson processes are recalled. If for $n \in \mathbb{N}$, Z_n is the number of individuals of the N-th generation and m the average number of children generated by an individual, it is shown that the martingale (Z_n/m^n) plays an important role in the analysis of such processes.

The Catalan trees are seen as a particular case of Galton-Watson process. The height of a Catalan tree with n nodes is of the order $C\sqrt{n}$ (Flajolet-Odlyzko) and the number of external leaves has a limiting distribution (Kesten-Pittel).

The binary search trees are related to a branching random walk, hence to marked trees. The analysis of their height involves large deviations results for this random walk; for a binary search tree with n nodes, it is of the order $C \log n$ (Devroye, Biggins).

1. Probabilistic Model

Definition 1. If $Q = (q_i)$ is a probability distribution on $\mathbb{N}$ ($q_i \geq 0$ for $i \geq 0$ and $\sum_{i=0}^{+\infty} q_i = 1$), a Galton-Watson process with generating distribution Q is a sequence of random variables (Z_n) defined by

$$Z_0 = 1, \qquad Z_{n+1} = \sum_{i=1}^{Z_i} G_{in},$$

where the (G_{ij}), $i, j \in \mathbb{N}$ are independent identically distributed random variables with distribution Q.

For $n \in \mathbb{N}$, Z_n is the number of individuals at the n-th generation. By convention the generation 0 contains only the ancestor ($Z_0 = 1$) and the i-th individual of the n-th generation has G_{in} children.

The underlying tree structure of such a process is obvious. It is nevertheless convenient to reformulate these processes within the framework of trees [9]. A tree ω is a subset of

$$U = \{\emptyset\} \cup \bigcup_{n \geq 1} \mathbb{N}^{*n}$$

with the following properties:

1. $\emptyset \in \omega$, i.e. the ancestor is in the tree;
2. If $u \cdot v \in \omega$, then $u \in \omega$, ($u \cdot v$ denotes the concatenation of strings);

FIGURE 1. Trees as subsets of U

3. If $u \in \omega$ then there exists $N_u(\omega) \in \mathbb{N}$ such that $u \cdot j \in \omega$ if and only if $1 \leq j \leq N_u(\omega)$. The variable $N_u(\omega)$ is the number of children of the node u. By convention $N_\emptyset = N$.

With this notation, the tree of the Figure 1 can be represented as

$$\omega = \{\emptyset, 1, 2, 3, 21, 211, 2111, 2112, 22, 221, 31, 311\}\,.$$

If $u \in U$, $|u|$ will denote the length of the string u, in particular

$$H(\omega) = \sup\{|u|, u \in \omega\},$$

is the height of the tree ω and if $z_n(\omega) = \{u \in \omega, |u| = n\}$, then $Z_n(\omega) = \mathrm{Card}(z_n(\omega))$ is the number of individuals of generation n. Finally, if $u \in \omega$, $T_u(\omega)$ will denote the subtree containing the elements of ω whose prefix is u. In the example of Figure 1,

$$T_{21}(\omega) = \{\emptyset, 1, 11, 12\}\,.$$

Definition 2. A Galton-Watson tree with generating distribution Q is a probability distribution P on the set of trees such that

1. $P(N = k) = q_k$;
2. Conditionally on the event $\{N(\omega) = n\}$, the subtrees $T_1(\omega), T_2(\omega), \dots, T_n(\omega)$ are independent with distribution P.

The first condition says that the number of children of the ancestor has distribution Q. The other condition gives an homogeneity property (the subtree $T_i(\omega)$ and ω have the same distribution for $i \leq n$). The independence of the behavior of the individuals, corresponds to the independence of the G_{i1}, $i = 1, \dots, n$ in our first definition. From now on, (Z_n) denotes a Galton-Watson process associated to Q.

2. Limiting Behavior of Galton-Watson Trees

Notice that if $q_0 = P(N = 0) > 0$, then it is possible that an individual does not generate children at all. Consequently, a complete extinction of the family of the ancestor is also possible. The following proposition describes this phenomenon.

Proposition 1. *If $m = E(G_{11}) = \sum_{i=0}^{+\infty} iq_i$ is the average number of children per individual, then*

$$P\left(\sum_{n=0}^{+\infty} Z_n < +\infty\right) = q,$$

where q is the smallest solution $s \in [0,1]$ of the equation $\sum_{i=0}^{+\infty} q_i s^i = s$. If $m \leq 1$, the Galton-Watson becomes extinct with probability 1, that is, $q = 1$; and if $m > 1$ then $q < 1$.

