INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Algorithms seminar, 1998-1999

Bruno SALVY, éditeur scientifique

N ° 3830
Décembre 1999

THÈME 2

Rapport de recherche

ISSN 0249-6399 ISRN INRIA/RR--3830--FR+ENG

Algorithms seminar, 1998-1999

Bruno SALVY, éditeur scientifique

Thème 2 — Génie logiciel
et calcul symbolique
Projet Algo

Rapport de recherche n° 3830 — Décembre 1999 — 112 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.

Key-words: combinatorics, symbolic computation, analysis of algorithms, probabilistic methods

(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, 1998-1999

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 : la combinatoire, le calcul formel, l'analyse asymptotique et l'analyse en moyenne d'algorithmes et de structures de données.

Mots-clé : combinatoire, calcul formel, analyse d'algorithmes, méthodes probabilistes

ALGORITHMS SEMINAR
1998–1999

Bruno Salvy
(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 eighth of our series of seminar proceedings. The previous ones have appeared as INRIA Research Reports numbers 1779, 2130, 2381, 2669, 2992, 3267 and 3504. The content of these proceedings consists of English summaries of the talks, usually written by a reporter from the audience[1].

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 28 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, random walks and graphs. Maps are a special class of graphs on which progress has been made recently, this is reported in [**1**], [**2**] and [**3**]. Random walks are a deceptively simple model of many probabilistic processes, they are treated in different contexts in [**4**] and [**5**]. Young tableaux are a central object of algebraic combinatorics that connects integer partitions and group representations. Important results on their asymptotic properties are presented in [**6**] and [**7**]. The worst and best case complexity of a large class of algorithms can be given an explicit form, this is discussed in [**8**]. The last talk is concerned with a problem connecting physics and combinatorics.

[**1**] Conjugation of Trees and Random Maps. *Gilles Schaeffer*
[**2**] Rooted Maps, Functional Equations and Continued Fractions. *Jean-François Béraud*
[**3**] What is the Complexity of a Random Map ? *Kevin Compton*

[1] The summaries for the past eight years are available on the web at the URL `http://algo.inria.fr/seminars/`.

PART II. SYMBOLIC COMPUTATION

The study of multiple zeta values is currently a very active field, involving combinatorialists and computer algebraists. This problem is approached using Lie series and Gröbner bases in [**10**]. Gröbner bases are often used to solve polynomial systems, but they suffer from a bad complexity. A different algorithm with better complexity characteristics is described in [**11**]. The next two talks are concerned with differential problems. In the first one [**12**], the study of polynomial relations among solutions of linear operators is exploited to get better resolution algorithms. The second one [**13**] deals with asymptotic properties of solutions of first order non-linear differential equations.

PART III. ANALYSIS OF ALGORITHMS AND DATA STRUCTURES

The first two talks in this part are concerned with basic algorithms of computer algebra: [**14**] introduces a new method based on functional analysis to analyze the complexity of the Euclidean gcd algorithms on integers and variants of it; [**15**] estimates the complexity of Gaussian elimination on huge sparse matrices that occur for instance in integer factoring. The probability that graphs obeying various constraints be connected is studied in great generality in [**16**]. Tools of a more probabilistic origin are at work in the next two talks [**17**] and [**18**]. Finally, [**19**] discusses extensions of classical compression algorithms to the bidimensional context.

PART IV. PROBABILISTIC METHODS

This part contains talks of a more probabilistic origin, but not necessarily very different from those of the previous part. The width of trees is related to Brownian motion in [**20**]. Results on random walks on graphs are surveyed in [**21**], while [**22**] studies a simple process on graphs. Finally, a queuing model is studied by [**23**] and [**24**] presents an analysis of a problem from wireless networking.

[**23**] Asymptotic Bounds for the Fluid Queue Fed by Subexponential on/off Sources. *Vincent Dumas*

[**24**] Optimal Carrier Sharing in Wireless TDMA. *Ed Coffman*

PART V. NUMBER THEORY

The visits of Ilan Vardi in our group resulted in several interesting talks. The first one on continued fractions [**25**], the second one [**26**] an introduction to analytic number theory and the last one [**27**] on the distribution of the leading digits of numbers. Another talk, by François Morain, gives an algorithmic viewpoint on classical algorithms in cryptography.

[**25**] Continued Fractions from Euclid to Present Days. *Ilan Vardi*

[**26**] An Introduction to Analytic Number Theory. *Ilan Vardi*

[**27**] Leading Digit and Algebraic Numbers. *Ilan Vardi*

[**28**] Algorithms in Classical Cryptanalysis. *François Morain*

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, most notably Cyril Banderier and Philippe Robert for writing more than their share of 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

Conjugation of Trees and Random Maps

Gilles Schaeffer
LaBRI, Université Bordeaux I

February 1, 1999

[summary by Alain Denise]

Abstract

We present a general scheme to generate uniformly at random planar maps of various kinds. Our algorithms rely on a combinatorial and bijective approach: we encode the planar maps by some classes of particular trees. This encoding is the basis of efficient random generators of maps of the most simple classes of planar maps. For more complex structures, we proceed by using a new general probabilistic scheme, that we call *extraction/rejection* algorithm.

1. Introduction

A *planar map* is an embedding of a graph in the plane, considered up to continuous deformations of the plane. Maps are allowed to have multiple edges and loops; otherwise there are called *simple maps*. The maps we consider are *rooted*: there is an oriented edge, called the *root*.

We present here two families of algorithms for the random generation of rooted planar maps. The first one applies to the few classes of maps which are counted by multiplicative closed formulas. Here are two examples from [2, 5]:

$$\text{Number of planar maps with } n \text{ edges: } \frac{2}{n+2}\frac{3^n}{2n+1}\binom{2n+1}{n},$$

$$\text{Number of bipartite cubic maps with } 3n \text{ vertices: } \frac{3}{n+2}\frac{2^{n-1}}{2n+1}\binom{2n+1}{n}.$$

Our approach consists in finding new bijections between these maps and some particular families of trees. More precisely, there exists, for each family of maps as above, a family of trees such that

$$\#\{\text{maps}\} = \frac{\#\{\text{free leaves}\}}{\#\{\text{leaves}\}} \cdot \#\{\text{trees}\},$$

and the bijection is given by the *closure* of the trees (terms like *free leaves* and *closure* will be explained below). Then the generation scheme is the following: *i)* generate uniformly at random a tree, by known efficient algorithms; *ii)* "decode" the tree to get its associated map. Table 1 gives the basic families that benefit from this approach, leading to linear generation algorithms. The method is illustrated in Section 2 on the family of bipartite cubic maps.

However, a number of families do not present simple formulas as above. In these cases we use a new method: *extraction/rejection*. It combines the usual rejection principle with *composition schemes* that are common for maps. See in Table 2 the new families reached with this new approach, which is presented in Section 3.

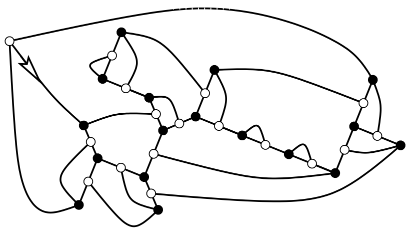


FIGURE 1. A bipartite cubic map with 17×2 vertices

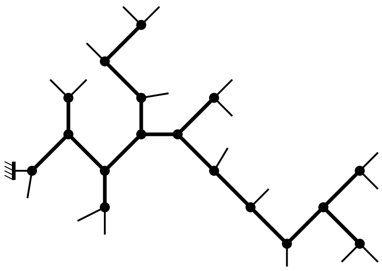


FIGURE 2. A planted plane tree with 17 internal nodes

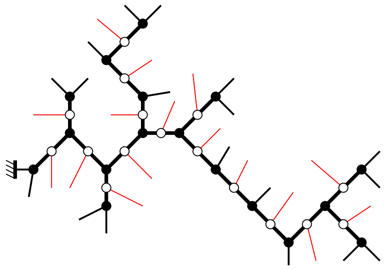


FIGURE 3. A blossom tree

2. **Bijective Approach**

We present here the method through the example of bipartite cubic maps: maps whose vertices have degree 3 and are colored in black or white in such a way that no edge joins two vertices of the same color (Figure 1).

These maps are in bijection with *blossom trees*, as we will see below. A *planted plane binary tree* is a plane binary tree whose root has degree one. Figure 2 presents such a tree (the leaves are omitted in the figure, except the root leaf at the left). A *blossom tree* is a particular tree which can be constructed from a planted plane tree as follows: in the middle of each internal edge, we put a white-colored vertex with a *bud* on one of the two sides, as in Figure 3. Now we call *partial closure* of a blossom tree the structure obtained after the following treatment: turn anti-clockwise around

main family	intermediate family	underlying trees
general	quartic (all degree 4)	binary
bipartite (or Eulerian)	bipartite cubic	binary
m-constellations	m-Eulerian	general
non separable	quartic without 2-cocycle	ternary
loopless triangulations	non separable cubic	ternary

TABLE 1. Maps (with n edges, loops and multiple edges allowed) generated in linear time

maps	simple	smooth	no leaf	2-c	non separ.	3-c	4-c
all	ok	ok	ok	ok	ok	ok	no
bipartite	ok	no	ok	ok	ok	no	no
triangulations	ok	-	-	-	-	ok	ok

TABLE 2. Some extra properties reachable via extraction/rejection. (Non separable means loopless 2-connected, smooth means without vertices of degree 2)

the tree, and join each bud to the nearest leaf so that no crossing occurs. (In this way, buds and leaves can be seen as a system of nested parentheses.) See in Figure 4 the partial closure of the blossom tree of Figure 3. Since there are 3 more leaves than buds in any blossom tree, there are necessarily 3 leaves which remain alone; we call them *single leaves*. We say that a blossom tree is *balanced* if its root is a single leaf in its partial closure. Finally the *complete closure* of a blossom tree is obtained by joining the three single leaves to a new vertex and rooting the resulting map towards the root leaf (Figure 5). This gives the map of Figure 1.

Theorem 1. *The complete closure defines a one-to-one correspondence between balanced blossom trees with n nodes and bipartite cubic maps with $3n$ edges.*

Now here is the way to generate uniformly at random a bipartite cubic map with $3n$ edges:

1. generate uniformly at random a planted binary tree with n nodes; this can be done in linear complexity with well known algorithms (see [1] for example);
2. toss a coin independently for each edge to place buds;
3. choose with probability $1/3$ one of the three possible balanced blossom trees and achieve the complete closure.

3. Extraction/Rejection Algorithms

Suppose that we have to generate uniformly at random a *bicolored triangulation* like the one in Figure 6, with a given number of faces. By duality, this is equivalent to generate a bipartite cubic map as the one in Figure 7: each black (resp. white) vertex in the map gives a black (resp. white) triangle in the triangulation, each face gives a vertex. But the map must be without *separator*, i.e., without configuration like the one on the left of Figure 8; otherwise the associated triangulation might present multiple edges, like in the right of the figure.

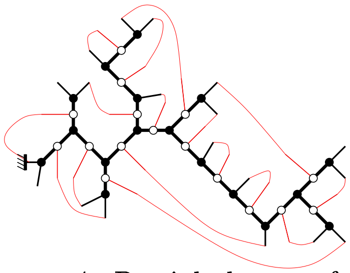


FIGURE 4. Partial closure of the blossom tree

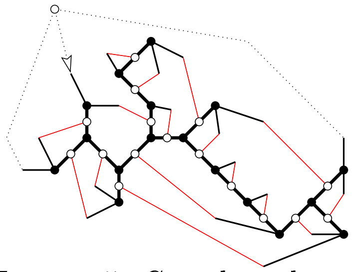


FIGURE 5. Complete closure of the blossom tree

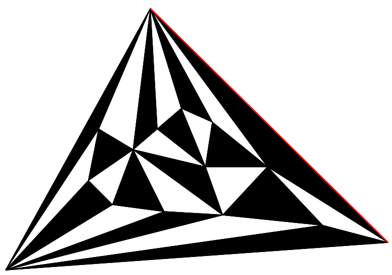


FIGURE 6. A bicolored triangulation

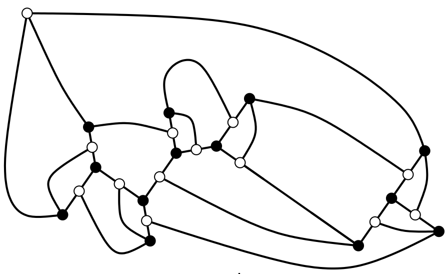


FIGURE 7. A bipartite cubic map without separator

A natural idea would be to use a rejection algorithm in order to generate maps without separators: draw uniformly at random bipartite cubic maps until we get a map without separator. Unfortunately, bipartite cubic maps without separators are very rare, so this approach is practically intractable. So we need another idea. Here is the extraction/rejection method:

1. Generate uniformly at random a bipartite cubic map with the algorithm of Section 2;
2. remove the possible separators (we get what we call the *core* of the map);
3. construct the triangulation from the core by duality.

An important problem appears here: if we generate a map with n vertices and remove the separators, the resulting map is likely to have less than n vertices! To fix this problem, we will generate *maps with too many vertices*: we can prove, using asymptotic analysis, that drawing bipartite cubic maps with $m = 3n$ vertices gives, with a good probability, cores having n vertices. This leads to an algorithm with complexity $O(n^{5/3})$.

This approach can be generalized for a number of families, as seen in Table 2. Details are given in [3, 4].

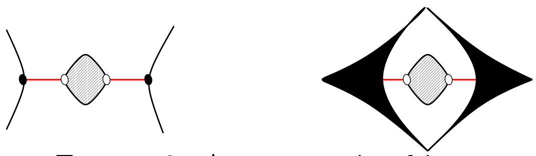


FIGURE 8. A separator in a bipartite cubic map and its result by duality

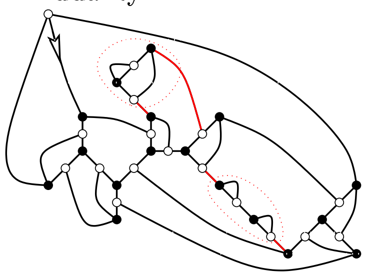


FIGURE 9. A map with separators

Bibliography

[1] Alonso (Laurent) and Schott (René). – *Random generation of trees.* – Kluwer academic publishers, 1995.

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

[3] Schaeffer (Gilles). – *Conjugaison d'arbres et cartes combinatoires aléatoires.* – PhD thesis, Université Bordeaux I, 1998.

[4] Schaeffer (Gilles). – Random sampling of large planar maps and convex polyhedra. In *Proceedings of STOC'99.* – Atlanta, 1999.

[5] Tutte (W. T.). – On the enumeration of planar maps. *Bulletin of the American Mathematical Society*, vol. 74, 1968, pp. 64–74.

Rooted Maps, Functional Equations and Continued Fractions

Jean-François Béraud
Université de Marne la Vallée, Institut Gaspard Monge

February 1, 1999

[summary by Dominique Gouyou-Beauchamps]

Abstract

The enumeration of rooted maps has been first studied by W. T. Tutte in the early 1960's, with planar maps. New results have been obtained since for rooted maps on more general surfaces (torus with 1, 2, 3 holes, projective plane, ...). I present the enumeration of rooted maps on the Klein bottle as a first step to the general case. Then I give an other approach of the enumeration of rooted maps, the rooted maps regardless to the genus of their associated surface. This leads to Riccati equations whose solutions are expressed as continued fractions. I obtain also a new equation generalizing the Dyck equation for rooted planar maps.

Details may be found in the recent works of D. Arquès and J. F. Béraud [2, 3]. Good introductions to maps and hypermaps can be found in [4, 1, 6, 5].

1. Definitions

There are two kinds of closed surfaces, orientable and nonorientable. The sphere, the torus, the double torus, the triple torus, and so on, are orientable. They are commonly denoted S_0, S_1, S_2, $S_3, \ldots$ It is proved that every closed connected orientable surface is homeomorphic to one of them.

The *Möbius band* is a surface that is neither closed nor orientable. What makes it nonorientable is that if a 2×2 coordinate system specifying a forward direction and a right direction is translated in the forward direction once around the center of the band, then the orientation of the right direction is reversed. The Möbius band has a boundary which is homeomorphic to the circle. For $k = 0, 1, \ldots,$ the surface obtained by cutting k holes in a sphere and closing them off with k Möbius bands is denoted N_k. It is proved that every closed, connected nonorientable surface can be obtained in such a way. The surface N_0 (resp. N_1, N_2) is called the sphere (resp. the projective plane, the Klein bottle). The projective plane, or its unclosed version the Möbius band [5], is also called a *crosscap*.

We define an *embedding* $i : G \to S$ of a graph G into a closed surface S to be a continuous one-to-one function from a topological representation of the graph into the surface (i.e. the edges do not intersect and the cells (vertices, edges and faces) are preserved). The *Euler characteristic of a cellular embedding* $G \to S$ of a connected graph G into a closed surface S is the value of the Euler formula $\#V - \#E + \#F$ (where V, E and F are the sets of vertices, edges and faces of G), and is denoted $\chi(G \to S)$. The invariance of Euler characteristic claims that for any cellular embedding $G \to S_g$ (resp. $G \to N_k$), then $\chi(G \to S_g) = 2 - 2g$ (resp. $\chi(G \to N_k) = 2 - k$). The *genus* of a compact surface is given by the relation $g = \frac{1}{2}(2 - \chi)$ (resp. $g = 2 - \chi$) in the orientable (resp. nonorientable) case.

The *genus range* (resp. *crosscap range*) of a graph G is defined to be the set of number g such that the graph G can be cellularly embedded in the surface S_g (resp. N_g). Of course, the minimum genus range (resp. crosscap range) is the genus (resp. crosscap number) $\gamma(G)$ (resp. $\bar{\gamma}(G)$) of the graph.

A *topological map* C on an orientable surface Σ of $\mathbb{R}^3$ is a partition of Σ in three finite set of *cells:*

1. the set of the vertices of C, that is a finite set of points;
2. the set of the edges of C, that is a finite set of simple open Jordan arcs, disjoint in pairs, whose extremities are vertices;
3. the set of the faces of C. Each face is homomorphic to an open disc, and its border is an union of vertices and edges.

The *genus of the map* is the genus of the surface Σ. A cell is called *incident* to another cell if one of them is in the border of the other. An *isthmus* is an edge incident on both sides to the same face. We call *half-edge* an oriented edge of the map. A map is called a *rooted map* if a half-edge $\tilde{h}$ is chosen. The half-edge $\tilde{h}$ is called the root half-edge of the map, and its initial vertex the *root vertex* of the map. We call *external face* (or *root face*), the face generated by the root half-edge $\tilde{h}$.

Two rooted maps with the same genus are isomorphic if there exists an homeomorphism of the associated surface, preserving its orientation, mapping the vertices, edges, faces and the root half-edge on the first map respectively on those of the second one. An isomorphic class of oriented (resp. nonoriented) rooted maps of genus g will simply be called an *orientable* (resp. *non orientable*) *rooted map*.

2. Series of Rooted Maps on the Klein Bottle

We denote by $P_i(u,z) = \sum a_{i,n,m} u^n z^m$, $i = 1,2,3$, the generating series where $a_{i,n,m}$ is the number of nonorientable rooted maps of genus i having its rooted face of degree n and having m edges. The generating series $P_0(u_1,u_2,z)$ is the generating series of 2-rooted planar maps (two half-edges are chosen).