We can now state a classical theorem for Galton-Watson processes.

Theorem 1. *The process $(W_n) = (Z_n/m^n)$ is a positive martingale with expected value 1, furthermore the sequence (W_n) is almost surely converging to a finite random variable W.*

Refinements. The following theorems give more insight on the behavior on the sequence (Z_n). There are three theorems, one for each of the three cases $m > 1$, $m = 1$ and $m < 1$.

Theorem 2 (Kesten-Stigum [7]). *If $m > 1$, the following conditions are equivalent*

1. *(Z_n/m^n) converge to W in $L_1(P)$;*
2. *$E(N \log N) = \sum_{i=2}^{+\infty} k \log(k) q_k < +\infty$;*
3. *$P(W = 0) = q$.*

The above result is mainly a strengthening of Theorem 1. It can be proved in an elegant way [8] with the formalism we described in the introduction. This proof uses a change of probability and the martingale (W_n).

The following theorem is more informative from a qualitative point of view. It says that in the critical case $(m = 1)$ the variable Z_n grows linearly conditionally on $\{Z_n > 0\}$ (remember that in this case, almost surely $Z_n = 0$ for n large enough).

Theorem 3. *If $m = 1$ and $\sigma = \mathrm{Var}(N) < +\infty$, conditionally on the event $\{Z_n > 0\}$, the random variable Z_n/n converges in distribution to an exponential distribution with parameter $\sigma/2$.*

The same conditioning procedure as in the critical case does not lead to the same phenomenon in the sub-critical case $(m < 1)$. Basically the conditioned variable Z_n stays bounded.

Theorem 4 (Yaglom [10]). *If $0 < m < 1$, then conditionally on the event $\{Z_n > 0\}$, the random variable converges in distribution to a finite random variable.*

3. Catalan Trees, Dyck Paths and Galton-Watson Processes

Definition 3.
1. A Catalan tree with n nodes is a random tree for the uniform distribution, that is, the probability of a tree ω is $P(\omega) = (n+1)/\binom{2n}{n}$, if $\mathrm{Card}(\omega) = n$ and 0 otherwise.
2. A Dyck path of length $2n$ is a positive path with the jumps 1, -1 starting at 0 and finishing at 0 for the $2n$-th jump.
3. An excursion of the simple random walk is the trajectory of the walk until it reaches 0 for the first time. A simple random walk is a walk which starts at 0 and whose jumps are 1 and -1 and equally likely.

Proposition 2.
- *The set of Catalan trees of size n and the set of Dyck paths with $2n$ steps have the same cardinality.*
- *The Galton-Watson process with $Q = (1/2^i)$ and the excursions of the simple random walk are isomorphic, i.e. there is a bijection which maps a Galton-Watson process to an excursion and preserves the distributions.*

Proof. The picture below shows how an excursion is transformed into a Galton-Watson process. □

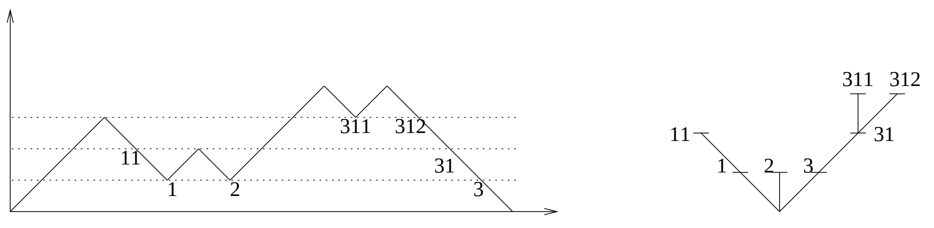


FIGURE 2. Equivalence between Galton-Watson processes and excursions

Remark. If one draws a contour starting at the left of the root of the tree in Figure 2 and following the vertices of the tree, when the contour arrives on the right of the root, its height will have performed the path followed by the random walk of Figure 2 above 1.

Bibliography

[1] Athreya (Krishna B.) and Ney (Peter E.). – *Branching processes.* – Springer-Verlag, New York, 1972, xi+287p. Die Grundlehren der mathematischen Wissenschaften, Band 196.

[2] Biggins (J. D.). – How fast does a general branching random walk spread? In *Classical and modern branching processes (Minneapolis, MN, 1994)*, pp. 19–39. – Springer, New York, 1997.

[3] Chauvin (Brigitte). – Sur la propriété de branchement. *Annales de l'Institut Henri Poincaré. Probabilités et Statistique*, vol. 22, n° 2, 1986, pp. 233–236.

[4] Devroye (Luc). – On the height of random m-ary search trees. *Random Structures & Algorithms*, vol. 1, n° 2, 1990, pp. 191–203.

[5] Flajolet (Philippe) and Odlyzko (Andrew). – The average height of binary trees and other simple trees. *Journal of Computer and System Sciences*, vol. 25, n° 2, 1982, pp. 171–213.

[6] Kesten (Harry) and Pittel (Boris). – A local limit theorem for the number of nodes, the height, and the number of final leaves in a critical branching process tree. *Random Structures & Algorithms*, vol. 8, n° 4, 1996, pp. 243–299.

[7] Kesten (Harry) and Stigum (B.). – A limit theorem for multidimensional Galton-Watson processes. *Annals of Mathematical Statistics*, vol. 37, 1966, pp. 1211–1223.

[8] Lyons (Russell), Pemantle (Robin), and Peres (Yuval). – Conceptual proofs of $L \log L$ criteria for mean behavior of branching processes. *The Annals of Probability*, vol. 23, n° 3, 1995, pp. 1125–1138.

[9] Neveu (Jacques). – Arbres et processus de Galton-Watson. *Annales de l'Institut Henri Poincaré. Probabilités et Statistique*, vol. 22, n° 2, 1986, pp. 199–207.

[10] Yaglom (A. M.). – Certain limit theorems of the theory of branching random processes. *Doklady Akad. Nauk SSSR (N.S.)*, vol. 56, 1947, pp. 795–798.

Convergence of Finite Markov Chains

Philippe Robert
INRIA-Rocquencourt

February 2, 1998

[summary by Jean-Marc Lasgouttes]

1. Framework

Let $X(t)$ be an aperiodic and irreducible Markov chain on a finite set S, with transition probabilities $P = (p(x, y))_{x,y\in S}$ and equilibrium distribution $(\pi(x))_{x\in S}$. It is often desirable to know how far $\Pr(X(t) = x)$ is from $\pi(x)$, in particular when $\pi(x)$ has a nice closed form, but the transient distribution is difficult to express. It is known (Doeblin) that there exists $\alpha \in]0, 1[$, such that

$$|P_y(t)(x) - \pi(x)| \le C\alpha^t, \quad \forall x, y \in S,$$

where $P_y(t)$ is the law of $X(t)$ when $X(0) = y$.

This talk is concerned with methods allowing to get more accurate estimates on this difference. The distance that will be used in the following is the *total variation* distance between two probability distributions P and Q on S, defined by

$$d_{tv}(P, Q) = \sup_{A\subset S} \{|P(A) - Q(A)|\} = \frac{1}{2}\sum_{i\in S} |P(\{i\}) - Q(\{i\})|,$$

or, more precisely

$$d(t) = \sup_{x\in S} d_{tv}(P_x(t), \pi).$$

One particularly interesting property is the existence of a *cutoff* (see Diaconis [2]):

Definition 1. There is a cutoff if there exist $a_n, b_n \to \infty$, $b_n/a_n \to 0$, such that

$$\lim_{n\to\infty} d(a_n + tb_n) = H(t),$$

with $\lim_{t\to-\infty} H(t) = 1$ and $\lim_{t\to+\infty} H(t) = 0$.

Two main methods can be used to evaluate $d(t)$:

– *Geometric* (see Diaconis and Stroock [3]): when X is a reversible Markov chain, then

$$d_{tv}(P_x(t), \pi) \le \frac{1}{2}\sqrt{\frac{1 - \pi(x)}{\pi(x)}}\,[\max\{\beta_1, |\beta_{m-1}|\}]^t,$$

where $-1 < \beta_{m-1} \le \beta_{m-2} \le \cdots \le \beta_1 < \beta_0 = 1$ are the eigenvalues of P. The values of β_1 and β_{m-1} can be obtained from the Rayleigh-Ritz principle.