Theorem 1. *The generating series $P_i(u,z)$, $i = 1,2,3$, of nonorientable rooted maps with respect to the degree of the rooted face and the number of edges verify the following equations:*

$$P_0(u,z) = 1 + u^2 z P_0(u,z)^2 + uz\frac{uP_0(u,z) - P_0(1,z)}{u-1}, \tag{1}$$

$$P_1(u,z) = u^2 z\left(2P_1(u,z)P_0(u,z) + \frac{\partial}{\partial u}\left[uP_0(u,z)\right]\right) + uz\frac{uP_1(u,z) - P_1(1,z)}{u-1}, \tag{2}$$

$$\begin{aligned} P_2(u,z) = {} & u^2 z\left(2P_2(u,z)P_0(u,z) + P_1(u,z)^2 + P_0(u,u,z) + \frac{\partial}{\partial u}\left[uP_1(u,z)\right]\right) \\ & + uz\frac{uP_2(u,z) - P_2(1,z)}{u-1}. \end{aligned} \tag{3}$$

The proof is based on the topological operation of deleting the root half-edge $\tilde{h}$ as introduced by W. Tutte [7]. If we introduce the formal power series $V(z) = 1/(1 - zV(z)P_0(V(z),z))$, in [1] we find a very simple proof that $A(V(z),z) = 0$ and that $z = (V(z)-1)(3-2V(z))/V(z)^2$ where $A(u,z) = 1 - u + u^2 z - 2(1-u)u^2 z P_0(u,z)$. Now, we remark that:

$$P_2(u,z)A(u,z) = uzP_2(1,z) + (1-u)u^2 z\left(\frac{\partial}{\partial u}\left[uP_1(u,z)\right] + P_1(u,z)^2 + P_0(u,u,z)\right).$$

Then the generating series $P_0(u_1, u_2, z)$ verifies the functional equation:

$$P_0(u_1,u_2,z) = 2u_1^2 z P_0(u_1,u_2,z)P_0(u_1,z) + u_1 z \frac{u_1 P_0(u_1,u_2,z) - P_0(1,u_2,z)}{u_1 - 1} + u_1 u_2 z \frac{\partial}{\partial u_2}\left[u_2 \frac{u_1 P_0(u_1,z) - u_2 P_0(u_2,z)}{u_1 - u_2}\right].$$

If we define the series p by the relation $z = p(1-3p)$, we obtain:

Theorem 2. *The generating series $P_2(1,z)$ counting rooted maps on the Klein bottle with respect to the number of edges is the solution of the following parameterized system of equations:*

$$\begin{cases} z &= p(1-3p), \\ P_2(1,z) &= \frac{(1-3p)\left(1-4p+\sqrt{(1-6p)(1-2p)}\right)}{(1-6p)^2(1-2p)}. \end{cases} \tag{4}$$

3. Series of Orientable Rooted Maps

We present here the first topological equation for the generating series of orientable rooted maps regardless to genus, with respect to vertices and edges. We denote by $M(y,z) = \sum a_{n,m} y^n z^m$ the generating series where $a_{n,m}$ is the number of orientable rooted maps of any genus having n vertices and m edges.

Theorem 3. *The generating series $M(y,z)$ of orientable rooted maps is the solution of the Riccati equation:*

$$M(y,z)) = y + zM(y,z)^2 + zM(y,z) + 2z^2 \frac{\partial}{\partial z} M(y,z). \tag{5}$$

The proof is based on the topological operation of deleting the root half-edge $\tilde{h}$ as introduced by W. Tutte [7]

4. Orientable Rooted Maps and Trees

Equation (5) is a Riccati differential equation. We present in Theorem 4 an iterative solution of (5), which leads to a very nice continued fraction form of the generating series of orientable rooted maps.

Theorem 4. *The generating series $M(y,z)$ of orientable rooted maps with respect to the number of vertices and edges is:*

$$M(y,z) = \cfrac{y}{1 - \cfrac{(y+1)z}{1 - \cfrac{(y+2)z}{1 - \cfrac{(y+3)z}{1 - \cdots}}}}$$

In Theorem 4 a new relation on maps appears:

Corollary 1. *The generating series $M(y,z)$ of orientable rooted maps with respect to the number of vertices and edges is the solution of the following generalized Dyck equation:*

$$M(y,z) = y + zM(y,z)M(y+1,z).$$

A *tree* (of any genus) is a map with only one face. We denote by $T(z)$ the generating series of orientable rooted trees with respect to the number of edges. By duality there exists a one-to-one correspondence between rooted trees and rooted maps with only one vertex. Thus the series of trees is the coefficient of y in the series of maps and:

$$T(z) = \left[\frac{M(y,z)}{y}\right]_{|y=0}.$$

Then we obtain the following results:

Corollary 2. *The generating series $T(z)$ of orientable rooted trees is the solution of the following differential equation:*

$$T(z)) = 1 + zT(z) + 2z^2 \frac{\partial}{\partial z} T(z).$$

The generating series $T(z)$ of orientable rooted trees is:

$$T(z) = \cfrac{1}{1 - \cfrac{z}{1 - \cfrac{2z}{1 - \cfrac{3z}{1 - \cfrac{4z}{1 - \cdots}}}}}.$$

Both generating series of orientable rooted trees and orientable rooted maps are linked by the relation:

$$T(z) = \frac{1}{1 - zM(1,z)}.$$

From the previous expressions, we deduce an explicit formula enumerating orientable rooted trees with a given number of edges:

Corollary 3. *The number of orientable rooted trees with n edges is equal to the number of fixed-point-free involutions on $[2n]$, namely the odd factorial: $(2n-1)(2n-3)\cdots 1 = (2n)!2^{-n}/n!$.*

Bibliography

[1] Arquès (Didier). – Une relation fonctionnelle nouvelle sur les cartes planaires pointées. *Journal of Combinatorial Theory. Series B*, vol. 39, n° 1, 1985, pp. 27–42.

[2] Arquès (Didier) and Béraud (Jean-François). – Énumération des cartes pointées sur la bouteille de Klein. *RAIRO Informatique Théorique et Applications. Theoretical Informatics and Applications*, vol. 31, n° 4, 1997, pp. 385–409.

[3] Arquès (Didier) and Béraud (Jean-François). – Rooted maps and hypermaps on surfaces. In *Proceedings Formal Power Series and Algebraic Combinatorics (FPSAC'99)*, pp. 18–29. – Universitat Politèchnica de Catalunya, Barcelona, 1999.

[4] Cori (Robert). – Un code pour les graphes planaires et ses applications. *Astérisque*, vol. 27, 1975.

[5] Gross (Jonathan L.) and Tucker (Thomas W.). – *Topological graph theory.* – John Wiley & Sons Inc., New York, 1987. A Wiley-Interscience Publication.

[6] Massey (William S.). – *Algebraic topology: an introduction.* – Springer-Verlag, New York, 1977. Reprint of the 1967 edition, Graduate Texts in Mathematics, Vol. 56.

[7] Tutte (W. T.). – On the enumeration of planar maps. *Bulletin of the American Mathematical Society*, vol. 74, 1968, pp. 64–74.

What is the Complexity of a Random Map?

Kevin Compton
University of Michigan

March 29, 1999

[summary by Gilles Schaeffer[1]]

This talk presents a joint work with Ed Bender and Bruce Richmond [2].

1. Introduction

A class of structures obeys a 0–1 law if every first-order sentence has an asymptotic probability of 0 or 1 within the class. Techniques used to prove 0–1 laws are closely related to average-case analyses of algorithms. For example, Abiteboul, Compton and Vianu [1] showed that the 0–1 law for random relational structures (which includes random graphs with constant edge probabilities) can be used to give an average-case analysis of certain database query optimizations. However, the random graph model is not a very realistic model for databases, so it is useful to examine other structures. A map, or embedding of a graph into a surface of fixed genus, may be a better model of certain kinds of geometric databases. Here we show that the class of random maps in surface of fixed genus obeys a 0–1 law. The proof is based on game strategies and keeping track of anchors.

2. First Order Logic on Maps

A *map* is an embedding of a connected graph G in a surface S such that all components of $S \setminus G$ are simply connected regions called *faces*. Maps are considered up to homeomorphisms *of the surface* taking vertices to vertices, edges to edges and faces to faces.

Like graphs, maps with a finite number of edges can be given various combinatorial representations. We shall use the *cross* representation, introduced by Tutte [9]: each edge is viewed as a fat ribbon with four corners or *crosses* (see Figure 1), and three fix-point free involutions are defined on the set A_c of crosses. The first two, γ and δ, relate two by two the four adjacent crosses of each edge, γ along faces and δ along vertices. The last one, τ, relates pairs of crosses sharing an incidence between a face and a vertex. The structure $\langle A_c, \gamma, \delta, \tau\rangle$ completely defines the map: for instance, vertices, faces and edges are respectively described by the orbits of the subgroups $\langle \gamma, \tau\rangle$, $\langle \delta, \tau\rangle$ and $\langle \gamma, \delta\rangle$.

Now let us consider the vocabulary Σ_1 consisting of a set of constants and the binary relations Γ, Δ and T. A map $\langle A_c, \gamma, \delta, \tau\rangle$ can then be seen as a structure over Σ_1, where the constants are taken in A_c and the binary relations are interpreted as the respective graphs of the three involutions. Our interest is in properties expressible by first order formulas on these structures. In order to allow quantification on vertices and faces, and not only on crosses, we enrich the vocabulary with two other sets of constants (for vertices and faces) and two other binary relations I and J, respectively interpreted as the incidence relations between vertices and crosses and between crosses and faces.

[1] See also the summary on the same subject by Frédéric Chyzak in the 1995–1996 edition.

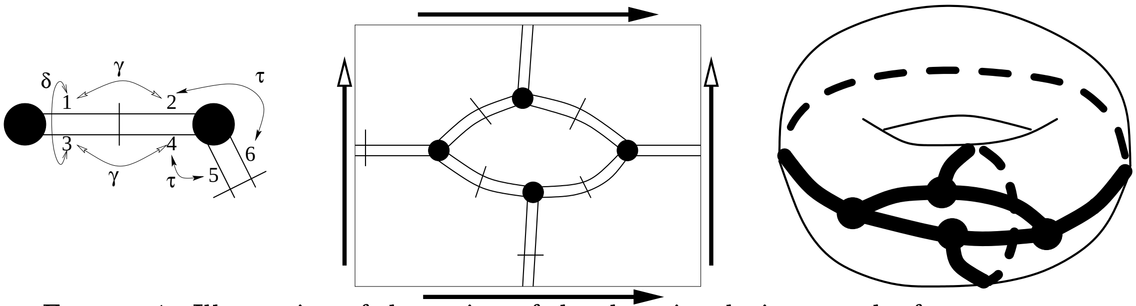


FIGURE 1. Illustration of the action of the three involutions on the four corners or crosses of edges, and two different drawings of the same map on the torus.

For convenience the binary relation E is also added to describe crosses that belong to the same edge (although E could be expressed in terms of Γ, Δ and T). Let Σ be this extended vocabulary.

For instance, the following sentence (*i.e.*, formula without free variable) is satisfied by maps containing a cycle of length three:

$$\begin{aligned}\exists v_1, v_2, v_3 \exists c_{12}, c_{21} \quad & c_{12} \neq c_{21} \wedge E(c_{12}, c_{21}) \wedge I(v_1, c_{12}) \wedge I(v_2, c_{21}) \\ \wedge \quad & \exists c_{13}, c_{31} \quad c_{13} \neq c_{31} \wedge E(c_{13}, c_{31}) \wedge I(v_1, c_{13}) \wedge I(v_3, c_{31}) \\ & \wedge \quad \exists c_{23}, c_{32} \quad c_{23} \neq c_{32} \wedge E(c_{23}, c_{32}) \wedge I(v_2, c_{23}) \wedge I(v_3, c_{32}).\end{aligned}$$

In the study of asymptotic 0–1 laws for random structures (here maps), we consider a class of structures $\mathcal{C}$ on Σ, with the uniform measure μ_n on the set $\mathcal{C}_n$ of structures of size n (here maps with n edges). Our interest is in the limit when n goes to infinity of

$$\mu_n(\phi) = \mu_n(\{\mathcal{A} \in \mathcal{C}_n \mid \mathcal{A} \models \phi\}).$$

If this limit exists, it is called the *asymptotic probability* of ϕ and denoted $\mu(\phi)$.

A class of structures has *an asymptotic first order 0–1 law* if all first-order sentences have an asymptotic probability of either 0 or 1.

3. 0–1 Laws and the Ehrenfeucht-Fraïssé Game

A classical logical tool to prove 0–1 laws is the Ehrenfeucht-Fraïssé game: essentially this game is used to show that if two structures have the same kinds of *local* substructures then they satisfy the same first-order sentences of given *quantifier rank.*

The *quantifier rank* of a formula is the maximal number of stacked quantifiers in the formula (*e.g.* the previous example has rank 5). Given two maps $\mathcal{A}$ and $\mathcal{B}$, we write $\mathcal{A} \equiv_m \mathcal{B}$ if they satisfy the same formulas of rank at most m. Remark that the number of inequivalent formulas of given rank over Σ is finite, so that the number of equivalence classes for $\equiv_m$ is finite, a fact that we shall use in Section 4. The following proposition is only a matter of rephrasing:

Proposition 1. *A class of structure $\mathcal{C}$ has an asymptotic first order 0–1 law if and only if for all m there exists an equivalence class $\mathcal{E}_m$ of $\equiv_m$, such that*

$$\lim_{n\to\infty} \mu_n(\{\mathcal{A} \in \mathcal{C}_n \mid \mathcal{A} \in \mathcal{E}_m\}) = 1.$$

Therefore, in order to prove a 0–1 law, one should define, for all m, a large enough class $\mathcal{E}'_m$ in which maps cannot be distinguished by rank m formulas. Here come the Ehrenfeucht-Fraïssé game in play: There are two players, SPOILER and DUPLICATOR, playing m rounds on two structures (here maps) $\mathcal{A}$ and $\mathcal{B}$. SPOILER starts each round by picking an element (a cross, a vertex or a face) in one of the maps and DUPLICATOR responds by picking an element of the same kind in the other map. These $2m$ elements are viewed as interpretations $d_1^{\mathcal{A}}, \ldots, d_m^{\mathcal{A}}$ and $d_1^{\mathcal{B}}, \ldots, d_m^{\mathcal{B}}$ of some fresh constants $d_1, \ldots, d_m$. After m rounds, DUPLICATOR wins if the two extended structures over $\Sigma \cup \{d_1, \ldots, d_m\}$ cannot be distinguished by *atomic* formulas (*i.e.*, without quantifier).

Theorem 1 (Fraïssé, Ehrenfeucht). *Let $\mathcal{A}$ and $\mathcal{B}$ be two structures over Σ.* DUPLICATOR *has a winning strategy in the m-round game if and only if $\mathcal{A} \equiv_m \mathcal{B}$.*

Hence we look for a large enough class $\mathcal{E}'_m$ on which we can describe a winning strategy for DUPLICATOR. As suggested by the classical approach, we want to consider the class of structures that contain many copies of all possible kinds of *local substructures.* In such a structure DUPLICATOR will always be able to find a local substructure on which to imitate SPOILER.

4. Distance and Richness in Maps

In order to formalize the idea of *local substructures* for maps we are led by existing results on random maps to consider:

- **Distances in the derived map:** a proper notion of distance can be defined (which is somewhat more complicated than distance on graphs) so that all relations of Σ are local (*i.e.*, they are false as long as elements are at a distance greater than, say, two).
- **Planar balls:** the substructures we consider are the finite radius balls (in the sense of the previous distance) which are planar.

While it is natural to define a distance and consider finite radius balls, the planarity assumption may be surprising. It comes from the theory of random maps: many families of maps (on surfaces of given genus) have the *large representativity* property, asserting that for a given d, in almost all maps, the balls of diameter d are planar submaps. All the families $\mathcal{C}$ of maps we will consider then have the following *richness* property:

Property 1 (Richness). *Let P be a fixed planar map occurring as a submap of some map in our family $\mathcal{C}$, and k be a non-negative integer. Then*

$$\mu(\forall a_1, \ldots, a_k \ \exists \text{ a submap isomorphic to } P \text{ not containing } a_1, \ldots, a_k) = 1$$

where $a_1, \ldots, a_k$ range over all vertices, faces and crosses.

At each round of the game, our DUPLICATOR will need to use richness to choose an element with a neighborhood isomorphic to the neighborhood of the element chosen by SPOILER. Unfortunately, given a diameter d, there are infinitely many possible planar balls with this diameter, so that the richness property is not sufficient. Instead of requiring DUPLICATOR to choose an isomorphic neighborhood, we will content with a neighborhood that is indistinguishable by rank-m-sentences. As there are only a finite number of $\equiv_m$-equivalence classes of planar balls with given diameter d, DUPLICATOR will only have to make his choice in a finite set of representative $\mathcal{B}_1, \ldots, \mathcal{B}_k$.

We are now in a position to define the class of maps $\mathcal{E}'_m$ on which DUPLICATOR has a winning strategy: let m be fixed, and consider the set of maps such that, for each $\mathcal{B}_i$ and $a_1, \ldots, a_k$ as above, there exists a submap isomorphic to $\mathcal{B}_i$ avoiding $a_1, \ldots, a_k$. As there are finitely many $\mathcal{B}_i$, Property 1 implies that this set $\mathcal{E}'_m$ is large enough, *i.e.*, satisfies

$$\lim_{n\to\infty} \mu_n(\{\mathcal{A} \in \mathcal{C}_n \mid \mathcal{A} \in \mathcal{E}'_m\}) = 1.$$

Therefore we need to prove that DUPLICATOR has a winning strategy for all couples of maps in $\mathcal{E}'_m$.

5. Winning Strategy and the Good Use of Anchors

The strategy for DUPLICATOR associates a security zone to each chosen element with the following requirements:

- The security zone of an element e chosen at round i contains all elements at distance at most 2^{m-i+1} of e.
- The security zones of the two elements chosen at each round are indistinguishable (*i.e.*, belong to the same $\equiv_m$-equivalence class).

Suppose now SPOILER chooses element e at round i; there are two cases:

1. if no previously chosen element is in the security zone $\mathcal{Z}$ of e, then DUPLICATOR chooses any element e' in the other map with a security zone $\mathcal{Z}'$ indistinguishable from $\mathcal{Z}$, and disjoint from previously chosen zones. In this case, e and e' are their own anchor. The assumption on $\mathcal{E}'$ assures that this is always possible.
2. if a previously chosen element f is in the security zone of e, then there is a chance that they interact. In this case, let g be the anchor of f. It is easy to see that e belongs to the security zone of g, because the sizes of the zones are exponentially distributed. Therefore DUPLICATOR can choose the image e' of e in the zone $\mathcal{Z}'$ associated to the security zone $\mathcal{Z}$ of g. The anchors of e and e' are respectively set to be g and g'.

At the end of the game, elements in $\mathcal{A}$ are either too far away to interact or share the same anchor. In both cases the corresponding elements in $\mathcal{B}$ will satisfy the same atomic formulas.

6. Conclusion

Richness properties have been proved for many families of rooted maps by Bender *et al.* [4, 3, 5, 6, 7]. Thanks to the work of Richmond and Wormald [8] these results hold as well for unrooted maps. Using the previously described machinery it implies 0–1 laws for the following families of maps on a surface of given genus: all maps, smooth maps, 2-connected maps, 3-connected maps, triangular maps, 2-connected triangular maps and 3-connected triangular maps.

Bibliography

[1] Abiteboul (S.), Compton (K. J.), and Vianu (V.). – Queries are easier than you though (probably). In *Proceedings of the ACM Symposium on Principle of Database Systems*. pp. 32–42. – Association for Computing Machinery, 1992.

[2] Bender (E. A.), Compton (K. J.), and Richmond (L. B.). – 0-1 laws for maps. *Random Structures & Algorithms*, vol. 14, n° 3, 1999, pp. 215–237.

[3] Bender (E. A.), Gao (Z.), and Richmond (L. B.). – Submaps of maps. I. General 0-1 laws. *Journal of Combinatorial Theory. Series B*, vol. 55, n° 1, 1992, pp. 104–117.

[4] Bender (E. A.), Gao (Z.), and Richmond (L. B.). – Almost all rooted maps have large representativity. *Journal of Graph Theory*, vol. 18, n° 6, 1994, pp. 545–555.