– *Coupling* (see Aldous [1]): let X and $\tilde{X}$ be 2 versions of the Markov chain with transition matrix P, such that $X(0) = x$ and $\tilde{X}(0) \sim \pi$. A coupling time is a finite random variable T such that $X(t) = \tilde{X}(t)$, for all $t \ge T$. The following inequality holds for such T:

$$d_{tv}(P_x(t), \pi) \le \Pr(T > t).$$

Moreover, there exists a coupling T^* such that, for all $x \in S$, $d_{tv}(P_x(t), \pi) = \Pr(T^* > t)$.

2. Application to Erlang's Model

As an example of these techniques, let $X_N(t)$, $t \in \mathbb{R}_+$ be the Markov process associated with a M/M/N/N queue with arrival rate λN and service rate 1. This process, known as an Erlang loss system with N slots, has the transition rates

$$\begin{aligned} x \to x+1 :& \quad \lambda N \mathbf{1}_{\{x \le N\}} \\ x \to x-1 :& \quad x \end{aligned}$$

and its equilibrium distribution is

$$\pi(x) = C_N \frac{(\lambda N)^x}{x!}, \quad x \le N.$$

This process has three different regimes:

$\lambda > 1$. The queue becomes full after a finite time and $N - X_N(t/N)$ is a Markov process whose generator tends as $N \to \infty$ to the generator of a birth and death process.

$\lambda < 1$. The queue is never full and the process $(X_N(t) - \lambda N)/\sqrt{N}$ has a generator which tends to the generator of an Ornstein-Ülenbeck process with parameter λ.

$\lambda = 1$. The queue becomes full at infinity and the process $(N - X_N(t))/\sqrt{N}$ has a generator which tends to the generator of the reflected Ornstein-Ülenbeck process on $\mathbb{R}_+$.

The main result obtained in Fricker, Robert and Tibi [4] is the existence of a cutoff in the possible regimes of Erlang's model:

Proposition 1. *In the case $\lambda > 1$,*

$$\lim_{N\to\infty} d_N(t) = \begin{cases} 1 & \text{if } t < \log \frac{\lambda}{\lambda-1}, \\ 0 & \text{if } t > \log \frac{\lambda}{\lambda-1}. \end{cases}$$

In the case $\lambda \ge 1$ the behaviour of d_N is such that, for any sequence $\phi(N)$ and for any $a \in \mathbb{R}^*$,

$$\lim_{N\to\infty} d_N \left[\frac{\log N}{2} + a\phi(N)\right] = \begin{cases} 1 & \text{if } a < 0, \\ 0 & \text{if } a > 0. \end{cases}$$

These results are obtained by coupling techniques and use as an auxiliary process the M/M/∞ queue $Y_N(t)$ with input rate λN, which is the unbounded version of $X_N(t)$. A central tool in the proof is the process

$$(\mathcal{E}_c(t))_{t\ge 0} = \left((1+ce^t)^{Y_N(t)} e^{-\lambda N c e^t}\right)_{t\ge 0},$$

which turns out to be a martingale for any $c \ge 0$.

Bibliography

[1] Aldous (David). – Random walks on finite groups and rapidly mixing Markov chains. In *Seminar on probability, XVII*, pp. 243–297. – Springer, Berlin, 1983.

[2] Diaconis (Persi). – The cutoff phenomenon in finite Markov chains. *Proceedings of the National Academy of Sciences of the United States of America*, vol. 93, n° 4, 1996, pp. 1659–1664.

[3] Diaconis (Persi) and Stroock (Daniel). – Geometric bounds for eigenvalues of Markov chains. *The Annals of Applied Probability*, vol. 1, n° 1, 1991, pp. 36–61.

[4] Fricker (Christine), Robert (Philippe), and Tibi (Danielle). – *On the rates of convergence of Erlang's model.* – Research Report n° 3368, Institut National de Recherche en Informatique et en Automatique, February 1998.

Long Range Dependence in Communication Networks

Jean Bolot
INRIA-Sophia Antipolis

April 27, 1998

[summary by Philippe Robert]

Abstract

We examine under which conditions the salient long range dependence feature of network traffic must be taken into account in network performance evaluation. We show that "it is all a matter of time scales". Specifically, when studying the performance of a networking system or an application, many time scales must be taken into account — the time scales in the input traffic, but also the time scales of the system (they show up for example because of finite buffer queues) and the time scales of the performance metric of interest.

1. Introduction

The talk is concerned with the behavior of a buffer of a node in a telecommunication network. Messages are assumed to arrive randomly at this node where they wait in the buffer for transmission. We denote by $(X(t))$ the stochastic process describing the number of messages arrived during the t-th unit of time. The autocorrelation function is defined as

$$r(t) = \frac{E(X(0)X(t)) - E(X(0))E(X(t))}{E(X(0)^2) - E(X(0))^2},$$

where $E(Y)$ denotes the expected value of the random variable Y. The arrival process is said to have mixing properties if $X(0)$ and $X(t)$ are nearly independent when t is large, $r(t)$ is converging to 0 as t goes to infinity. Usually this assumption is satisfied; notice however that the periodic traffics are not mixing.

A simple characterization of the input traffic is provided by the rate at which $r(t)$ tends to 0. Up to now, most of the models analyzed assumed an exponential convergence to 0. This is clearly the case if the $(X(t))$ are i.i.d. random variables, $r(t) = 0$ for all $t \geq 0$. In this case, if the buffer size is infinite, it is known that at equilibrium the number $L(t)$ of messages at time t waiting for transmission has an exponential tail; that is, there exists $\gamma > 0$ such that

$$\lim_{x \to +\infty} e^{\gamma x} P(L(t) \geq x) = c \in \mathbb{R}_+.$$

This result has practical implications. Because the buffer sizes cannot be infinite, it implies that it is not necessary to design a big buffer because large queues of messages are (exponentially) very unlikely.

However a careful statistical analysis of data collected over a wide variety of networks [4] has provided ample evidence that network traffic processes are not exponentially mixing. In this case we shall say that the traffic exhibits a long range dependence (LRD) behavior. This is the case if $r(t) \sim C/t^\beta$ for some $\beta > 0$. A popular explanation of these LRD traffics is the following: an ON/OFF traffic generated by a single source consists in random burst intervals during which the source sends many messages alternating with idle intervals. An LRD traffic can be obtained by the superposition of an infinite number of ON/OFF traffics having larger and larger bursts (and idle) intervals.

In some of the (few) models analyzed with this kind of input traffic, it has been shown that if the buffer size is infinite then the number of messages at equilibrium has the following behavior: there exists $\delta > 0$ such that

$$P(L(t) \geq x) \sim \frac{c}{t^{\delta}}.$$

Notice that for the design of buffer sizes, the situation has changed. It is not clear that a small buffer will be sufficient because large queues of messages are not so unlikely.

Remark. It is possible to give a description of the occurrence of the "rare" events, when the number of messages in the buffer is greater that K, K large. In the case of the exponential decay of the autocorrelation function, it happens gradually, i.e., during some time interval the number of messages increases steadily at rate γ until it reaches K and then it decreases rapidly to 0. In the LRD case, the number of messages is greater than K in one big jump [1, 2].

2. Results

The point of view of the talk is slightly different from the usual presentation of these problems described above. It is stressed that these phenomena must be analyzed with *finite* buffer sizes, instead of guessing the behavior of the finite case from the infinite case. Simulations and measurements of various traffics over the Internet are used to carry out this analysis. The impact of the long range dependence is analyzed through the loss rate of the node, i.e., the average number of messages rejected because of the congestion of the node. The main conclusions of this approach are the following:

- The dependence on the past is limited by the size of the buffer. In other words, it is not necessary to consider a (very) long range dependent traffic to have a realistic traffic input;
- For a long range dependent traffic, increasing the buffer size has less impact than for a short range dependent traffic.

Bibliography

[1] Asmussen (Søren). – Rare events in the presence of heavy tails. In *Stochastic networks (New York, 1995)*, pp. 197–214. – Springer, New York, 1996.

[2] Durrett (Richard). – Conditioned limit theorems for random walks with negative drift. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 52, n° 3, 1980, pp. 277–287.

[3] Grossglauser (Matthias) and Bolot (Jean). – On the relevance of long-range dependence in network traffic. In *Proceedings ACM Sigcomm '96*. – Stanford, CA, September 1996.

[4] Leland (Will), Taqqu (Murad), Willinger (Walter), and Wilson (Daniel). – On the self-similar nature of ethernet traffic. *IEEE/ACM Transactions on Networking*, vol. 2, n° 1, February 1994, pp. 1–15.