[5] Bender (E. A.), Gao (Z.), Richmond (L. B.), and Wormald (N. C.). – Asymptotic properties of rooted 3-connected maps on surfaces. *Australian Mathematical Society. Journal. Series A. Pure Mathematics and Statistics*, vol. 60, n° 1, 1996, pp. 31–41.

[6] Bender (E. A.) and Richmond (L. B.). – Submaps of maps. III. k-connected nonplanar maps. *Journal of Combinatorial Theory. Series B*, vol. 55, n° 1, 1992, pp. 125–132.

[7] Gao (Z.). – A pattern for the asymptotic number of rooted maps on surfaces. *Journal of Combinatorial Theory. Series A*, vol. 64, n° 2, 1993, pp. 246–264.

[8] Richmond (L. B.) and Wormald (N. C.). – Almost all maps are asymmetric. *Journal of Combinatorial Theory. Series B*, vol. 63, n° 1, 1995, pp. 1–7.

[9] Tutte (W. T.). – *Graph theory*. – Addison-Wesley Publishing Co., Reading, Mass., 1984, *Encyclopedia of Mathematics and its Applications*, vol. 21, xxi+333p. With a foreword by C. St. J. A. Nash-Williams.

Loop-Erased Random Walks

Richard Kenyon
Université de Paris-Sud

May 31, 1999

[summary by Cyril Banderier]

Abstract

The loop-erased random walk is the simple curve obtained by removing in the chronological order the loops of the original random walk. A basic aspect of these walks in $\mathbb{Z}^2$ is studied: its average length (thus solving a conjecture of Guttmann). The techniques are combinatorial and use a bijection due to Temperley between maximal trees and perfect coupling.

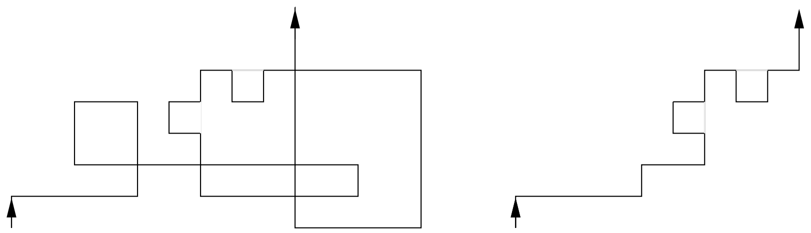


FIGURE 1. A random walk and its associated LERW

1. LERW=ST=DT

This is not a new equality between new complexity classes but it simply emphasizes the fact that loop-erased random walk (LERW), spanning tree (ST) and domino tiling (DT) are essentially the same object.

Indeed, in [12] shows that, for a uniformly chosen spanning tree on a region of $\mathbb{Z}^2$, the unique arc (branch) between two points has the same distribution as the LERW between these two points. Moreover, Temperley [13] gives a constructive one-to-one correspondence between spanning trees and domino tilings.

From the other talk of Richard Kenyon, we know that domino tiling (the so-called two dimensional lattice dimer model, a model which has some ties with Ising model) is the only nontypical *ad hoc* statistical physical model where conformal invariance is proved, so representations of the Virasoro algebra [15] could help finding critical exponents.

In order to solve this "self-avoiding walk model" (*i.e.*, to set the critical exponent), R. Kenyon does not use representation theory, but a "discrete Laplacian", from which he gets the full asymptotics. Whereas a lot is known about properties of the continuous Laplacian [5], works on the discrete Laplacian are more recent [10].

As conjectured by Bursill and Guttmann [4], the exponent for LERW is 5/4. Richard Kenyon proves this by applying the "equality" LEWR=ST on the following theorem

Theorem 1. *On the uniform spanning tree process on $\mathbb{N}\times\mathbb{Z}$, the expected number of vertices on the arc from $(0,0)$ to ∞ which lie within distance N of the origin is $N^{5/4+o(1)}$.*

The next theorem is sometimes attributed to Kirschoff [11] and proven in [1].

Theorem 2 (Matrix-tree Theorem)**.** *For a graph G with set of vertices $\{v_i\}$, let*

$$\Delta := \begin{pmatrix} \deg(v_1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \deg(v_n) \end{pmatrix} - \mathrm{Adj}(G),$$

then the number of spanning trees of G is the product of the nonzero eigenvalues of Δ divided by the size of G. For an $m\times n$ rectangle, the number of spanning trees is thus

$$\prod_{\substack{(j,k)\neq 0\\ j=0,\dots,m-1\\ k=0,\dots,n-1}} \left(4-2\cos(\frac{\pi k}{n})-2\cos(\frac{\pi j}{m})\right).$$

It is possible to extend this kind of result to a class of polygons which are decomposable in rectangles, the so-called Temperleyan polyominoes. (Triangulations are also a way, as there is a determinant-like expression for triangles.)

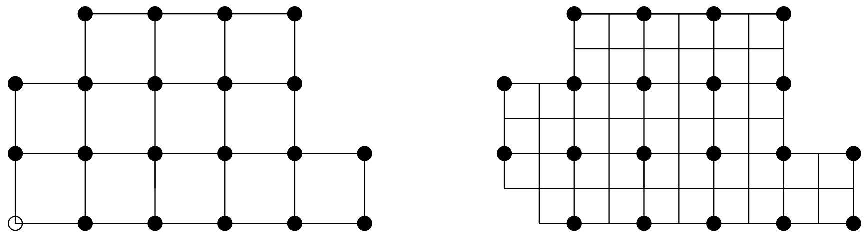


FIGURE 2. A graph and its associated Temperleyan polyomino

The number of spanning trees of the graph is the number of domino tilings of its Temperleyan polyomino. Taking the log in the previous formula gives a special case of the following theorem:

Theorem 3. *Let $U\subset\mathbb{R}^2$ be a rectilinear polygon with V vertices. For each $\epsilon>0$, let P_ϵ be a Temperleyan polyomino in $\epsilon\mathbb{Z}^2$ approximating U in the natural sense (the corners of p_ϵ are converging to the corners of U). Let A_ϵ be the area and* Perim_ϵ *be the perimeter of P_ϵ. Then the log of the number of domino tilings of P_ϵ is*

$$\frac{c_0 A_\epsilon}{\epsilon^2}+\frac{c_1\,\mathrm{Perim}_\epsilon}{\epsilon}+O(\log(\epsilon))$$

where $c_0=\frac{G}{\pi}$, $G=1-\frac{1}{3^2}+\frac{1}{5^2}-\cdots$ is Catalan's constant, $c_1=\frac{G}{2\pi}+\frac{\log(\sqrt{2}-1)}{4}$.

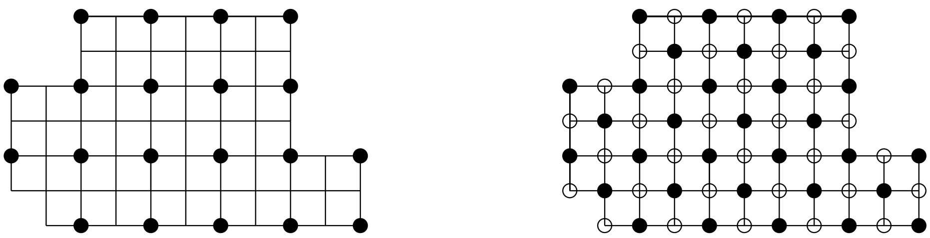
According to the author, "Part of the motivation for the above theorem is to validate a certain heuristic, which attempts to explain how the presence of the boundary affects the long-range structure of a random tiling. In particular it attempts to explain how the boundary affects the densities of local configurations far from the boundary [3]. This heuristic is called the 'phason strain' principle. The heuristic is as follows: The boundary causes the *average height function* of a tiling to deviate slightly from its entropy-maximizing value of 0. At a point in the region where the average height function has nonzero slope, the "local" entropy there is smaller than the maximal possible entropy, by an amount proportional to the square of the gradient of the average height function.

The system behaves in such a way as to maximise the total entropy subject to the given boundary values of the height function, and the resulting average height function is the function which minimises the (integral of) the square gradient. That is, the average height function is harmonic."

Anyway an exact application of the phason strain principle gives in fact slightly different asymptotics (from the one given in the theorem 3), so this principle is not totally valid here, but however it gives a good approximation.

2. **Height Function**

For a given tiling, the height function h is easily defined [14] by bicolouring the Temperleyan polyomino (there are no adjacent vertices of the same colour):



then, for each oriented edge AB on the border of a domino,

$$h(A) - h(B) := \begin{cases} +1 & \text{if the square on the left of } AB \text{ is black,} \\ -1 & \text{otherwise.} \end{cases}$$

Note that, up to an arbitrary additive constant, the height of the boundary is independent of the tiling.

For a smaller and smaller lattice (e.g., $\epsilon\mathbb{Z}^2$), one can approximate any domain U of $\mathbb{C}$. For a very fine lattice (in fact, taking the limit when $\epsilon \to 0$), one can study the probability of appearance in the tiling of some patterns, their repartition in the tiling and also how the shape of the boundary influences the tiling. It appears that there are links with conformal theory, as explained below.

Let P_ϵ be a Temperleyan polyomino associated to a rectilinear polygon U of $\mathbb{C}$. Now, let h_ϵ be the average height function of P_ϵ, that is the average height over all domino tilings of P_ϵ and then define

$$h(x) := \lim_{\epsilon \to 0} h_\epsilon(x_\epsilon).$$

For $x \in \partial U$, $h(x)$ is defined by continuity from values of h in the interior.

The remarkable fact is that this limiting average height function h can be expressed as

$$h(v) = \frac{4}{\pi} \Im \int_{b_0}^{v} \lim_{z \to v} \left(F_+(v,z) - \frac{2}{\pi(z-v)} \right) du = -\frac{2}{\pi} \Im \log \wp'(z),$$

where $\wp$ is the Weierstrass elliptic function and where $F_+(u,z)\,du$ is a meromorphic 1-form, thus allowing some links with conformal mapping theory. We refer to "Conformal invariance of domino tiling" (1997) and to "The asymptotic determinant of the discrete Laplacian" (1999) for further informations[1].

[1] Like other recent preprints of the author, they are available at his home page
`http://topo.math.u-psud.fr/~kenyon/`

Bibliography

[1] Brooks (R. L.), Smith (C. A. B.), Stone (A. H.), and Tutte (W. T.). – The dissection of rectangles into squares. *Duke Mathematical Journal*, vol. 7, 1940, pp. 312–340.

[2] Burton (Robert) and Pemantle (Robin). – Local characteristics, entropy and limit theorems for spanning trees and domino tilings via transfer-impedances. *The Annals of Probability*, vol. 21, n° 3, 1993, pp. 1329–1371.

[3] Destainville (N.), Mosseri (R.), and Bailly (F.). – Configurational entropy of codimension-one tilings and directed membranes. *Journal of Statistical Physics*, vol. 87, n° 3-4, 1997, pp. 697–754.

[4] Guttmann (A.) and Bursill (R.). – Critical exponent for the loop-erased self-avoiding walk by Monte-Carlo methods. *Journal of Statistical Physics*, vol. 59, 1990, pp. 1–9.

[5] Kac (Mark). – Can one hear the shape of a drum? *American Mathematical Monthly*, vol. 73, n° 4, part II, 1966, pp. 1–23.

[6] Kenyon (Richard). – Rigidity of planar tilings. *Inventiones Mathematicae*, vol. 107, n° 3, 1992, pp. 637–651.

[7] Kenyon (Richard). – Tiling a polygon with parallelograms. *Algorithmica*, vol. 9, n° 4, 1993, pp. 382–397.

[8] Kenyon (Richard). – Local statistics of lattice dimers. *Annales de l'Institut Henri Poincaré. Probabilités et Statistiques*, vol. 33, n° 5, 1997, pp. 591–618.

[9] Kenyon (Richard). – Tilings of convex polygons. *Annales de l'Institut Fourier*, vol. 47, n° 3, 1997, pp. 929–944.

[10] Kenyon (Richard). – Tilings and discrete Dirichlet problems. *Israel Journal of Mathematics*, vol. 105, 1998, pp. 61–84.

[11] Kirchhoff (G.). – Über die Auflösung der Gleichungen, auf welche man bei der Untersuchung der linearen Verteilung galvanischer Ströme geführt wird. *Annalen für der Physik und der Chemie*, vol. 72, 1847, pp. 497–508.

[12] Pemantle (Robin). – Choosing a spanning tree for the integer lattice uniformly. *The Annals of Probability*, vol. 19, n° 4, 1991, pp. 1559–1574.

[13] Temperley (H. N. V.). – Enumeration of graphs on a large periodic lattice. In *Combinatorics. London Mathematical Society Lecture Note Series*, pp. 155–159. – Cambridge University Press, 1974. Proceedings of the British Combinatorial Conference, University College, Wales, Aberystwyth, 1973.

[14] Thurston (William P.). – Conway's tiling groups. *The American Mathematical Monthly*, vol. 97, n° 8, 1990, pp. 757–773.

[15] Virasoro (M. A.). – *Physical Review D. (3)*, 1970, pp. 2933–2936.

The Local Limit Theorem for Random Walks on Free Groups

Steve Lalley
Purdue University

May 31, 1999

[summary by Cyril Banderier]

Abstract

Local limit theorems and saddlepoint approximations are given for random walks on a free group whose step distributions have finite support. These are derived by exploiting a set of algebraic relations among certain generating functions that arise naturally in connection with the transition probabilities of the random walks. Basic tools involved in the analysis are the elementary theory of algebraic functions, the Perron-Frobenius theory of nonnegative matrices, and standard techniques of singularity analysis.

1. Walks on Groups

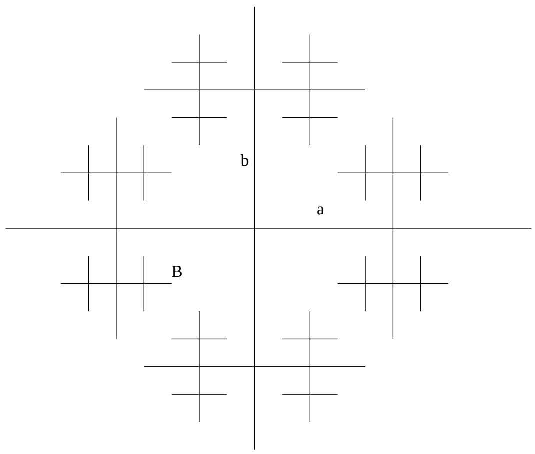


FIGURE 1. A representation (Cayley graph) of the infinite free group $\mathbb{Z} \star \mathbb{Z}$

Let $\mathbb{G}$ be a the free group with generators $a_1, \ldots, a_L$. For example, the free group $\mathbb{Z} \star \mathbb{Z}$ has two generators a and b. The word $aba\bar{a}\bar{b}\bar{a}\bar{a}\bar{b}aa$ corresponds to the point B, the associated reduced word is $\bar{a}\bar{b}aa$.

A finite-range random walk $\{Z_n\}_{n\geq 0}$ is a Markov chain on $\mathbb{G}$ with $Z_0 := e$ (the identity of the group, the "origin", the starting point) and transition probabilities

$$\Pr\{Z_{n+1} = yx | Z_n = y\} = p_x \qquad \forall x, y \in \mathbb{G}, n \geq 0,$$

where p_x for $x \in \mathbb{G}$ is a probability distribution with finite support (in other words, p_x is the probability of the "jump" x).

Note $p^{*n}(x)$ the probability of being in x after n steps. It is assumed that the random walk is irreducible and aperiodic, that is, that

$$\forall x \in \mathbb{G} \qquad \sum_{n\geq 1} p^{*n}(x) > 0 \qquad \text{(irreducibility);}$$
$$\mathrm{GCD}\{n; p^{*n}(e) > 0\} = 1 \qquad \text{(aperiodicity).}$$

Another important condition is the following:

Positivity: $\quad p_e > 0$ and $p_g > 0$ for all generators g of $\mathbb{G}$ (and their inverses).

Similarly to the random walk in the Euclidian case $\mathbb{Z}^d$, a local limit theorem is given by the asymptotics

$$p^{*n}(x) \sim \frac{B_x R^{-n}}{\sqrt{2\pi R} n^{3/2}}.$$

Similar results were already known when all the steps are of size one (*nearest neighbour* random walk [3]) or when all the words at a same distance from the origin are equiprobable (the so-called *isotropic* random walk [2, 8, 9]).

2. **Singularity Analysis**

This section is devoted to the analysis of some probability generating functions (PGF) related to the walk. For $x \in \mathbb{G}$ and $z \in \mathbb{C}$ ($|z| < 1$), define

- the random variable coding where one is after n steps: Z_n,
- the PGF to reach x in n steps: $G_x(z) := \sum_n p^{*n}(x) z^n$,
- the PGF of the excursions (Green's function): $G(z) := G_e(z)$,
- the first time x is reached: $T_x := \inf\{n \geq 0 : Z_n = x\}$,
- the PGF to reach x for the first time in n steps: $F_x(z) := \sum_n \Pr\{T_x = n\} z^n$.

Note that aperiodicity and irreducibility imply that for all sufficiently large $n \geq 1$, $p^{*n}(e) > 0$ and $p^{*n}(y) > 0$, for any (inverse of a) generator y.

The following (combinatorially trivial) relations

$$G_x(z) = F_x(z) G(x),$$

$$G(z) = 1 + z\left(p_e + \sum_{x\neq e} p_x F_{x^{-1}}(z)\right) G(z) = \left(1 - zp_e - z\sum_{x\neq e} p_x F_{x^{-1}}(z)\right)^{-1}$$

allow to prove that all of the functions F_x and G_x have the same radius of convergence R, $1 < R < \infty$ (the less obvious is that R is *strictly* greater than 1).

Let $\mathbb{B}$ be the set of points at distance $\leq K$, where K is such that there is no smaller ball in which the support of the step distribution $\{p_x\}$ is contained. Define now

- the first time that x is exceeded: τ_x
- the PGF to go from a to xb while x as never been exceeded before:

$$H_x^{ab} = \sum_n \Pr\{Z_n = xb | Z_0 = a \text{ and } Z_{i<n} \notin x\mathbb{B}\} z^n$$

- the PGF to go from x to the origin: $F_{x^{-1}}(z)$

The formula

$$\forall x \neq e \qquad F_x(z) = \sum_{b \in \mathbb{B}-\{e\}} H_x^{eb}(z) F_{b^{-1}}(z)$$

leads to an expression of $F_x = uH_x(z)v = uH_{x_1}(z)\cdots H_{x_m}(z)v$ where u is the projection on e and v a vector whose entries are the $F_{b^{-1}}(z)$ for $b \in \mathbb{B}$ and where the product of matrices is over $x_1 \cdots x_m$, the reduced word associated to x.

It is then proven by the Markov property that all the non-constant $H_{x_i}^{ab}$ satisfy polynomial relations ($H_{x_i} = Q_i(H_{x_1}, H_{x_2}, \dots)$, see [6] for exact relations) and that they have the same radius of convergence.

By elimination (Gröbner basis or resultants), the functions F_x and G_x are algebraic. Their Puiseux expansion leads to an algebraic singularity with exponent $1/2$.

Here is a sketch of the proof that the exponent is indeed $\alpha = 1/2$. Define J_z the Jacobian matrix $\left(\partial Q_i / \partial H_{x_j}\right)$, the polynomials Q_i have nonnegative coefficients, thus there exists n such that J_z^n is an aperiodic and irreducible matrix with strictly positive coefficients. By the Perron-Frobenius theorem, J_z has a positive eigenvalue λ_z of multiplicity 1. The function λ_z is increasing and real-analytic and $\lambda_R = 1/R$. Considering a left eigenvector of J_R and using the shape of the Q_i yields to the relations $(R-z)(C+\cdots) = C'(R-z)^{2\alpha} + \cdots$, thus $2\alpha = 1$.