Some Dynamical Routing Algorithms in Large Systems

Nikita D. Vvedenskaya
Institute of Information Transmission Problems
Russian Academy of sciences
Moscow 101447, GSP-4, 19 Bolshoi Karetnyi
Russia

November 3, 1997

[summary by Philippe Robert]

Abstract

We consider a system with N servers and messages arriving according to a Poisson process. The service time of a message is exponentially distributed. Two strategies to process the messages are compared. In the first strategy, an arriving message is sent randomly to one of the servers. In the second strategy, for each message two servers are selected randomly, and the message is directed to the least busy one. The queue length distribution is investigated as N tends to infinity.

1. Introduction

We assume that we have a set of N servers with N queues, these servers process a stream of jobs arriving to that system. Once an arriving job has been allocated to the queue of one of the servers, it cannot switch to another queue. We assume that the arrivals are Poisson with rate λN and the processing times are exponentially distributed with rate 1. Inside the queues, the service discipline is First In First Out. We shall assume that $\lambda < 1$, with this condition the system will not explode with the service disciplines which we consider.

The simplest strategy, S_{ind} say, to allocate the jobs is to distribute them at random to the servers. In this case the system is equivalent to a set of N independent queues with arrival rate λ and service rate 1. It is well known that, at equilibrium, in each queue the number of jobs has geometric distribution with parameter λ, in particular the probability that there is at least k jobs in a queue is λ^k.

A more efficient strategy S_{sh}, consists in choosing the shortest queue at the arrival of the job. Unfortunately, this kind of discipline is very difficult to analyze, in particular it would be desirable to compare it quantitatively with our first discipline. The exact analysis has been carried out by Flatto and Mac Kean [2] in the case $N = 2$, using uniformisation techniques. This approach does not seem to extend to a higher dimension.

The object of this talk is to analyze an intermediate discipline, S_{int}, for which it is possible to derive some quantitative results. An arriving job takes two servers at random and chooses the one with the shortest queue. Notice that for S_{sh}, there is a tight correlation between the queues, all of them are considered to allocate an arriving job. Here, only two of them determine the destination of the job. For a fixed N, a quantitative analysis remains difficult; however, as N goes to infinity, a given queue depends weakly of any other queue. As we shall see, asymptotically the queues behave independently. This phenomenon allows to write down one-dimensional equations. This approach is called the mean field method in statistical physics.

2. The Differential Equations

For this model, it is convenient to describe the queues in the following way: $u_{k,N}(t)$ will denote the fraction of the N queues which have at least k jobs at time t. Clearly

$$1 = u_{0,N}(t) \geq u_{1,N}(t) \geq \cdots u_{k,N}(t) \geq u_{k+1,N}(t) \geq \dots,$$

and $0 \leq u_{k,N}(t) \leq 1$, the vector $U_N(t) = (u_{k,N}(t))$ belongs to the state space $\mathcal{S} = [0,1]^{\mathbb{N}}$ which is compact for the point-wise convergence. It is easily seen that $(U_N(t))$ is a Markov process since the vector of the number of jobs in each queue is a Markov process and the order of the queues does not matter. If F is a measurable functional on $\mathcal{S}$, then $F(U_N(t))$ satisfies the stochastic differential equation,

$$\begin{aligned}(1)\quad dF(U_N)(t) = &\sum_{k=1}^{+\infty} N(u_{k,N}(t) - u_{k+1,N}(t))\left(F(U_N(t) - \frac{e_k}{N}) - F(U_N(t))\right) dt \\ &+ \sum_{k=1}^{+\infty} \lambda N(u_{k-1,N}^2(t) - u_{k,N}^2(t))\left(F(U_N(t) + \frac{e_k}{N}) - F(U_N(t))\right) dt + dM_N(t),\end{aligned}$$

where e_k is the vector $(1_{\{i=k\}})$. The first term in the right hand side is the contribution of departures, $N(u_k(t) - u_{k+1}(t))$ is the number of queues with k jobs hence the rate at which $U_N(t) \to U_N(t) - \frac{e_k}{N}$. The second term concerns the arrivals, $(u_{k-1}^2(t) - u_k^2(t))$ is the probability that two queues chosen at random have a size $\geq k$. The last term $M_N(t)$ is a martingale (which depends on F), i.e. roughly speaking, a stochastic perturbation; in particular $E(M_N(t)) = E(M_N(0))$ for all $t \geq 0$. It is easily seen using standard results concerning Poisson processes that

$$E(M_N^2(t)) \leq \frac{Kt}{N},$$

this simply means that the stochastic perturbation is vanishing as $N \to +\infty$. Taking $F(U) = u_k$, this suggests that the equation (1) becomes a deterministic differential equation,

$$(2)\qquad \frac{du_k(t)}{dt} = -(u_k(t) - u_{k+1}(t)) + \lambda(u_{k-1}^2(t) - u_k^2(t)), \quad k \geq 1.$$