As $z = R$ is the dominant singularity of F_x and G_x, one has the two following theorems:

Theorem 1 (Local limit theorem, access)**.** *Assuming irreducibility and aperiodicity, one has, for a positive constant B_x:*

$$p^{*n}(x) \sim \frac{B_x}{\sqrt{2\pi R} R^n n^{3/2}}.$$

Theorem 2 (Local limit theorem, first access)**.** *Assuming positivity, one has, for a positive constant A_x:*

$$\Pr\{x \textit{ is reached for the first time after } n \textit{ steps}\} \sim \frac{A_x}{\sqrt{2\pi R} R^n n^{3/2}}.$$

3. Saddlepoint Approximations

The probability to reach a point x at a distance m of the origin in n steps is

$$p^{*n}(x) \sim \frac{\exp(n\beta(m/n))}{\sqrt{\ddot{\psi}(m/n)}} C(m/n)$$

for appropriate functions β, C and $\ddot{\psi}$ (see the correct definitions / notations in [6]).

This uniform asymptotics in x and n corresponds to the classical saddlepoint approximation (sharp large deviations theorems) for sums of iid random vectors in $\mathbb{R}^d$.

The saddlepoint approximations are of interest for another reason. For large n, nearly all the mass in the probability distribution $p^{*n}(x)$ is concentrated in the region $|x| \geq \epsilon n$, where the local limit approximations are not accurate. This contrasts with the situation for finite range random walk in Euclidean space. In fact, Guivarch [4] has shown that for random walks in $\mathbb{G}$, the distance from the origin grows linearly in n. Sawyer and Steger [10] have further shown that $(|Z_n| - n\beta)/\sqrt{n}$ converges in law to a normal distribution.

Finally, S. Lalley, using a special matrix product and results on Ruelle's Perron-Frobenius operators, derives a saddlepoint approximation, uniformly for m/n in a given compact

$$\Pr\{|Z_n| = m\} \sim \frac{\exp(nB(m/n))}{\sqrt{2\pi m D(m/n)}} C(m/n).$$

Bibliography

[1] Cartwright (Donald I.) and Sawyer (Stanley). – The Martin boundary for general isotropic random walks in a tree. *Journal of Theoretical Probability*, vol. 4, n° 1, 1991, pp. 111–136.

[2] Figà-Talamanca (Alessandro) and Picardello (Massimo A.). – *Harmonic analysis on free groups.* – Marcel Dekker Inc., New York, 1983, viii+145p.

[3] Gerl (Peter) and Woess (Wolfgang). – Local limits and harmonic functions for nonisotropic random walks on free groups. *Probability Theory and Related Fields*, vol. 71, n° 3, 1986, pp. 341–355.

[4] Guivarc'h (Y.). – Sur la loi des grands nombres et le rayon spectral d'une marche aléatoire. In *Conference on Random Walks (Kleebach, 1979)*, pp. 47–98, 3. – Société Mathématique de France, Paris, 1980.

[5] Lalley (Steven P.). – Saddle-point approximations and space-time Martin boundary for nearest-neighbor random walk on a homogeneous tree. *Journal of Theoretical Probability*, vol. 4, n° 4, 1991, pp. 701–723.

[6] Lalley (Steven P.). – Finite range random walk on free groups and homogeneous trees. *The Annals of Probability*, vol. 21, n° 4, 1993, pp. 2087–2130.

[7] Lalley (Steven P.) and Hueter (Irene). – Anisotropic branching random walks on homogeneous trees. *Preprint*, 1999.

[8] Picardello (Massimo A.). – Spherical functions and local limit theorems on free groups. *Annali di Matematica Pura ed Applicata. Serie Quarta*, vol. 133, 1983, pp. 177–191.

[9] Sawyer (Stanley). – Isotropic random walks in a tree. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 42, n° 4, 1978, pp. 279–292.

[10] Sawyer (Stanley) and Steger (Tim). – The rate of escape for anisotropic random walks in a tree. *Probability Theory and Related Fields*, vol. 76, n° 2, 1987, pp. 207–230.

[11] Seneta (E.). – *Nonnegative matrices and Markov chains.* – Springer-Verlag, New York, 1981, second edition, xiii+279p.

Limit Shape Theorems for Partitions

Anatoly Vershik
IHES, Bures-sur-Yvette

March 8, 1999

[summary by Sylvie Corteel]

Abstract

Many combinatorial and geometrical problems can be reduced to a problem about partitions of natural numbers or vectors, etc. The main asymptotic question is the behaviour of the shape of such a partition when the statistics or dynamics are fixed. This leads us to the problem of limit shapes. Example: what is the typical limit shape of the uniformly distributed partition of the integers? An explicit answer can be given.

A partition of a nonnegative integer n is a sequence $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_N)$ such that $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N \geq 1$, $n(\lambda) = \sum_{i=1}^{N} \lambda_i = n$. The λ_i's are the summands of the partitions. Let $\mathcal{P}_n$ denote the set of all partitions of the integer n and $\mathcal{Q}_n$ the set of partitions of the integer n with distinct summands. Let $r_k(\lambda)$ be the multiplicity of the summand k, that is $r_k(\lambda) = \#\{j \mid \lambda_j = k\}$. Clearly, $n(\lambda) = \sum_k k r_k(\lambda)$ and $N(\lambda) = \sum_k r_k(\lambda)$. Recall that $\#\mathcal{P}_n = p(n)$ is the Euler function and the generating function $\sum_n p(n)x^n$ is $\prod_{i\geq 1}(1-q^i)^{-1}$. The author associates a function φ_λ on $[0,\infty)$ with the partition $\lambda \in \mathcal{P}_n$ by the following rule:

$$\varphi_\lambda(t) = \sum_{k\geq t} r_k(\lambda)$$

φ_λ is a step function, continuous on the right and $\int_0^\infty \varphi_\lambda(t) = n$. Let $a = \{a_n\}_{n\geq 0}$ with $a_n > 0$ for all n; the function

$$\tilde{\varphi}_\lambda(t) = \frac{a_n}{n} \sum_{k\geq a_n t} r_k(\lambda) = \frac{a_n}{n}\varphi_\lambda(a_n t)$$

is φ_λ normed by a_n, so that $\int_0^\infty \tilde{\varphi}_\lambda(t) = 1$.

Let μ^n be the uniform measure on the set $\mathcal{P}_n$ of all partitions of the integer $n : \mu^n(\lambda) = p(n)^{-1}$, $\lambda \in \mathcal{P}_n$; the question is whether one can normalize the partitions in such a way that, in some properly chosen space, the measures μ^n have a weak limit on generalized diagrams, and whether this limit is singular. In the last case, the limit measure is concentrated on a limit shape. An affirmative answer to these questions, as well as explicit formulas for limit shapes, are given in the sequel.

Theorem 1. *The scaling $a = \{a_n\}$ for the uniform measure on $\mathcal{P}_n$ such that a non trivial limit exists in the space of generalized diagrams is $a_n = \sqrt{n}$.*

The same scaling is appropriate for the uniform measure on $\mathcal{Q}_n$.

Theorem 2. *Under the previous scaling, the measures μ^n have a weak limit. This limit is singular and concentrated on a continuous curve.*

The limit shape of the uniformly distributed ordinary partitions and partitions into distinct summands can now be stated.

Theorem 3. *For any $\epsilon > 0$, $0 < x, y < \infty$, there exists n_0 such that for all $n > n_0$*

$$\mu^n\{\lambda \in \mathcal{P}_n \mid \sup_{t\in[x,y]} |\tilde{\varphi}_\lambda(t) - C(t)| < \epsilon\} > 1 - \epsilon,$$

where $C(t) = -(\sqrt{6}/\pi)\ln(1 - e^{\pi t/\sqrt{6}})$, or in more symmetric form

$$e^{-\pi x/\sqrt{6}} + e^{-\pi y/\sqrt{6}} = 1.$$

Theorem 4. *For any $\epsilon > 0$, $0 < x, y < \infty$, there exists n_0 such that for all $n > n_0$*

$$\mu^n\{\lambda \in \mathcal{Q}_n \mid \sup_{t\in[x,y]} |\tilde{\varphi}_\lambda(t) - C(t)| < \epsilon\} > 1 - \epsilon,$$

where $C(t) = -(\sqrt{12}/\pi)\ln(1 + e^{-\pi t/\sqrt{12}})$, or in more symmetric form

$$e^{-\pi y/\sqrt{12}} - e^{-\pi x/\sqrt{12}} = 1.$$

The limit shape can also be obtained for the uniform measure on partitions included in a rectangle, partitions with a given number of summands, vector partitions, ... and other kinds of measures called *multiplicative measures.* The detailed results and links with statistical mechanics are presented in [2].

Bibliography

[1] Andrews (George E.). – *The theory of partitions.* – Addison-Wesley Publishing Co., Reading, Mass., 1976, *Encyclopedia of Mathematics and its Applications*, vol. 2, xiv+255p.

[2] Vershik (A. M.). – Statistical mechanics of combinatorial partitions, and their limit configurations. *Rossiĭskaya Akademiya Nauk. Funktsional'nyĭ Analiz i ego Prilozheniya*, vol. 30, n° 2, 1996.

Asymptotic Combinatorics and Representations of Infinite Symmetric Groups (a Survey)

Anatoly Vershik
IHES, Bures-sur-Yvette

March 8, 1999

[summary by Philippe Chassaing]

Introduction: Multiplicative Measures

In a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ of a nonnegative integer $n = n(\lambda) = \sum_{i=1}^{N} \lambda_i$, the summands λ_i are in decreasing order, and $r_k(\lambda)$ denotes the multiplicity of k, i.e. $r_k(\lambda) = \#\{j | \lambda_j = k\}$. Let $\mathcal{P}_n$ denote the set of partitions of the integer n, and set $\mathcal{P} = \cup_n \mathcal{P}_n$.

One of the questions addressed by this talk is to scale the associated Young diagram $\varphi_\lambda(t)$ defined on $[0, +\infty]$ by

$$\varphi_\lambda(t) = \sum_{k \geq t} r_k(\lambda)$$

in order to obtain nontrivial limit shapes, for the family of *multiplicative measures* on $\mathcal{P}$. A multiplicative measure on $\mathcal{P}$ is defined by a sequence $(\mathcal{F}_k)_{k \geq 1}$ of generating functions

$$\mathcal{F}_k(x) = \sum_{r \geq 0} s_k(r) x^r,$$

as follows: it defines a measure μ^n on $\mathcal{P}_n$ through

$$\mu^n(\lambda) = Q_n^{-1} \prod_k s_k(r_k(\lambda)) = Q_n^{-1} F(\lambda),$$

in which Q_n is chosen so that μ^n is a probability measure on $\mathcal{P}_n$. Assuming that the series

$$\mathcal{F}(x) = \sum_{n \geq 0} Q_n x^n$$

converges for $x \in [0, x_0)$, a probability measure μ_x is then defined on $\mathcal{P}$ as follows:

$$\mu_x = \frac{\sum_n Q_n x^n \mu^n}{\mathcal{F}(x)}.$$

One derives the following facts easily:

- $\mathcal{F}(x) = \prod_{k \geq 1} \mathcal{F}_k(x^k)$;
- according to the measure μ_x, the r_k's are independent random variables;
- the conditional law of a partition λ, given that $\lambda \in \mathcal{P}_n$, is μ^n.

Though the Plancherel measure does not fall in the class of multiplicative measures, most important ones do belong to it.

1. Examples

– *Uniform statistics on $\mathcal{P}_n$.* Let $\mu^n(\lambda) = p(n)^{-1}$, in which $p(n) = \#\mathcal{P}_n$ is the Euler function, $\mathcal{F}_k(x) = 1/(1-x)$ does not depend on k, and as expected:

$$\mathcal{F}(x) = \prod_{k \geq 1} \frac{1}{1-x^k};$$

– *Uniform statistics on partitions with different summands.* $\mathcal{F}_k(x) = 1 + x$, giving

$$\mu_x(\lambda) = x^{n(\lambda)} \prod_{k=1}^{+\infty} (1 + x^k)^{-1};$$

– *Bell's statistics.* Here μ^n can be seen as the law of the projection on $\mathcal{P}_n$ of a random partition of a set with n elements, giving:

$$\mu^n(\lambda) = \frac{1}{\prod_k r_k(\lambda)!(k!)^{r_k(\lambda)}}, \qquad \mathcal{F}_k(x) = e^{y/k!}, \qquad \mathcal{F}(x) = e^{e^x - 1};$$

– *Haar's statistics and Poisson-Dirichlet measures.* This example is a family $\mu_{x,\theta}$ of multiplicative measures. The case $\theta = 1$ is the partition structure derived from the cycles of a random permutation. The general case arises in various applications in graph theory, or also in genetics under the name of Ewens sampling formula:

$$\mu_\theta^n(\lambda) = \frac{\theta^{\#\lambda}}{[\theta]^{n(\lambda)} \prod_k r_k(\lambda)! k^{r_k(\lambda)}}, \qquad \mathcal{F}_k(x) = e^{\theta y/k}, \qquad \mathcal{F}(x) = (1-x)^{-\theta},$$

in which $\#\lambda$ stands for the number of summands of λ, and $[\theta]^n = \theta(\theta+1)\cdots(\theta+n-1)$.

2. Limit Shapes and Scaling

For a sequence $a = (a_n)_{n \geq 0}$, let $\tau_a \lambda$ denote the scaled Young diagram $t \mapsto a_{n(\lambda)} \varphi_\lambda(a_{n(\lambda)} t)/n(\lambda)$, and for any measure μ on $\mathcal{P}$, let $\tau_a \mu$ denote the image of μ under τ_a. Ergodicity occurs when there exists a normalizing sequence a, such that $\tau_a \mu^n$ converges weakly to a Dirac mass at a given limit shape. The Plancherel measure, as well as the first cases above, are ergodic, but not the last case, where the weak limit is nondegenerate, and can be expressed in terms of the Poisson-Dirichlet distribution with parameter θ. Among the possible tools, a method analog to the saddle-point method allows to derive convergence of $\tau_a \mu^n$ when $n \to +\infty$ from the convergence of $\tau_a \mu_x$ when $x \to x_0$, the latter convergence being easier to prove owing to the independence of r_k's.

The author also developed on heap problems, roof and entropy, on the Young graph, Kingman problem (partition structures), Ulam problem (length of the longest increasing sequence in a sequence of n numbers) and its connection with the spectrum of Gaussian matrices.

Bibliography

[1] Vershik (A. M.). – Statistical mechanics of combinatorial partitions, and their limit configurations. *Rossiĭskaya Akademiya Nauk. Funktsional'nyĭ Analiz i ego Prilozheniya*, vol. 30, n° 2, 1996, pp. 19–39.

[2] Vershik (Anatoly M.). – Asymptotic combinatorics and algebraic analysis. In *Proceedings of the International Congress of Mathematicians (Zürich, 1994)*. pp. 1384–1394. – Birkhäuser, Basel, 1995.

Exact Largest and Smallest Size of Components in Decomposable Structures

Daniel Panario

University of Toronto

June 21st, 1999

[summary by Bruno Salvy]

Abstract

In [2], the number of permutations of n objects with largest cycle length equal to k is studied in detail. The purpose of [3] which is summarized here is to show that these results generalize in a straightforward manner to all labelled sets, unlabelled sets and unlabelled powersets.

Sets are a basic combinatorial construction. Many properties of general structures are direct consequences of their being sets. Special cases of sets are: graphs of various kinds (sets of connected components), permutations (sets of cycles), polynomials over finite fields (sets of factors). In all those cases, the statistics of the largest and smallest component are related to the complexity of algorithms operating over these structures. Very explicit results concerning these statistics can be obtained by extracting coefficients from the proper generating functions, which in this case is a refined way of performing an inclusion-exclusion argument.

The study is based on three generating functions corresponding to three different ways of considering sets, depending on whether the atomic objects (those of size 1) are labelled or unlabelled and on whether repetitions are allowed or not in sets (in the unlabelled case). Let $C(z)$ be the generating function of the objects of which a set is being made (ordinary in the unlabelled case and exponential in the labelled case):

$$C(z) = \sum_{n\geq 0} c_n z^n \quad \text{or} \quad C(z) = \sum_{n\geq 0} c_n \frac{z^n}{n!},$$

where c_n is the number of objects of size n and it is assumed that $c_0 = 0$ so that the enumeration is well-defined. Then the generating functions under study are

$$\begin{aligned} L(z) &= \exp(C(z)) =: \sum_n l_n \frac{z^n}{n!}, \\ P(z) &= \exp\left(C(z) - C(z^2)/2 + C(z^3)/3 - \cdots\right), \\ S(z) &= \exp\left(C(z) + C(z^2)/2 + C(z^3)/3 + \cdots\right), \end{aligned}$$

$L(z)$ is the exponential generating function in the labelled case, $P(z)$ and $S(z)$ are the ordinary generating functions in the unlabelled case, with repetitions allowed for S and forbidden for P. These equations and their derivations are classical, see for instance [1].

Setting all the c_n to 0 for $n > k$ leads to formulæ for sets whose largest component has size at most k. Similarly, setting all the c_n to 0 for $n < k$ yields formulæ for sets whose smallest component has size at least k. Taking the difference between largest size at most k and largest size at most $k-1$

gives the formulæ for largest size exactly k, and similarly for the smallest size. The corresponding generating functions will be denoted $L_k^\ell(z)$, $L_k^s(z)$, $P_k^\ell(z)$, ... Thus for instance

$$L_k^\ell(z) = \exp\left(\sum_{m=0}^{k-1} \frac{c_m z^m}{m!}\right)(e^{c_k z^k/k!} - 1) = (e^{c_k z^k/k!} - 1)L(z)\exp\left(-\sum_{m\geq k} \frac{c_m z^m}{m!}\right). \tag{1}$$

The simultaneous study of the number of components in the set is achieved by changing C into uC for a new variable u, which leads to bivariate generating functions the coefficient of $u^k z^n$ of which is the number of sets of size n with k elements.

Various combinations of these techniques produce numerous results. We exemplify the ideas in the labelled case below. The procedure is the same in the unlabelled case and the results are slightly more complicated.

Expanding the first exponential in (1) and extracting the coefficient of z^n yields

$$\begin{aligned}[z^n]L_k^\ell(z) &= \frac{c_k}{k!}\frac{l_{n-k}}{(n-k)!}, && n/2 < k \leq n\\ &= \frac{c_k}{k!}\left(\frac{l_{n-k}}{(n-k)!} + \frac{c_k}{2k!}\frac{l_{n-2k}}{(n-2k)!} - \sum_{m=k}^{n-2k}\frac{c_m}{m!}\frac{l_{n-m-k}}{(n-m-k)!}\right), && n/3 < k \leq n/2,\end{aligned}$$

and more and more complicated formulæ as more terms of the exponentials have to be taken into accounts. These formulæ generalize all of the results in [2], except one which is derived by noticing that $L = \sum_k L_k^\ell$ leading to a recurrence expressing $[z^n]L_k^\ell(z)$ in terms of the $[z^{n-ki}]L_j^\ell(z)$, $j \leq k-1$, $i \leq \lfloor n/k \rfloor$.

Formulæ involving the smallest component are derived in a similar manner from

$$L_k^s(z) = \exp\left(\sum_{m>k} \frac{c_m z^m}{m!}\right)(e^{c_k z^k/k!} - 1).$$

Extracting coefficients yields

$$\begin{aligned}[z^n]L_k^s(z) &= \frac{c_k}{k!}, && k = n,\\ &= 0, && n/2 < k < n,\\ &= \frac{c_k^2}{2k!^2}, && k = n/2,\\ &= \frac{c_k}{k!}\frac{c_{n-k}}{(n-k)!}, && n/3 < k < n/2, \ldots\end{aligned}$$

And again a recurrence formula can be derived. In all cases, an obvious inclusion-exclusion argument can be read off the formula.