If $(u_k(0)) \in L_1$, that is $\sum_{k=0}^{+\infty} u_k(0) < +\infty$, using a truncation procedure, it can be proved that (2) has a unique solution. So, as $N \to +\infty$, the $(u_{k,N}(t))$ should converge to a solution of this equation.

Rigorously, Doob's inequality [1] tells us that

$$P\left(\sup_{0\leq s\leq t} |M_N(s)| > a\right) \leq \frac{Kt}{a^2 N},$$

hence

$$\begin{aligned}(3)\quad P\Bigg(\sup_{0\leq s\leq t}\Bigg| &u_{k,N}(s) - u_{k,N}(0) + \\ &\int_0^s (u_{k,N}(x) - u_{k+1,N}(x)) - \lambda(u_{k-1,N}^2(x) - u_{k,N}^2(x))dx\Bigg| > a\Bigg) \leq \frac{Kt}{a^2 N}.\end{aligned}$$

It is easy to check that if $(u_{k,N}(0))$ converges to $(u_k(0))$ as $N \to +\infty$, then the sequence of processes

$$(u_{k,N}(s))_{0\le s\le t},\ N \in \mathbb{N}$$

is relatively compact. The identity (3) gives that any limit $(u_k(s))_{0\le s\le t}$ (in distribution) satisfies the differential equation (2) with probability one. We deduce that if $(u_k(0)) \in L_1$ then $(u_{k,N}(s))$ converges in distribution to the unique solution of (2).

3. The Convergence of the Invariant Measures

Up to now, we have only looked at the transient behavior of the queues. That is, for a fixed t, we proved that the state at time t converges in distribution. For $N \in \mathbb{N}$, the model of size N has an equilibrium distribution π_N; the (delicate) question is: as $N \to +\infty$ does the sequence (π_N) converge to a stable point of (2) ?

If $U(0) \in L_1$, then it is easily seen that (λ^{2^k}) is the unique stable point of (2). Notice that the π_N are probability measures on a compact space, thus the sequence is relatively compact. If one can show that every limit point is a stable point of (2) which belongs to L_1, then necessarily the sequence converges to (λ^{2^k}). This is done using the following estimation: for any continuous function $f : L_1 \to \mathbb{R}$,

$$\lim_{N\to+\infty} \sup_{v\in L_1} \|E_v(f(U_N(t))) - f(u_v(t))\| = 0,$$

where E_v denotes the expectation with the initial condition $U_N(0) = v$ and u_v is the solution of (2) with $u(0) = v$. This gives a kind of uniform convergence of the processes U_N.

4. Conclusion

For the strategy S_{int}, the queue length has a super exponential tail. We have seen that for S_{ind}, the tail was only exponential. It is remarkable that with a little improvement of S_{ind}, the tail distribution drops significantly. For the optimal discipline S_{sh}, asymptotically, it is easy to see that there will be an unbounded number of empty queues.

Bibliography

[1] Ethier (S.N.) and Kurtz (T.G.). – *Markov Processes, characterization and convergence.* – John Wiley & Sons Ltd, 1986, *Probability and mathematical statistics.*

[2] Flatto (L.) and McKean (H.P.). – Two queues in parallel. *Communications in Pure and Applied Mathematics*, vol. XXX, 1977, pp. 255–263.

[3] Vvedenskaya (N. D.), Dobrushin (R. L.), and Karpelevich (F. I.). – A queueing system with a choice of the shorter of two queues –an asymptotic approach. *Problemy Peredachi Informatsii*, vol. 32, n° 1, 1996, pp. 20–34.

Contents

Part 4. Probabilistic Methods

Unité de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unité de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unité de recherche INRIA Rhône-Alpes, 655, avenue de l'Europe, 38330 MONTBONNOT ST MARTIN
Unité de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105,
78153 LE CHESNAY Cedex
Unité de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS
Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex
(France)
http://www.inria.fr
ISSN 0249-6399