Bibliography

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

[2] Golomb (Solomon W.) and Gaal (Peter). – On the number of permutations of n objects with greatest cycle length k. *Advances in Applied Mathematics*, vol. 20, n° 1, 1998, pp. 98–107.

[3] Panario (Daniel) and Richmond (Bruce). – Exact largest and smallest size of components in decomposable structures. – June 1999. Preprint.

Dimers in $\mathbb{Z}^2$

Richard Kenyon
Université de Paris-Sud

May 31, 1999

Abstract

Kasteleyn's theorem computes the number of perfect couplings of a planar graphs as a determinant. We extend this theorem to compute the densities of local configurations in a random coupling of a large area in $\mathbb{Z}^2$.

Bibliography

[1] Kenyon (Richard). – Dimères sur un réseau. – Preprint, 1998. Available at http://topo.math.u-psud.fr/~kenyon/preprints.html.

Part 2

Symbolic Computation

Polylogarithms and Multiple Zeta Values

Michel Petitot
University of Lille I

April 19, 1999

[summary by Bruno Salvy]

The *polylogarithm* is defined by the series

$$L_{x_0^{n_1-1}x_1\cdots x_0^{n_k-1}x_1}(z) := \sum_{n_1>\cdots>n_k>0} \frac{z^{n_1}}{n_1^{s_1}\cdots n_k^{s_k}}.$$

The convergence of this series at 1 is granted when $s_1 > 1$, and the limit is denoted $\zeta(s_1,\ldots,s_k)$ and is called a *multiple zeta value* since it extends the classical Riemann zeta function. The number $\sum s_i$ is called the *weight* of the polylogarithm or multiple zeta.

Many polynomial identities relating multiple zeta values at integers are known. For instance, reorganizing double sums yields the following identity between multiple zetas of weight 4:

$$\zeta(2,2) = \sum_{n_1>n_2>0} \frac{1}{n_1^2 n_2^2} = \frac{1}{2}\left(\sum_n \frac{1}{n^2}\right)^2 - \frac{1}{2}\sum_n \frac{1}{n^4} = \frac{1}{2}(\zeta(2)^2 - \zeta(4)). \tag{1}$$

This could be simplified further using the well-known values of ζ at even integers.

This is a very active and diverse area. The reader is encouraged to consult [1, 2] for surveys of many beautiful results, generalizations and conjectures. One of the most famous conjectures is the following.

Conjecture 1 (Zagier)**.** *The set of multiple zeta values $\zeta(s_1,\ldots,s_k)$ with s_i positive integers, $s_1 \geq 2$ and $s_1+\cdots+s_k \leq n$ generates a vector space over $\mathbb{Q}$ whose dimension d_n obeys*

$$d_{n+3} = d_{n+1} + d_n, \qquad d_1 = 0, \quad d_2 = d_3 = 1.$$

Note that since even the irrationality of $\zeta(5)$ is still unproven, this conjecture is completely out of reach. Even a proof that this sequence gives an upper bound is still to be found.

1. Shuffle and Stuffle

The manipulation leading to identity (1) is a special case of a more general mechanism involving products of multiple sums. By considering how indices in multiple sums can be reorganized, it is natural to define the *stuffle product* of two words over $\mathbb{N}$. (Stuffle is a contraction of "shuffle" and "stuff".) Using lowercase symbols to denote letters and capital symbols to denote words, this is the formal sum defined recursively by

$$\epsilon \star W = W \star \epsilon = W, \qquad aS \star bT = a(S \star bT) + b(aS \star T) + (a+b)(S \star T).$$

This definition is motivated by the following important *stuffle relation*:

$$\zeta(A)\zeta(B) = \sum_{S\in A\star B} \zeta(S).$$

A simple example is $\zeta(2)\zeta(3) = \zeta(2,3) + \zeta(3,2) + \zeta(5)$. Another one is the identity (1) which is obtained from $(2) \star (2) = 2(2,2) + 2(4)$.

In the same way as the stuffle product arises in the reorganization of multiple sums, multiple integrals lead to considering the *shuffle product* of words over the alphabet $X = \{x_0, x_1\}$. This is defined by the same formula as the stuffle product except that the last term in the sum is omitted. A bijection between words over $\mathbb{N}^\star$ and words of $X^\star x_1$ is provided by the encoding

$$(s_1, \dots, s_k) \leftrightarrow x_0^{s_1-1}x_1 \cdots x_0^{s_k-1}x_1.$$

This makes it possible to extend the shuffle product to these words. For instance,

$$(2) ш (2) \mapsto x_0x_1 ш x_0x_1 = 2x_0x_1x_0x_1 + 4x_0x_0x_1x_1 \mapsto 2(2,2) + 4(3,1),$$

$$(2) ш (3) \mapsto x_0x_1 ш x_0x_0x_1 = 6x_0^3x_1^2 + 3x_0^2x_1x_0x_1 + x_0x_1x_0^2x_1 \mapsto 6(4,1) + 3(3,2) + (2,3).$$

The following integral representation is then proved by induction

$$(2) \qquad L_{x_1}(z) = \log\frac{1}{1-z} = \int_0^z \frac{dt}{1-t}, \qquad L_w(z) = \begin{cases} \int_0^z \frac{dt}{t} L'_w(t), & \text{if } w = x_0w', \\ \int_0^z \frac{dt}{1-t} L'_w(t), & \text{if } w = x_1w'. \end{cases}$$

The recursive definition of the shuffle now reads $UV = \int U'V + \int UV'$, whence the *shuffle relation*:

$$L_A(z)L_B(z) = \sum_{S \in A \,ш\, B} L_S(z).$$

Setting $z = 1$ in these identities yields new identities concerning multiple ζ values. Our examples above thus lead to $\zeta(2)^2 = 2\zeta(2,2) + 4\zeta(3,1)$, $\zeta(2)\zeta(3) = 6\zeta(4,1) + 3\zeta(3,2) + \zeta(2,3)$.

Conjecture 2. *All known relations concerning multiple zeta values follow from the stuffle product of multiple zetas and the shuffle product of polylogarithms specialized at 1.*

This has been checked up to weight 12 [3], and the set of identities thus obtained coincides with the bound provided by Zagier's conjecture.

2. Monodromy and Consequences

A first step towards proving the conjecture above is provided by the following theorem.

Theorem 1 ([4])**.** *The ideal of algebraic relations between polylogarithms at z is generated by the shuffle relations.*

A *Lyndon word* is a non-empty word which precedes its strict right factors in the lexicographic order. A classical theorem due to Radford states that the Lyndon words form a basis of the shuffle algebra. This leads to the following result.

Corollary 1. *The polylogarithms indexed by Lyndon words form a transcendence basis of the polylogarithms. In particular, the classical polylogarithms $\mathrm{Li}_k = L_{x_0^k x_1}$ are algebraically independent.*

This theorem is proved for relations involving polylogarithms of weight bounded by a fixed number. Using the shuffle relations, any polynomial in polylogarithms can be reduced to a linear combination of polylogarithms. Since the shuffle relations form a Gröbner basis for the total degree order (degrevlex), any polynomial which is not in the ideal is thus reduced to a *nonzero* linear combination. The theorem is thus reduced to proving that the polylogarithms are *linearly* independent. This is done by computing the monodromy of polylogarithms as we now describe.

It turns out to be convenient to prove a more general theorem where polylogarithms with indices ending in x_0 are allowed. Consistency with the shuffle relations is achieved with

$$L_{x_0}(z) := \int_1^z \frac{dt}{t} = \log z, \qquad L_{x_0^m}(z) := \int_1^z \frac{dt}{t} L_{x_0^{m-1}}(t) = \frac{1}{m!}\log^m z.$$

At $z=0$, the situation is simple: a word ending with x_1 corresponds to an analytic polylogarithm, whence a trivial monodromy. An easy induction on the weight shows that all words ending in x_0 can be rewritten as a sum of shuffles of powers of x_0 and words ending in x_1. Here are the corresponding relations up to weight 3:

$$L_{x_1x_0} = L_{x_1}L_{x_0} - L_{x_0x_1}, \quad L_{x_1^2x_0} = L_{x_1^2}L_{x_0} - L_{x_1x_0x_1} - L_{x_0x_1^2},$$
$$L_{x_0x_1x_0} = L_{x_0x_1}L_{x_0} - 2L_{x_0^2x_1}, \quad L_{x_1x_0^2} = L_{x_1}L_{x_0^2} - L_{x_0x_1}L_{x_0} + L_{x_0^2x_1}.$$

Let $\mathcal{M}_0 f(z)$ be $f(ze^{2i\pi})$; applying $\mathcal{M}_0 - \mathrm{Id}$ on the right-hand sides of these identities only affects the $L_{x_0^k}$. Their monodromy follows from $(\mathcal{M}_0 - \mathrm{Id})L_{x_0} = 2i\pi$. Another shuffle thus shows that

$$(\mathcal{M}_0 - \mathrm{Id})L_{Ux_0} = 2i\pi L_U + \sum_V \mu_V L_V, \qquad (\mathcal{M}_0 - \mathrm{Id})L_{Ux_1} = 0,$$

where the words V in the sum all have weight smaller than the weight of U.

We now proceed to prove the analogous property at 1 with $\mathcal{M}_1 f(1-z) := f((1-z)e^{2i\pi})$:

$$(\mathcal{M}_1 - \mathrm{Id})L_{Ux_1} = -2i\pi L_U + \sum_V \mu_V L_V, \qquad (\mathcal{M}_1 - \mathrm{Id})L_{Ux_0} = 0. \tag{3}$$

At $z=1$, words ending with x_0 correspond to polylogarithms that are analytic there, hence, have a trivial monodromy. This is the second identity. The situation is slightly more complicated than at the origin because of divergence. As above, an induction on the weight shows that all words beginning with x_1 can be rewritten as a sum of shuffles of powers of x_1 and words beginning with x_0. The monodromy of $L_{x_1^k}$ follows from that of the logarithm. The remaining words are those beginning with x_0 and ending with x_1. Consider the path consisting of a straight line from z to a circle of radius ϵ around 1, turning around 1 in the anti-clockwise direction and coming back to z. Then Cauchy's theorem implies that

$$(\mathcal{M}_1 - \mathrm{Id})L_{x_0Ux_1}(z) = \lim_{\epsilon\to 0}\int_{1-\epsilon}^z \frac{dt}{t}(\mathcal{M}_1 - \mathrm{Id})L_{Ux_1}(t) + \lim_{\epsilon\to 0}\oint_{|1-t|=\epsilon}\frac{dt}{t}L_{Ux_1}(t).$$

Another induction shows that the rightmost integral tends to 0, while convergence of L_{Ux_1} at 1 reduces the first limit to

$$\int_1^z \frac{dt}{t}(\mathcal{M}_1 - \mathrm{Id})L_{Ux_1}(t).$$

This makes it possible to compute all the monodromies of words ending in x_1 and proves (3). Here are the corresponding relations up to weight 3, using p to denote $2i\pi$:

$$(\mathcal{M}_1 - \mathrm{Id})L_{x_1^k} = \sum_{j=1}^k L_{x_1^{k-j}}\frac{(-p)^j}{j!}, \qquad (\mathcal{M}_1 - \mathrm{Id})L_{x_0x_1} = -pL_{x_0}, \quad (\mathcal{M}_1 - \mathrm{Id})L_{x_0^2x_1} = -pL_{x_0^2},$$

$$(\mathcal{M}_1 - \mathrm{Id})L_{x_0x_1^2} = -p(L_{x_0x_1} - \zeta_{x_0x_1}) + \frac{p^2}{2}L_{x_0}, \quad (\mathcal{M}_1 - \mathrm{Id})L_{x_1x_0x_1} = 2L_{x_0x_1^2} - pL_{x_1x_0} - 2p\zeta_{x_0x_1}.$$

The proof of Theorem 1 is concluded by considering the maximal weight involved in a minimal non-trivial linear combination: applying both operators $(\mathcal{M}_0 - \mathrm{Id})$ and $(\mathcal{M}_1 - \mathrm{Id})$ leads to linear relations of smaller weight, that have to be trivial.

3. Changes of Variables

The group of six rational functions z, $1-z$, $1/z$, $1/(1-z)$, $1-1/z$, $z/(1-z)$ permutes the singularities 0, 1, ∞. If h is an element of this group, then

$$L_{xU}(h(z)) = \int_0^{h(z)} L_U(t) w_x(t)\,dt = \int_{h^{-1}(0)}^{z} L_U(h(s)) w_x(h(s)) h'(s)\,ds.$$

It turns out that for all h in the group and all $x \in \{x_0, x_1\}$, $w_x(h(s))h'(s)$ can be rewritten as a linear combination of ds/s and $ds/(1-s)$. Thus by induction, all polylogarithms at $h(z)$ can be rewritten in terms of polylogarithms at z. For the classical dilogarithm $\mathrm{Li}_2 = L_{x_1 x_0}$, we get

$$\mathrm{Li}_2(1-z) + \mathrm{Li}_2(z) = L_{x_0}(z)L_{x_1}(z) + \zeta(2),\ \mathrm{Li}_2(z) - \mathrm{Li}_2(1-z^{-1}) = L_{x_0}(z)L_{x_1}(z) + \zeta(2) + L_{x_0^2}(z).$$

Setting z to $1/2, \pm\phi, \pm 1/\phi, 1+\phi, 1-1/\phi$, where ϕ is the golden ratio, yields the only known values of Li_2 in closed form.

4. Noncommutative Generating Function

All the inductions mentioned here are conveniently handled by introducing the noncommutative generating function $L(z) = \sum L_W(z) W$ where the sum is over all words of $\mathcal{X} = \{x_0, x_1\}^\star$. The integral representation of polylogarithms is equivalent to a linear differential equation:

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

A consequence of the rewriting of words ending by x_0 is that all polylogarithms except $L_{x_0}^k$ tend to 0 at the origin. This leads to the initial condition $L(\epsilon) = e^{\ln \epsilon x_0} + O(\epsilon^{1-\delta})$, for $\epsilon \to 0$, where δ is an arbitrarily small real number. The shuffle relation then implies that this generating function is a *Lie exponential.* A noteworthy consequence is that it can be factored as a product of Lie exponentials indexed by Lyndon words, which turns out to yield an efficient algorithm for computing identities [3].

The inductions used in the monodromy computations translate very explicitly into

$$\mathcal{M}_0 L(z) = L(z) e^{2i\pi x_0}, \qquad \mathcal{M}_1 L(z) = L(z) Z^{-1} e^{-2i\pi x_1} Z,$$

where Z is very close to being the generating function of the multiple zeta values: it is the unique Lie exponential such that

$$(Z|x_0) = (Z|x_1) = 0, \qquad (Z|x_0 W x_1) = \zeta_{x_0 W x_1}, \quad W \in \mathcal{X}.$$

Similarly, the changes of variables can be interpreted at the level of $L(z)$ [5].

Bibliography

[1] Borwein (Jonathan M.), Bradley (David M.), Broadhurst (David J.), and Lisoněk (Petr). – Special values of multiple polylogarithms. *Transactions of the American Mathematical Society*, 1999. – To appear.

[2] Lewin (Leonard) (editor). – *Structural properties of polylogarithms.* – American Mathematical Society, Providence, RI, 1991, xviii+412p.

[3] Minh (Hoang Ngoc) and Petitot (Michel). – Lyndon words, polylogarithms and the Riemann ζ function. *Discrete Mathematics*, *Toappear*.

[4] Minh (Hoang Ngoc), Petitot (Michel), and Van der Hoeven (Joris). – Shuffle algebra and polylogarithms. In *Formal Power Series and Algebraic Combinatorics.* – 1998. Proceedings PFSAC'98, Toronto.

[5] Minh (Hoang Ngoc), Petitot (Michel), and Van der Hoeven (Joris). – L'algèbre des polylogarithmes par les séries génératrices. In *Formal Power Series and Algebraic Combinatorics.* – 1999. Proceedings PFSAC'99, Barcelona.

A Gröbner Free Alternative for Polynomial System Solving

Grégoire Lecerf

Laboratoire GAGE, École polytechnique

July 5, 1999

[summary by Éric Schost]

Abstract

Let $f_1, \dots, f_n$ and g be polynomials in $\mathbb{Q}[x_1, \dots, x_n]$, such that the system $f_1 = \cdots = f_n = 0$ and $g \neq 0$ has only a finite number of solutions. Following a long series of theoretical papers, G. Lecerf, M. Giusti and B. Salvy propose a new algorithm to obtain a *geometric resolution* of the zero-set of the system. This algorithm is valid under the hypothesis that the system $f_1, \dots, f_n$ forms a reduced, regular sequence outside $V(g)$. This talk presents the complexity of the algorithm, details some crucial steps and finally compares the implementation in Magma called Kronecker[1] to other available softwares. It is based on [3].

1. Introduction

The algorithm presented here is devoted to the resolution of zero-dimensional systems. For a zero-dimensional variety $\mathcal{V}$, a geometric resolution consists in the following elements:

- a *primitive element* u of the extension $\mathbb{Q} \to \mathbb{Q}[\mathcal{V}]$;
- its *minimal polynomial* $q \in \mathbb{Q}[U]$;
- the *parametrization* of the coordinates of the form $q'(u)x_i = w_i(u)$, $1 \leq i \leq n$

such that $\{q(u) = 0, x_i = w_i(u)/q'(u)\}$ is a description of the points of $\mathcal{V}$.

The algorithm presented by G. Lecerf lies in the continuation of earlier, theoretical work by the TERA group [1, 2] that gave algorithms to obtain geometric resolutions of reduced, regular systems.

The present work inherits the specifics of these papers: the algorithm takes into account the evaluation properties of the input system and can work outside a given hypersurface. It also includes refinements that simplify previous algorithms and improve their complexity. Finally, note that it is a probabilistic algorithm. The author proposes an implementation in Magma called Kronecker that validates this approach.

In the specific case of zero-dimensional systems, a geometric resolution also bears the name Rational Univariate Representation, following F. Rouillier's denomination. In [8], he gives an algorithm to compute this object that relies on the precomputation of a Gröbner basis. This computation is avoided here, whence the title.

The presentation is organized as follows. First, a rough sketch of the resolution algorithm is given. The complexity of this algorithm is then stated in terms of some suitably defined quantities. The most relevant steps of the resolution are detailed. The implementation is compared with

[1] See also the Kronecker homepage: `http://www.gage.polytechnique.fr/~lecerf/software/kronecker`

implementations of Gröbner bases and Rational Univariate Representation (Gb by J.-C. Faugère, RealSolving by F. Rouillier), and of Gröbner bases in Magma.

2. **Outlook of the Algorithm**

Notation. $\mathcal{V}_i$ will denote $\overline{V(f_1,\ldots,f_i)\backslash V(g)}$.

Input. The input system $f_1,\ldots,f_n$ must form a regular, reduced sequence outside $V(g)$, that is:

- $V(f_{i+1})$ intersects $\mathcal{V}_i$ regularly, so that $\dim \mathcal{V}_i = n - i$;
- $\mathcal{V}_i$ is reduced.

These polynomials will be evaluated on many objects, so they are thought (and given) as Straight-Line Programs.

Output. The output of the algorithm is a geometric resolution of $\mathcal{V}_n$.

Sketch of the Algorithm. The algorithm is an iterative intersection process. It works the following way:

- Apply a generic linear change of coordinates.
- Compute incrementally a resolution in $\mathbb{Z}/p\mathbb{Z}$, for some prime p. The i-th step consists in:

$$\text{Resolution of } \mathcal{V}_i \text{ at } x_1,\ldots,x_{n-i}=0$$

$$\downarrow \text{Lifting of } x_{n-i}$$

$$\text{Resolution of } \mathcal{V}_i \text{ at } x_1,\ldots,x_{n-i-1}=0$$

$$\downarrow \text{Intersection}$$

$$\text{Resolution of } \mathcal{V}_i \cap V(f_{i+1}) \text{ at } x_1,\ldots,x_{n-i-1}=0$$

$$\downarrow \text{Cleaning}$$

$$\text{Resolution of } \mathcal{V}_{i+1} \text{ at } x_1,\ldots,x_{n-i-1}=0$$

- Unapply the change of variables.
- Lift the resolution to a big enough precision p^k and reconstruct a rational resolution.

Why a Generic Change of Variables? The algorithm heavily relies on specializations and unspecializations of variables, so that we need generic enough coordinates. Thus, the linear change of variables must ensure that all the intermediate varieties $\mathcal{V}_i$ are in Noether position, that their fiber above $x_1,\ldots,x_{n-i}=0$ is reduced and that the first dependent variable x_{n-i+1} is a separating (primitive) element for this fiber.

Are There SLP's Left ? The rough algorithm shown above handles only zero- and one-dimensional varieties, as the reader will easily check, with the consequence that all computations are performed on uni- or bi-variate polynomials, which are not represented by SLP's. This follows the deforestation technique introduced in [9] and already used in [4]. Only the input polynomials are coded as SLP's, as they are evaluated on various data throughout the resolution.

Probabilistic Aspects. The algorithm is probabilistic. The success relies on a lucky prime number p and a lucky linear change of coordinates. The unlucky change of coordinates are enclosed in a strict algebraic subset of $\mathrm{GL}(n)$.

The algorithm is not Las Vegas. Still, we can test whether the solution it outputs satisfies the input system. If it does, we might only miss some of the solutions. In the special case when the output contains $\Pi \deg(f_i)$ solutions, we know we have all of them.

3. Complexity

The quantities that appear in the complexity are of two kinds. First, the syntactic complexity of the input system:

- d, the maximum of the degrees of the polynomial $f_1, \ldots, f_n$;
- h, the maximum of the heights of these polynomials;
- L, the number of binary arithmetic operations required to evaluate the polynomials $f_1, \ldots, f_n$ and g; that is the size of the SLP that encodes them.

The complexity also depends on some parameters that are intrinsic to the varieties $\mathcal{V}_i$:

- δ, the maximum of the degrees of the varieties $\mathcal{V}_1, \ldots, \mathcal{V}_{n-1}$;
- D, the degree of $\mathcal{V}_n$. It is the number of solutions of the system;
- η, the height of the integers of the resolution (that depends on the choice of the primitive element).

The following theorem establishes the time-complexity of the whole resolution process. As usual, the term $O_{\log}(X)$ indicates a complexity of X up to logarithmic factors. The constant Ω is related to the complexity of linear algebra operations over a commutative ring. Note that $\Omega < 3$ is valid on a field. On a ring, we may take $\Omega \leq 4$, using Berkowitz' algorithm.

Theorem 1. *The time-complexity of the modular computations is*

$$n(nL + n^{\Omega})O_{\log}\left((d\delta)^2\right).$$

The time necessary to lift the integers is

$$(nL + n^{\Omega})O_{\log}(D)O_{\log}(\eta).$$

This complexity improves upon earlier results. The papers [1] gave algorithms with complexity $L(nd\delta\eta h)^{O(1)}$. More recently, [5] refines these algorithms, so that the power of δ that appears is 3.

The following three sections detail the iterative step of the modular resolution, and in particular:

- the lifting step that now relies on a global Newton process;
- the intersection step that uses methods that go back to Kronecker [6], and are detailed in [7].

The minimal polynomial of a resolution will always be noted q (or $\tilde{q}$, Q, ...). The situation is slightly more complicated regarding parametrizations. The reader should be aware that a resolution can bear many forms, depending on the choice of the denominator of the parametrization. The so-called "Kronecker" form has the derivative of the minimal polynomial as denominator; the associated parametrization will be noted $\mathbf{w}$. The polynomial parametrization (i.e., with denominator 1) will be noted $\mathbf{v}$.

It is always possible to go from one type of parametrization to another one, by inverting the denominator modulo the minimal polynomial. This will often be done, without further notice.

4. Lifting

We enter the i-th step with a resolution of the variety $\mathcal{V}_i$ specialized at $x_1, \dots, x_{n-i} = 0$, which is a zero-dimensional set. The lifting step "unspecializes" the last free variable x_{n-i} and thus builds a resolution of the one-dimensional set $\mathcal{V}_i$ specialized at $x_1, \dots, x_{n-i-1} = 0$, which will be called a *lifted curve.*

Input. A geometric resolution modulo p of $\mathcal{V}_i$ at $x_1, \dots, x_{n-i} = 0$, with primitive element x_{n-i+1}:

$$q(x_{n-i+1}) = 0, \qquad \begin{cases} x_{n-i+1} & = v_{n-i+1}(x_{n-i+1}), \\ & \vdots \\ x_n & = v_n(x_{n-i+1}). \end{cases}$$

Output. The lifted curve is represented as a parametrized version of the previous representation, where now both the minimal polynomial and the parametrizations have coefficients in $\mathbb{Z}/p\mathbb{Z}[x_{n-i}]$. The minimal polynomial and the parametrizations in Kronecker form have total degree less than the degree of q.

$$Q(x_{n-i}, x_{n-i+1}) = 0, \qquad \begin{cases} x_{n-i+1} & = V_{n-i+1}(x_{n-i}, x_{n-i+1}), \\ & \vdots \\ x_n & = V_n(x_{n-i}, x_{n-i+1}). \end{cases}$$

How Does it Work? The core of the routine is a global Newton iteration, which is summarized in the following scheme.

$$\begin{array}{c} q(x_{n-i+1}) = 0, \\ \mathbf{f}(\mathbf{v}) = 0 + O(x_{n-i}) \mod q, \end{array} \qquad \begin{cases} x_{n-i+1} & = v_{n-i+1}(x_{n-i+1}), \\ & \vdots \\ x_n & = v_n(x_{n-i+1}). \end{cases}$$

$$\downarrow \text{Global Newton}$$

$$\begin{array}{c} \tilde{q}(x_{n-i}, x_{n-i+1}) = 0 + O(x_{n-i}^2), \\ \mathbf{f}(x_{n-i}, \tilde{\mathbf{v}}) = 0 + O(x_{n-i}^2) \mod \tilde{q}, \end{array} \qquad \begin{cases} x_{n-i+1} & = \tilde{v}_{n-i+1}(x_{n-i}, x_{n-i+1}), \\ & \vdots \\ x_n & = \tilde{v}_n(x_{n-i}, x_{n-i+1}). \end{cases}$$

This makes sense, since at the beginning of the i-th step, the system can be seen as polynomials over $\mathbb{Z}/p\mathbb{Z}[x_{n-i}]$ for which we have a resolution modulo $I = (x_{n-i})$. A global Newton iteration enables to compute a resolution to the precision I^2, and, by successive applications, to any I^{2^k}. The bound on the degrees in the Kronecker form indicates the number of steps to perform. Let's detail the first pass.

The point is to consider that we are given a representation modulo I of an underlying resolution over the ring $\mathbb{Z}/p\mathbb{Z}[x_{n-i}]$. This resolution has a separating element T which is x_{n-i+1} modulo I, and such that $\mathbf{f}(x_{n-i}, \mathbf{v}(T)) = 0 + O(x_{n-i})$ modulo $q(T)$—recall that this only means that the input is a resolution for the specialization $x_{n-i} = 0$.

First, an iteration of the classical Newton iterator yields new parametrizations V that satisfy $\mathbf{f}(x_{n-i}, \mathbf{V}(T)) = 0 + O(x_{n-i}^2)$ modulo $q(T)$. This is not satisfying yet, for we seek expressions that involve x_{n-i}, not T. The trick is to see that the new parametrization of x_{n-i+1} is

$x_{n-i+1} = T + x_{n-i}\Delta(T) + O(x_{n-i}^2)$, for some polynomial Δ with coefficients in $\mathbb{Z}/p\mathbb{Z}$, according to the remark above. Furthermore, $x_{n-i}\Delta(T)$ is $x_{n-i}\Delta(x_{n-i+1})$ modulo I^2 (this is a first-order expansion). The corresponding substitution $T \leftarrow x_{n-i+1} - x_{n-i}\Delta(x_{n-i+1})$ thus yields the desired resolution modulo I^2.

5. Intersection

We go back to the description of a step of the iterative resolution process. This second part consists in intersecting $\mathcal{V}_i$ specialized at $x_1, \ldots, x_{n-i-1} = 0$ with the hypersurface defined by f_{i+1}.

Input. The output of the lifting step and f_{i+1}

Output. A geometric resolution of $\mathcal{V}_i \cap V(f_{i+1})$ at $x_1, \ldots, x_{n-i-1} = 0$ with x_{n-i} as primitive element.

To this effect, we perform the following linear change of variables: $x_{n-i} = X - tx_{n-i+1}$. The corresponding minimal polynomial and parametrizations are noted $Q_t(X, x_{n-i+1})$ and $\mathbf{V}_t(X, x_{n-i+1})$. This idea naturally leads to what we called Kronecker parametrizations, and is already to be found in his papers.

We compute $A := \mathrm{Resultant}_{x_{n-i+1}}(Q_t, f_{i+1}(X - tx_{n-i+1}, \mathbf{V}_t))$ at order $O(t^2)$, that we shall write $A = A_0 + tA_1 + O(t^2)$. As $A(x_{n-i} + tx_{n-i+1}) = 0$, it follows that the eliminating polynomial of x_{n-i} is A_0 and that the the parametrization of x_{n-i+1} is $-A_1(x_{n-i})/A_0'(x_{n-i})$.

6. Cleaning Step

This is the last part of each iteration, that consists in removing the unwanted components lying in $V(g)$.

Input. A resolution of $\mathcal{V}_i \cap V(f_{i+1})$ at $x_1, \ldots, x_{n-i-1} = 0$ as produced by the intersection routine.

Output. A resolution of $\mathcal{V}_{i+1}$ at $x_1, \ldots, x_{n-i-1} = 0$.

The computation is straightforward: compute the gcd p of q and $g(v)$ and replace q by q/p to obtain a new resolution.

7. Experimental Results

The algorithm is implemented in Magma, in a package called Kronecker. It has been compared with existing softwares, namely Gb, RealSolving and Magma on different examples. All computations were done on the MEDICIS machines (`http://www.medicis.polytechnique.fr`).

The first series of examples consists in n generic polynomials of degree 2, with coefficients of h decimal digits, for various n and h. The systems have then full degree $D = 2^n$. This example aims at illustrating the good behaviour of Kronecker regarding the growth of the coefficients. The timings are given in Table 1. The computations were performed on a Compaq Alpha EV6, 500 MHz, 128 Mb.

The second example (Table 2) is inspired by the Kruppa equations. It consists in 7 equations in 7 variables with integers coefficients of size 18, each equation is a product of two linear forms minus a constant coefficient. The computations were performed on a DEC Alpha EV56, 400 Mhz, OSF/1 4.0b, 1024 Mb.

n	h	Kronecker	Gb Grevlex + Real Solving
4	4	6 s	0.5s +0.5s
4	8	8 s	1s + 1.3s
4	16	11s	2.5s + 3.7s
4	32	21s	7s + 9.3s
5	4	36s	5s + 18s
5	8	50s	17s + 57s
5	16	88s	65s + 180s
5	32	208s	244s + 592s
6	4	260s	209s + >317s
6	8	412s	773s + ∞
6	16	875s	2999s + ∞
6	32	2312s	5652s + ∞

TABLE 1

Kronecker	Magma Grevlex
5h	13.6h

TABLE 2

Bibliography

[1] Giusti (M.), Hägele (K.), Heintz (J.), Morais (J. E.), Montaña (J. L.), and Pardo (L. M.). – Lower bounds for Diophantine approximation. *Journal of Pure and Applied Algebra*, vol. 117/118, 1997, pp. 277–317. – Proceedings MEGA'96.

[2] Giusti (M.), Heintz (J.), Morais (J. E.), Morgenstern (J.), and Pardo (L. M.). – Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, vol. 124, 1998, pp. 101–146.

[3] Giusti (M.), Lecerf (G.), and Salvy (B.). – A Gröbner free alternative for polynomial system solving. In *Proceedings FOCM'99*. – 1999.

[4] Giusti (Marc), Hägele (Klemens), Lecerf (Grégoire), Marchand (Joël), and Salvy (Bruno). – *Computing the Dimension of a Projective Variety: the Projective Noether Maple Package*. – Research report n° 3224, Institut National de Recherche en Informatique et en Automatique, July 1997.

[5] Heintz (J.), Matera (G.), and Waissbein (A.). – On the time-space complexity of geometric elimination procedures. – 1999. Manuscript of Universidad Favaloro, Buenos Aires, Argentina.

[6] Kronecker (L.). – Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für die reine und angewandte Mathematik*, vol. 92, 1882, pp. 1–122.

[7] Macaulay (F. S.). – *The Algebraic Theory of Modular Systems*. – Cambridge University Press, 1916.

[8] Rouillier (F.). – *Algorithmes efficaces pour l'étude des zéros réels des systèmes polynomiaux*. – PhD thesis, Université de Rennes I, may 1996.

[9] Wadler (P.). – Deforestation: transforming programs to eliminate trees. *Theoretical Computer Science*, vol. 73, 1990, pp. 231–248. – Special issue of selected papers from 2nd ESOP.

Concrete Resolution of Differential Problems using Tannakian Categories

Jacques-Arthur Weil
Département de Mathématiques, Université de Limoges

April 19, 1999

[summary by Frédéric Chyzak]

Abstract

Given a linear ODE with polynomial coefficients, one easily finds local information about its solutions. To obtain global information of algebraic nature (operator factorization, explicit finite form, algebraic relations between solutions), one classically reduces the problem to determining rational or exponential solutions of auxiliary linear ODE's. The latter are often uneasy to compute in practice, and we show by a few examples how to advantageously substitute differential systems that are simpler to construct, solve or study.

1. Solving Linear Differential Equations

The main question when studying a linear differential operator L is how to "solve" for its solutions. "Solving", however, covers several meanings. Throughout this text, L denotes a differential operator acting on a function y in the variable x by $L(y) = a_n y^{(n)} + \cdots + a_0 y$ for polynomials a_i in x with coefficients in a field C. This field is $\mathbb{Q}$, $\bar{\mathbb{Q}}$ or $\mathbb{C}$ in practice.

The simplest way to solve is the determination of local information, like a basis of formal solutions in the neighbourhood of 0. The general form of a formal solution is the formal series

$$y = x^{\alpha}(p_0(\ln x) + p_1(\ln x)x^{1/r} + \cdots + p_i(\ln x)x^{i/r} + \cdots)$$

for polynomials p_i with uniformly bounded degrees. Here, r is a positive integer, the ramification, and p_0 is assumed to be non-zero so as to ensure that the highest possible power has been incorporated into the generalized exponent $\alpha \in C[x^{1/r}]$. The power x^{α} is nothing but $\exp \int \alpha/x\,dx$, the formal solution of $y' = (\alpha/x)y$. This approach by generalized exponents is due to Van Hoeij [12] and unifies regular and irregular singular expansions. A similar treatment was developed in the case of systems by Barkatou [1] and Pflügel [5].

Of course, the most generally understood acceptance of "solving" relates to resolution in closed form. By simultaneously considering the bases of formal solutions in the neighbourhood of all possible singularities of the operator L, namely, the zeroes of its leading coefficient $a_n(x)$, several algorithms are available to search for solutions in various classes of closed form, like polynomial solutions $y \in C[x]$, rational solutions $y \in C(x)$, exponential solutions y for which $y'/y \in C(x)$, or liouvillian solutions y for which y'/y is algebraic over $C(x)$. See [4, 13] and the references there.

Note that each solution s in the above classes supplies a first-order right-hand factor of the operator L, namely $\partial - s'/s$ where ∂ denotes the derivation operator with respect to x. A more general problem is that of the factorization of operators from the ring $C(x)[\partial]$ of linear differential operators with rational function coefficients, and the search for higher-order right-hand factors. This relates to differential Galois theory. More specifically, polynomial, rational, and exponential solutions correspond to factorization in this ring, whereas liouvillian solutions correspond to the more complex problem of absolute factorization [13], i.e., factorization of an operator $L \in C(x)[\partial]$ with factors in $K[\partial]$ for an algebraic closure K of $C(x)$. In any case, factorization relates to solving since any solution of any right-hand factor is a solution of the original operator. Furthermore, specialized algorithms exist for linear differential equations of small orders.

Right-hand factors of an operator are a first type of auxiliary operators or lower order that simplify solving. More generally, another form of "solving" the operator L is by looking for its solutions that can be viewed as powers, products, or wronskians of an auxiliary operator, or system of operators, of lower order. This is the main discussion of the next sections. Applications include the classification of solutions, connexion problems, number theory (by looking for differential equations of minimal order), and the search for first integrals of non-linear differential equations.

2. Lower Order Equations and Symmetric Power Solutions

As an example, consider the third-order equation $y''' - 4ry' - 2r'y = 0 \quad (r \in C(x))$. It admits a basis of solutions of the form $(z_1 = y_1^2, z_2 = y_2^2, z_3 = y_1 y_2)$, where both y_1 and y_2 are solutions of the same second-order equation $y'' = ry$. To obtain such special solutions of a higher-order operator L, the crucial relation to be used is $z_1 z_2 = z_3^2$. Indeed, considering the formal solution $\tilde{z}_i = x^{\alpha_i}\Sigma_i$ corresponding to the expansion of each actual function z_i, we obtain that the formal expansion of the product $z_1 z_2$ is the product of formal expansions $\tilde{z}_1\tilde{z}_2 = x^{\alpha_1+\alpha_2}\Sigma_1\Sigma_2$. Identifying those generalized exponents for L that can be a sum of two terms therefore supplies a set of candidate exponents for the auxiliary operator and the z_i. Note that the original third-order equation has been replaced by a "simpler system" consisting of a second-order equation and a quadratic relation.

3. Liouvillian Solutions

To solve an operator L for its liouvillian solutions, one looks for the possible irreducible polynomials P of the form $X^m - b_{m-1}X^{m-1} - \cdots - b_0$ such that $P(u) = 0$ implies $L(\exp \int u\, dx) = 0$ [10]. Given the order n of the operator, differential Galois theory shows that only finitely many degrees are possible for the polynomial P. There exists an algorithm to compute the list of the possible numbers m: for $n = 2$, the list is 1, 2, 4, 6, and 12; for $n = 3$, it is 1, 3, 6, 9, 21, and 36 [6, 7, 9]; for $n = 4$ and higher, a formula is known for the maximum number of the list.

By construction, the roots u_i of P are logarithmic derivatives y_i'/y_i of a solution of L, and $b_{m-1} = \sum_i u_i = \sum_i y_i'/y_i$ is the logarithmic derivative of the product $\prod_i y_i$. A necessary and sufficient condition for the existence of a polynomial P of degree m above, which describes the liouvillian solutions of L is that there exists a polynomial of degree m in solutions of L whose logarithmic derivative is rational, and which is the product of linear factors. More specifically, for a solution basis $(z_1, \ldots, z_m)$ of L the product $\prod_i y_i$ is searched for under the form $\prod_i (c_{i,1}z_1 + \cdots + c_{i,m}z_m)$.

The search for liouvillian solutions therefore reduces to the search for exponential solutions. To this end, the present work allows to avoid computing the equation for the symmetric power, which is too large, but prefers a more compact representation.

4. Factorization and Alternate Power Solutions

As another typical example, let us consider the search for a right-hand factor $H = \partial^2 - b_1\partial - b_0$ of order 2 of the operator $L = \partial^4 - a_2\partial^2 - a_1\partial - a_0$ of order 4. For any solution basis (y_1, y_2) of H, the operator H is given by the determinantal representation

$$H(y) = \begin{vmatrix} y_1 & y_2 \\ y_1' & y_2' \end{vmatrix}^{-1} \begin{vmatrix} y & y_1 & y_2 \\ y' & y_1' & y_2' \\ y'' & y_1'' & y_2'' \end{vmatrix} = y'' - \frac{\omega_{0,2}}{\omega_{0,1}}y' + \frac{\omega_{1,2}}{\omega_{0,1}}y \quad \text{where} \quad \omega_{i,j} = \begin{vmatrix} y_1^{(i)} & y_2^{(i)} \\ y_1^{(j)} & y_2^{(j)} \end{vmatrix}.$$

To obtain a factor of order 2, we now search for an exponential solution and show that it can be interpreted as a determinant $\omega_{0,1}$. Let A be the companion matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a_0 & a_1 & a_2 & 0 \end{pmatrix}, \qquad \text{and let} \qquad Y = \begin{pmatrix} y \\ y' \\ y'' \\ y''' \end{pmatrix}, \qquad \text{so that} \qquad Y' = AY.$$

Let us introduce the vector $Z = (\omega_{0,1}, \omega_{0,2}, \omega_{0,3}, \omega_{1,2}, \omega_{1,3}, \omega_{2,3})^T$. In view of their definition, the $\omega_{i,j}$ satisfy differential relations like $\omega'_{0,1} = \omega_{0,2}$, $\omega'_{0,3} = \omega_{1,3} + a_0\omega_{0,0} + a_1\omega_{0,1} + a_2\omega_{0,2}$, and so on. From them, we find a matrix

$$\Lambda_2(A) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ a_1 & a_2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ -a_0 & 0 & a_2 & 0 & 0 & 1 \\ 0 & -a_0 & 0 & -a_1 & 0 & 0 \end{pmatrix} \qquad \text{such that } Z' = \Lambda_2(A)Z.$$

Again, we then only look for exponential solutions Z of the matrix $\Lambda_2(A)$, which is easy to construct and contains more information than the usual single auxiliary equation used for factorization. Finally, one has to check that the solution Z is a determinant. For this, a necessary and sufficient condition is the Plücker relation, which here simply reduces to $\omega_{0,1}\omega_{2,3} - \omega_{0,2}\omega_{1,3} + \omega_{0,3}\omega_{1,2} = 0$.

To rephrase the method in a more formal way, introduce V, the solution space of L. The search for Z is indeed a search for objects in the 2-exterior power $\Lambda_2(V)$, i.e., the vector space of linear combination of formal 2-exterior products $v \wedge w$, $(v, w) \in V^2$, which satisfy the rule $w \wedge v = -v \wedge w$. Pure exterior product $u \wedge v$ are interpreted as determinants. The search for Z is therefore equivalent to the search for a pure exterior product $\omega_{0,1} \in \Lambda^2(V)$ such that the 1-dimensional vector space $C\omega_{0,1}$ is stable under the action of the differential Galois group of L.

Here the search for a second-order right-hand factor of a fourth-order equation has been reduced to solving a "simpler" system of six first-order equations.

5. Module and Dual Module Associated with an Operator

As an important tool for the study of a linear differential operator L, one classically associates a canonical module in the following way. For L in the algebra $k[\partial]$ of linear differential operators with coefficients in a field k, one considers the quotient $M = k[\partial]/k[\partial]L$ of $k[\partial]$ by its left ideal $k[\partial]L$. The left module M can be viewed as the module $k[\partial]y$ generated by a generic solution y of the operator L. Linear constructs on and between solution spaces of operators, like (direct or usual) sums, (symmetric or exterior or usual commutative) products, (indefinite) integration, and so on, correspond to constructs on and between the corresponding $k[\partial]$-modules.

A variant module is obtained by endowing the dual k-vector space M^* with a $k[\partial]$-module structure. Let r be the order of L, then M is of dimension r and its dual $M^* = \mathrm{Hom}_k(M, k)$ is isomorphic to k^r. Now let A be the companion matrix of L and $(b_1, \dots, b_r)$ be the canonical basis of M^*. The latter is turned into a $k[\partial]$-module by defining an operator ∇ on M^* by the action

$$(\nabla b_1, \dots, \nabla b_r)^T = -A^T(b_1, \dots, b_r)^T$$

and letting ∂ act by ∇. Thus, $\nabla(am) = a\nabla m + a'm$ when $a \in k$ and $m \in M$. From this Leibniz rule applied to the product $y_1b_1 + \cdots + y_rb_r = (y_1, \dots, y_r)(b_1, \dots, b_r)^T$, we derive the equality

$$Y' = AY \qquad \text{for} \qquad Y = (y_1, \dots, y_r)^T$$

whenever $\nabla(y_1 b_1 + \cdots + y_r b_r) = 0$. Note that this $k[\partial]$-module structure on M^* usually does not make it the dual $k[\partial]$-module $\mathrm{Hom}_{k[\partial]}(M, k)$, for the operator L usually has no solution in k.

The modules M^* allow for a better description of the calculations suggested in the previous sections through a link between the solution space $V = \mathrm{Sol}(L)$ and the $k[\partial]$-module M^*. This link is obtained by introducing the map ϕ from V to M^* defined by $\phi(y) = yb_1 + \cdots + y^{(r-1)} b_r$. Calculations with elements of the C-vector space $\mathrm{Sol}(L)$ have their counterparts in the $k[\partial]$-module M^*. For example, one recovers the determinants of the previous sections from the following identity for exterior products in the module $\Lambda^2 M^*$

$$\phi(y_1) \wedge \phi(y_2) = \sum_{1 \le i < j \le r} \omega_{i-1,j-1}\, b_i \wedge b_j \qquad \text{with} \qquad \omega_{i,j} = \begin{vmatrix} y_1^{(i)} & y_2^{(i)} \\ y_1^{(j)} & y_2^{(j)} \end{vmatrix}.$$

Again, constructs at the level of solution spaces translate into constructs at the level of the corresponding $k[\partial]$-modules.

6. Tannakian Definition of the Differential Galois Group

This section is based on my (Chyzak's) study and tentatively reflects what was not presented by the speaker for lack of time. It aims at defining differential Galois groups by the Tannakian viewpoint, as an alternative to Kolchin's more traditional and elementary definition by differential extension fields. Interestingly, some properties are easier to derive by the Tannakian viewpoint, for instance that it is a linear algebraic group (i.e., a subgroup of $\mathrm{GL}_n(C)$ and an algebraic variety). Another consequence is the possibility to rephrase algorithms in such a way that differential Galois theory, in the sense of Kolchin, is only used as a classification tool to prove the correction of the algorithms, while calculations take place at the level of modules in a more efficient way. This presentation is based on a discussion with the speaker, on conference proceedings by Ramis and Martinet [8, Part 2, Chapter 1], and on unpublished notes by Churchill [2, 3]. More direct references may be works by Bertrand, Deligne, and Katz. The Tannakian construction has a natural counterpart in difference Galois theory [11, Section 1.4].

For comparison sake, Kolchin's definition of the differential Galois group of a linear differential operator $L \in k[\partial]$ is as follows. Let C be the subfield of constants of k, n be the order of L, and consider the Picard-Vessiot extensions k' of k associated with L, i.e., the differential field extensions of k that contain an n-dimensional C-vector space of solutions of L and do not enlarge the constant field C. Then the differential Galois group of L is defined as the group G of differential field automorphisms (i.e., field automorphisms that respect the differential structure) of *any* Picard-Vessiot extension k' that additionally respect the action of k on k'. This mimics the classical Galois theory for a polynomial $P \in k[X]$, where one introduces the group of field automorphisms of a suitable extension k' of k which contains all solutions of P and restrict to the identity on k. While the (algebraic) Galois group of a polynomial is a subgroup of a permutation group $\mathcal{S}_n$, the differential Galois group of an operator is a subgroup of the linear group $\mathrm{GL}_n(C)$ for the common field of constants C of k and k'.

For its part, instead of a single extension k' of k, the Tannakian presentation simultaneously considers a whole collection of $k[\partial]$-modules, and introduces the differential Galois group as a group of internal transformations on this collection. Crucially, each transformation has to transform all the modules in a way compatible with the linear maps between the modules. Moreover, each module M is associated with a solution set that can be viewed as the kernel of the derivation on M, and the above-mentioned transformations have to be compatible with taking solutions.

At the heart of the Tannakian construction are k-vector spaces V that are closed under the action of an operator ∇ which extends the action of the derivation on k by the Leibniz rule:

$$\nabla(af) = a\nabla(f) + a'f, \qquad \text{when } a \in k \text{ and } f \in V.$$

This makes V a $k[\partial]$-module with ∂ acting by ∇.

From now on, we restrict to $k[\partial]$-modules that are finite-dimensional k-vector spaces. Fundamental examples are the modules $M = k[\partial]/k[\partial]L$ discussed in the previous section. We also restrict to $k = \mathbb{C}(z)$. An element $h \in \ker\nabla$ is called a horizontal vector. As has been explained when discussing dual modules M^*, horizontal vectors in M^* correspond to solutions $y \in k^r$ of the equation $\Delta y = 0$ where $\Delta = d/dz - A$ for $(\nabla b_1, \ldots, \nabla b_r)^T = -A^T(b_1, \ldots, b_r)^T$ once a basis $(b_1, \ldots, b_r)$ of M^* has been chosen. Rather than enlarging the space M where we have a solution for L, as is the case in the traditional differential Galois theory, we now enlarge the coefficient field of M^* so as to ensure the existence of a solution to Δ and thus of horizontal vectors for ∇. To this end, consider a non-singular point $a \in \mathbb{C}$ of the operator L, and introduce the field $\mathcal{M}_a$ of germs of meromorphic functions at a, which is isomorphic to the field of convergent Laurent series $\mathbb{C}\{z-a\}[(z-a)^{-1}]$. By Cauchy's theorem, the C-vector space $\ker\Delta$, where Δ is now viewed as acting on $(\mathcal{M}_a)^r$, is of dimension r and supplies with horizontal vectors of ∇ in $\mathcal{M}_a \otimes_{\mathbb{C}(z)} M$. Note that $\ker\Delta$ and $\ker\nabla$ usually have no more structure than that of C-vector spaces.

As an example, let us consider the $\mathbb{C}(z)[\partial]$-module generated by the Bessel function of the first kind $J_0(z)$. It is a two-dimensional $\mathbb{C}(z)$-vector space with basis $(J_0(z), J_1(z))$, and $J_0' = -J_1$. With the above notation,

$$\begin{pmatrix} \nabla J_0 \\ \nabla J_1 \end{pmatrix} = \begin{pmatrix} J_0' \\ -J_0'' \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1/z \end{pmatrix} \begin{pmatrix} J_0 \\ J_1 \end{pmatrix}, \qquad \text{so that} \qquad A = \begin{pmatrix} 0 & -1 \\ 1 & 1/z \end{pmatrix}.$$

As a result of a simple computation, $h = f_1 J_0 + f_2 J_1$ is a horizontal vector of ∇ if and only if

$$\begin{pmatrix} f_1 \\ f_2 \end{pmatrix} \in \ker\Delta = \mathbb{C}z \begin{pmatrix} -J_1(z) \\ J_0(z) \end{pmatrix} \oplus \mathbb{C}z \begin{pmatrix} -Y_1(z) \\ Y_0(z) \end{pmatrix},$$

where $Y_\nu(z)$ are the Bessel functions of the second kind, and where J_ν and Y_ν now denote germs of the corresponding functions (their local expansions at $a \neq 0$). This simplifies to $h \in \mathbb{C}z(Y_0 J_1 - J_0 Y_1)$, whence h is a constant by the Wronskian relation $Y_0 J_1 - J_0 Y_1 = 2/\pi z$.

To the module M above and any non-singular point $a \in \mathbb{C}$, we have just associated the $\mathbb{C}$-vector space of horizontal vectors of ∇ in the form of local expansions at a. Denote $\eta_a(M)$ this vector space. We now proceed to associate horizontal vectors to more involved module constructions. Denote $\{M\}$ the smallest class of $k[\partial]$-modules containing M and closed under finite direct sums and products, finite symmetric and exterior products, dualization, and taking the module of homomorphisms between two modules, and submodules. One can extend ∇ from M to any $V \in \{M\}$ in a canonical way; in particular:

$$\nabla|_{V\oplus W} = \begin{pmatrix} \nabla|_V & 0 \\ 0 & \nabla|_W \end{pmatrix}, \qquad \nabla|_{V\otimes W} = \nabla|_V \otimes 1|_W + 1|_V \otimes \nabla|_W.$$

This class becomes a category for the usual $k[\partial]$-module morphisms. The map η_a extends to $\{M\}$ by $\eta_a(V) = \ker(\nabla|_{\mathcal{M}_a \otimes_{\mathbb{C}(z)} V})$. In particular, $\eta_a(V \oplus W) = \eta_a(V) \oplus \eta_a(W)$ and $\eta_a(V \otimes W) = \eta_a(V) \otimes \eta_a(W)$. The crucial fact is that η_a is compatible with the maps that are natural between modules on the one hand and horizontal vector spaces on the other hand. Specifically, any $k[\partial]$-module homomorphism h between two modules V and W induces a C-linear homomorphism $\eta_a(h)$

between $\eta_a(V)$ and $\eta_a(W)$. This makes η_a a functor, in the sense that the diagram

$$\begin{array}{ccc} V & \xrightarrow{h} & W \\ \downarrow{\scriptstyle \eta_a} & & \downarrow{\scriptstyle \eta_a} \\ \eta_a(V) & \xrightarrow{\eta_a(h)} & \eta_a(W) \end{array}$$

is commutative for any two modules V and W.

To relate horizontal vectors at two non-singular points a and b, consider the maps σ that associate with any $k[\partial]$-module V a $\mathbb{C}$-linear map $\sigma(V) : \eta_a(V) \to \eta_b(V)$, subject to the constraint that

$$\begin{array}{ccc} \eta_a(V) & \xrightarrow{\eta_a(h)} & \eta_a(W) \\ \downarrow{\scriptstyle \sigma(V)} & & \downarrow{\scriptstyle \sigma(W)} \\ \eta_b(V) & \xrightarrow{\eta_b(h)} & \eta_b(W) \end{array}$$

is a commutative diagram for any homomorphism $h : V \to W$.

Such a map σ (from $\{M\}$ to the linear morphisms in the category of C-vector space) is called a morphism from (the functor) η_a to (the functor) η_b. The collection of such morphisms when a and b vary is a semigroup for composition. The corresponding notion of isomorphisms (of functors) is obtained when each of the linear maps $\sigma(V)$ is invertible. Two cases are of interest: when $a \neq b$, one of those isomorphisms is provided by analytic continuation along a path from a to b; when $a = b$, the isomorphisms from η_a into itself form a group (the group of automorphisms of the functor η_a). This group is the differential Galois group of L, following the Deligne-Katz definition.

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] Churchill (R. C.). – Connections on modules. – February 1997. Unpublished Notes for the Kolchin Seminar in Differential Algebra.

[3] Churchill (R. C.). – A comparison of the Kolchin and Deligne-Katz definitions of a differential Galois group. – February 1998. Unpublished Notes for the Kolchin Seminar in Differential Algebra.

[4] Pflügel (Eckart). – ISOLDE, a package for computing invariants of systems of ordinary linear differential equations. In Salvy (Bruno) (editor), *Algorithms Seminar, 1997-1998*, *INRIA Research Report*, pp. 79–82. – 1998.

[5] Pflügel (Eckhard). – An algorithm for computing exponential solutions of first order linear differential equations. In Küchlin (W.) (editor), *ISSAC'97 (July 21–23, 1997. Maui, Hawaii, USA)*. pp. 164–171. – ACM Press, 1997.

[6] Singer (Michael F.). – Liouvillian solutions of nth order homogeneous linear differential equations. *American Journal of Mathematics*, vol. 103, n° 4, 1981, pp. 661–682.

[7] Singer (Michael F.) and Ulmer (Felix). – Liouvillian and algebraic solutions of second and third order linear differential equations. *Journal of Symbolic Computation*, vol. 16, n° 1, 1993, pp. 37–73.

[8] Tournier (E.) (editor). – *Computer Algebra and Differential Equations.* – Academic Press, *Computational Mathematics and Applications*, 1989.

[9] Ulmer (Felix). – On Liouvillian solutions of linear differential equations. *Applicable Algebra in Engineering, Communication and Computing*, vol. 2, n° 3, 1992, pp. 171–193.

[10] Ulmer (Felix). – Linear differential equations and liouvillian solutions. In Salvy (Bruno) (editor), *Algorithms Seminar, 1993–1994*, *INRIA Research Report*, pp. 41–44. – 1994.

[11] van der Put (Marius) and Singer (Michael F.). – *Galois Theory of Difference Equations.* – Springer, 1997, *Lecture Notes in Mathematics.*

[12] Van Hoeij (Mark). – Formal solutions and factorization of differential operators with power series coefficients. *Journal of Symbolic Computation*, vol. 24, n° 1, 1997, pp. 1–30.

[13] Weil (Jacques-Arthur). – Absolute factorization of differential operators. In Salvy (Bruno) (editor), *Algorithms Seminar, 1996–1997*, *INRIA Research Report*, pp. 33–36. – 1997.

An Intermediate Value Property for First-Order Differential Polynomials

Lou van den Dries
University of Illinois

June 28, 1999

[summary by Philippe Dumas & Bruno Salvy]

A theorem of Rubel [4] shows that solutions of algebraic differential equations can present pathological asymptotic behaviours. Therefore when studying differential equations from an asymptotic viewpoint it is natural to restrict to solutions obeying extra smoothness conditions. A convenient context for these questions is provided by Hardy fields, which are defined below. A typical differential equation dealt with by the techniques of this work is

$$F(x,y,y') = (x+y^2)y'^3e^x + yy'\log x + y^4 - e^{e^x} = 0.$$

It is easily seen that for $y = e^{e^x}$, $F(x,y,y')$ is asymptotically positive, while for $y = x$, $F(x,y,y')$ is asymptotically negative. It is therefore natural to wonder whether there exists a solution to this equation whose growth is between that of x and of e^{e^x}. The work summarized here [5] gives a positive answer to this question, and proves that there exists such a solution in a Hardy field.

1. Hardy Fields

A *Hardy field* is a field closed under differentiation, whose elements are germs at ∞ of real-valued functions [1]. (Think of it as the set of possible asymptotic behaviours.) Examples of Hardy fields are the field $\mathbb{R}$ of (germs of) constant functions, the field $\mathbb{R}(x)$ of (germs of) rational functions over $\mathbb{R}$. Hardy fields are named after G. H. Hardy, who proved in [2] that exp-log functions (i.e., functions obtained from $\mathbb{R}(x)$ by field operations, the functions exp and $\log|.|$) form a Hardy field.

The main constraint here is that non-zero elements of Hardy fields have to be invertible, and thus cannot have arbitrarily large zeros. Consequently, since their derivatives belong to the field, they have to be ultimately monotonic and tend to a possibly infinite limit. Also, differences of two (germs of) functions of a Hardy field are also in the field and possess a limit, so that this field is ordered. A Hardy field $\mathbb{K}$ can be extended by a C^∞ function y if for all polynomials $P \in \mathbb{K}[Y]$, $P(y)$ is either 0 or does not have arbitrarily large zeros. A Hardy field $\mathbb{K}$ can be extended by real solutions of polynomials in $\mathbb{K}[Y]$ and by antiderivatives of elements of $\mathbb{K}$ [3]. This is how exp-log functions can be built from $\mathbb{R}(x)$.

The order induces a natural topology, a basis of the open sets being given by the open intervals. Thus continuous functions are defined and for instance, the differentiation operator is continuous since $y' > f$ implies $y > \int f$. This is an open set since the field can be extended by $\int f$ if necessary.

The aim of this work is to prove the following.

Theorem 1. *Let K be a Hardy field and $F \in \mathbb{K}[x,y]$. Assume there exist ϕ and ψ in $\mathbb{K}$ such that $F(\phi,\phi') < 0 < F(\psi,\psi')$. Then there exists η in a Hardy field extension of $\mathbb{K}$ such that $F(\eta,\eta') = 0$.*

The function $y \mapsto F(y,y')$ is continuous, but in general Hardy fields are not Archimedean (consider 1 and x in $\mathbb{R}(x)$). Consequently, the intermediate value theorem may not hold. The proof consists in lifting properties of continuous functions over $\mathbb{R}$ to Hardy fields. The same question for higher-order differential polynomials is still a conjecture.

2. Basic Case

We first consider equations of the form

$$y'(x) = G(x, y(x)), \tag{1}$$

where G is C^1 in the neighborhood of $\mathcal{S} = \{(x, y), r \leq x, a(x) \leq y \leq b(x)\}$, for some $r \in \mathbb{R}$ and a and b in a Hardy field $\mathbb{K}$ giving different signs to $y'(x) - G(x, y(x))$. A simple reasoning based on the intermediate value theorem shows the existence of a C^1 solution $\eta(x)$ of (1) with $a(x) < \eta(x) < b(x)$ for $x \geq r$.

If, moreover, $x \mapsto G(x, h(x))$ belongs to $\mathbb{K}$ for all h in $\mathbb{K}$, then η belongs to an extension of $\mathbb{K}$. This is proved in three steps. First, if η has arbitrarily large zeros then so does $x \mapsto G(x, 0)$ but since this belongs to a Hardy field, we get $G(x, 0) = 0$ and $\eta = 0$ is the unique solution of the differential equation. Next, if $h \neq \eta$ belongs to an extension of $\mathbb{K}$, then $\theta = \eta - h$ cannot have arbitrarily large zeros, using the same argument as before with the equation

$$\theta'(x) = G(x, \theta(x) + h(x)) - h'(x).$$

Noting that any polynomial $P \in \mathbb{K}[Y]$ can be factored in linear factors or quadratic factors with negative discriminant extends this argument to $P(\eta)$ and concludes the proof.

3. General First Order Case

The aim is to reduce the general case $F(y, y') = 0$ to the basic case considered in the previous section. This is achieved through an analogue of the cylindric-algebraic decomposition: the interval (ϕ, ψ) is split into subintervals $\phi = a_1 < \cdots < a_n = \psi$ such that in every interval (a_i, a_{i+1}) there are finitely many functions $f_{i,j}$ algebraic over $\mathbb{K}$ and the polynomial $F(y, z)$ has constant sign in the cell $a_i < y < a_{i+1}$, $f_{i,j}(y) < z < f_{i,j+1}(y)$. Note that everything here also depends on x through the coefficients of F.

It is now sufficient to exhibit two functions a, b, with $a_i < a < b < a_{i+1}$ for some i, such that $a' - f_{i,j}(a) < 0 < b' - f_{i,j}(b)$ for some j. Let A be the set of $y \in (\phi, \psi)$ such that $F(y, y') < 0$ and similarly B for $F(y, y') > 0$. If A (resp. B) has an upper (resp. lower) bound, then this is a solution of the equation and we are done. Otherwise, it is possible to select $a \in A$ and $b \in B$ belonging to the same interval (a_i, a_{i+1}) (if not, one of the a_i's would be a solution of the equation). Necessarily, (a, a') and (b, b') do not belong to the same cell and therefore one of the $f_{i,j}$ fulfills our needs. We denote it f. The reduction to the basic case requires that the application $(x, y) \mapsto f(y)$ be C^1 in the domain $\mathcal{S}$. This follows from the analyticity of the roots of a polynomial equation with respect to its coefficients outside of singular varieties and the C^1 property of these coefficients for x sufficiently large.

Bibliography

[1] Bourbaki (N.). – *Éléments de Mathématiques*, Chapter V: Fonctions d'une variable réelle (appendice), pp. 36–55. – Hermann, Paris, 1961, 2nd edition.

[2] Hardy (G. H.). – *Orders of Infinity*. – Cambridge University Press, 1910, *Cambridge Tracts in Mathematics*, vol. 12.

[3] Rosenlicht (Maxwell). – Hardy fields. *Journal of Mathematical Analysis and Applications*, vol. 93, n° 2, 1983, pp. 297–311.

[4] Rubel (L. A.). – A universal differential equation. *Bulletin of the American Mathematical Society*, vol. 4, n° 3, May 1981, pp. 345–349.

[5] van den Dries (Lou). – An intermediate value property for first-order differential polynomials. – 1999. Preprint.

Part 3

Analysis of Algorithms and Data Structures

Unified Analysis of Euclidean Algorithms

Brigitte Vallée
Université de Caen

March 29, 1999

[summary by Cyril Banderier]

Abstract

The average behavior of nine algorithms derived from the Euclidean Algorithm is analysed. Some of them are useful in computing the Jacobi symbol. It is shown that these algorithms form two classes: the fast and the slow algorithms ($\Theta(\ln N)$) versus $\Theta(\ln^2 N)$). The author suggests a general method, in which the algorithm and the set of its data are viewed as a dynamical system. The Ruelle operator and functional analysis are key tools. This unified approach gives not only the previously known results for classical Euclidean algorithms but also new results about the binary GCD and Jacobi symbol algorithms. In particular, conjectures due to Brent, Bach and Shallit are solved. The average behavior is linked to the entropy of the dynamical system, thus new universal constants (explicit for classical cases, computed numerically in the other cases) are exhibited.

1. Euclidean Algorithms

A previous talk of Brigitte Vallée (see the summary in the proceedings of year 97/98) was devoted to the complete analysis of the binary GCD algorithm. The summary ended by mentioning the application of Vallée's method to the Jacobi Symbol. The last year has seen a unification of the approaches and the reader will find here the analysis of nine algorithms. These are "flip and reduce" algorithms and are more or less variations of the "classical Euclid algorithm", an algorithm which dates from 300BC and which can also be found in a first-century AD Chinese text (Chiu Chang Suan Shu).

Before the "functional analytic number theoretical dynamical systematic" approach of Vallée, the state of the art was due to Brent [1], Knuth [5], Heilbron [4], Dixon [3], Vardi [10], Bach, Shallit [7].

Vallée and her student, C. Lemée, gave some new results for the analysis of the average complexity of the computation of a fundamental function in number theory: the Jacobi symbol, which allows to determine whether a number is a square in a given modular arithmetic or not.

The Legendre symbol is defined for an odd prime number v as

$$(\frac{u}{v}) = \begin{cases} 0, & \text{if } u \equiv 0 \bmod v; \\ 1, & \text{if } v \text{ is a square modulo } v; \\ -1, & \text{if } v \text{ is not a square mod} v. \end{cases}$$

The Jacobi symbol extends the Legendre symbol and is defined as

$$J(u,v) := \prod_{i\in I} (\frac{u}{v_i})^{e_i} \qquad \text{for } v = \prod_{i \in I} v_i^{e_i} \text{ with odd primes } v_i.$$

Of course one does not need to know the factorisation of v in order to compute $J(u,v)$. Instead, one uses the following formulæ:

$$\begin{aligned}
\text{Quadratic reciprocity law:}\quad & J(u,v) = (-1)^{(u-1)(v-1)/4} J(v,u) \qquad \text{for } u,v \text{ odd positive integers,}\\
\text{Modulo law:}\quad & J(v,u) = J(v-bu,u),\\
\text{Multiplicativity law:}\quad & J(vw,u) = J(v,u)J(w,u),\\
\text{Special values:}\quad & J(2,v) = (-1)^{(v^2-1)/8}, \qquad J(\epsilon,u) = \epsilon^{(u-1)/2} \quad \text{for } \epsilon = \pm 1.
\end{aligned}$$

Then one has several Euclidean-like possible algorithms. We distinguish the nine following cases (name, constraints of the algorithm and an example are given):

Classical with positive remainders
$v = cu + r$, $0 \le r < u$

$$\tfrac{13}{75} = \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{3+0}}}}$$

Subtractive classical
$v = u + (v - u)$

$$\tfrac{13}{75} = \cfrac{1}{1+1+1+1+1+ \cfrac{1}{1 + \cfrac{1}{1+1+1+ \cfrac{1}{1+1+1}}}}$$

Classical with negative remainders
$v = cu - r$
$0 \le r < u$

$$\tfrac{13}{75} = \cfrac{1}{6 - \cfrac{1}{5 - \cfrac{1}{2 - \cfrac{1}{2+0}}}}$$

Classical with centred remainders
$v = cu + \epsilon r$
$c \ge 2, \epsilon = \pm 1, (c,\epsilon) \neq (2,-1)$
$0 \le r \le u/2$

$$\tfrac{13}{75} = \cfrac{1}{6 - \cfrac{1}{4 + \cfrac{1}{3}}}$$

Even CF
$v = cu + \epsilon s$,
c even, $\epsilon = \pm 1$ s odd, $0 < s < u$

$$\tfrac{13}{75} = \cfrac{1}{6 - \cfrac{1}{4 + \cfrac{1}{4-1}}}$$

Odd CF
$v = cu + \epsilon 2^k s$,
c odd, $\epsilon = \pm 1$,
s odd, $k \ge 1, 0 \le 2^k s < u$

$$\tfrac{13}{75} = \cfrac{1}{5 + \cfrac{2}{3 - \cfrac{2}{5+0}}}$$

Ordinary CF
$v = cu + 2^k s$, $s = 0$ or s odd,
$k \geq 0$,
$0 \leq 2^k s < u$

$$\frac{13}{75} = \cfrac{1}{5 + \cfrac{2}{2 + \cfrac{1}{1 + \cfrac{2}{3+0}}}}$$

Centred CF
$v = cu + \epsilon 2^k s$,
$s = 0$ or s odd, $k \geq 0$,
$0 \leq 2^k s < u/2$

$$\frac{13}{75} = \cfrac{1}{6 - \cfrac{1}{4 + \cfrac{1}{3+0}}}$$

Binary GCD
$v = au + 2^k r$,
a odd,
$a < 2^k$, $r \leq u$

$$\frac{13}{75} = \cfrac{1}{1 + 2 + \cfrac{2^2}{1 + \cfrac{2^2}{1+2^3}}}$$

2. Functional Analytic Number theory

Performing l steps of one of the above algorithms gives a continued fraction of height l and the expression of the rational u/v as

$$\frac{u}{v} = h_1 \circ h_2 \circ \cdots \circ h_l(\alpha) \tag{1}$$

where α is 1 or 0 and where the h_i's are "linear fractional transformations" or LFT ("homographie" in French). Of course the values of a, b, c, d in $h_i = \frac{az+b}{cz+d}$ depend on the algorithms. What is more, the shape of the first and last LFT can be different from the other "intermediate" generic LFT, depending on the initial and stopping conditions of the algorithm.

Introduce the double Dirichlet generating function

$$S(s, w) := \sum_{l \geq 1} \sum_{n > 1} \frac{\nu_n^{[l]}}{n^s} w^l$$

where $\nu_n^{[l]}$ is the number of rationals of Ω (set of valid inputs in [0,1] or [0,1/2], depending on the algorithm) of the form u/n which give a continued fraction of height l. Defining a_n and b_n by

$$S(s,1) =: \sum_{n>1} \frac{a_n}{n^s} \qquad \text{and} \qquad \frac{\partial}{\partial w} S(s,w)|_{w=1} =: \sum_{n>1} \frac{b_n}{n^s}$$

allows to express S_N, the average number of steps of the algorithm on the rationals u/v of Ω for $u \leq N$, as

$$S_N = \frac{\sum_{n \leq N} b_n}{\sum_{n \leq N} a_n} = \frac{\sum_{n \leq N} \sum_{l \geq 0} l \nu_n^{[l]}}{\sum_{n \leq N} \sum_{l \geq 0} \nu_n^{[l]}}.$$

Thus the average behavior of the algorithm is dictated by the asymptotics of partial sums of coefficients of the function S.

For any Dirichlet series $F(s)$ with nonnegative coefficients a_n converging in $\Re(s) > \sigma > 0$, a theorem of Delange gives

$$\sum_{n \leq N} a_n = \frac{A}{\sigma \Gamma(\gamma+1)} N^\sigma \ln^\gamma N (1 + o(N)).$$

As for any Tauberian theorem, $F(s)$ has to fulfill some hypotheses (analyticity on $\Re(s) = \sigma$ for $s \neq \sigma$ and there exist A, B analytic at σ such that $F(s) = A(s)(s-\sigma)^{-\gamma-1} + B(s)$). A major part of the the work consists in proving that these properties hold.

Recall that for each algorithm, there are 4 sets of LFT: the single LFT's $\mathcal{K}$, the initial LFT's $\mathcal{I}$, the final LFT's $\mathcal{F}$ and the intermediate LFT's $\mathcal{H}$. Now define the "Ruelle operator" A relative to a set $\mathcal{A}$ of LFT's by

$$A_s(f) = \sum_{h \in \mathcal{A}} \frac{f \circ h}{\mathrm{denom}(h)^s}.$$

The decomposition of an algorithm as a single LFT or as final+sequence(intermediate)+initial LFT's (for short $\mathcal{K} + \mathcal{F}\mathcal{H}^*\mathcal{J}$) leads to $S(s, w) = wK_s(1)(\alpha) + w^2 F_s \circ (I - wH_s)^{-1} \circ J_s(1)(\alpha)$ (where α is defined as in equation 1 and where $\circ$ is the composition over the space of operators). Variations for Markovian cases are possible and lead to the same treatment.

Finally, spectral properties of $I - H_s$ allow to determine $\sigma = 2$ and $\gamma = 1$ or 2 (in some cases, one needs to choose an adequate functional space in order to establish this).

Here is a summary of the average number of steps performed by the nine algorithms:

positive remainders	$\frac{12 \ln 2}{\pi^2} \ln N$	$.842 \ln N$	Heilbron & Dixon 70
subtractive	$\frac{6}{\pi^2} (\ln N)^2$	$.607 (\ln N)^2$	Knuth & Yao 75
negative remainders	$\frac{3}{\pi^2} (\ln N)^2$	$.303 (\ln N)^2$	Vardi 92
centred remainders	$\frac{12 \ln \phi}{\pi^2} \ln N$	$.585 \ln N$	Rieger 80
even	$\frac{2}{\pi^2} (\ln N)^2$	$.202 (\ln N)^2$	Vallée & Lemée 98
odd	$A_O \ln N$	$.435 \ln N$	Vallée & Lemée 98
ordinary	$A_U \ln N$	$.535 \ln N$	Vallée & Lemée 98
centred	$A_C \ln N$	$.430 \ln N$	Vallée & Lemée 98
binary GCD	$A_B \ln N$	$.555 \ln N$	Vallée 98

The author also makes the link between the constants given here and the entropy of the dynamical system related to the algorithm.

The results presented here are mainly in [9] and in a preprint of Brigitte and her student [6]. Like other preprints of the author, it is available at her home page
`http://www.info.unicaen.fr/~brigitte/Publications/`

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] Shallit (Jeffrey). – Origins of the analysis of the Euclidean algorithm. *Historia Mathematica*, vol. 21, n° 4, 1994, pp. 401–419.

[8] Vallée (Brigitte). – The complete analysis of the binary Euclidean algorithm. In *Proceedings ANTS'98*. – 1998.

[9] Vallée (Brigitte). – A Unifying Framework for the Analysis of a Class of Euclidean Algorithms. In *Proceedings FOCS'99*. – 1999.

[10] Vardi (Ilan). – Dedekind sums have a limiting distribution. *Duke Mathematical Journal*, n° 1, 1993, pp. 1–12.

An Approximate Probabilistic Model for Structured Gaussian Elimination

Edward A. Bender
Department of Mathematics, University of California, San Diego

November 2, 1998

[summary by François Morain]

1. Introduction

Modern algorithms [5, 7] for factoring integers or for solving discrete logarithms problems work in two phases. In the first one, one collects a huge amount of data that help create a large matrix that is triangularized in the second phase. For instance, the largest non-trivial number ever factored as of today is $(10^{211}-1)/9$, which involved finding dependencies in a $4,820,249 \times 4,895,741$ boolean matrix (see [2]). The easiest way to solve the problem is to find a computer with enough memory so that the matrix fits in core and Gaussian elimination can be used. If such a behemoth is not available, alternative methods have to be used. A method that is widely used relies on the fact that the matrix we are interested in is sparse. For instance the matrix referred to above has only 48.1 non-zero coefficients per row on average. Moreover the structure of the matrix is very peculiar: the leftmost columns are very dense, while the rightmost ones are very sparse. This has led several authors to work out what is called the *Structured Gaussian Elimination* (SGE) method. Apart from this approach, one can use two probabilistic iterative methods to solve the problem, namely Wiedemann's method [9] or Lanczos's [6]. In practice, these approaches are commonly combined.

We will concentrate here on linear algebra for integer factorization. For the discrete logarithm problem, the same ideas can be used with some (sometimes not so trivial) modifications. The aim of the talk is to describe one variant of SGE and try to analyse it.

2. Integer Factorization and Linear Algebra

Suppose we want to factor a large integer N. The basic idea is to look for two integers X and Y such that $X^2 \equiv Y^2 \bmod N$, but $X \not\equiv \pm Y \bmod N$. If this is the case, then $\gcd(X-Y,N)$ is a non-trivial factor of N. How do we proceed to find X and Y? This is usually done using a combination of congruences of the type:

$$x_i^2 \equiv \prod_{j=1}^{k} p_j^{\alpha(i,j)} \bmod N \tag{1}$$

where the p_j's are prime numbers forming the factor basis $\mathcal{B} = \{p_1, p_2, \ldots, p_k\}$. Now we look for a subset I of these such that $\prod_i \prod_j p_j^{\alpha(i,j)}$ is the square of an integer, say Y^2, leading to $\left(\prod_{i\in I} x_i\right)^2 \equiv Y^2 \bmod N$ and we have solved our problem. The method of generation of the auxiliary congruences (1) vary from an algorithm to the other, see the references given above for more details.

Finding a subset I boils down to a linear algebra problem. Indeed, $\prod_i \prod_j p_j^{\alpha(i,j)}$ is the square of an integer if and only if $\prod_j p_j^{\sum_i \alpha(i,j)}$ is, or equivalently, $\sum_i \alpha(i,j)$ is an even integer for all j, which in turn is equivalent to the fact that we have found a relation between some rows of the matrix $M = (m_{i,j})$ where $m_{i,j} = \alpha(i,j) \bmod 2$, that is a vector x such that $xM = 0$.

What is the shape of the matrix? It is rather easy to guess that a prime number p_j occurs in a factorization with probability $O(1/p_j)$. If we number our primes w.r.t. their magnitude, the left columns of M are seen to be much more dense than the right ones.

3. Structured Gaussian Elimination

The idea of the method [4, 8] is to try to perform Gaussian elimination on the sparse part of the matrix, as long as the fill-in is not too important. We will present here the version given in [1][1]. The *weight* of a row (resp. column) is the number of its non-zero coefficients.

Step 0. [Initial deactivation] deactivate some (small) fraction of the columns and call all remaining columns *light*.

Step 1. [Initial clean up] repeat the following steps (a) and (b) until all columns have weight greater than 1:

(a) Eliminate columns of weight 0 (it is of no use).

(b) If a column has weight 1, eliminate it and the row intersecting it (since it cannot be part of a dependency).

Step 2. [Deactivation] repeat steps (a) and (b) until all columns have been either deactivated or eliminated:

(a) If any row has weight 1, eliminate it and the light column intersecting it. Repeat as often as possible.

(b) Deactivate a column of high weight and repeat (a).

Step 3. [Final step] Find the dependencies of the small matrix and build back the solutions of the initial system.

This algorithm is an iterative process that decreases the size of the matrix. It can happen that more and more rows are eliminated in Step 2a, leading to what is called a "catastrophe" in [8]. Among the questions we ask are: what is the size of the smallest reduced matrix that we can obtain before the catastrophe begins?

4. Branching Processes and the Critical Product

Let us review the basic properties of a Galton-Watson branching process, in the view of applying it to SGE. Theoretical properties on this topic can be found in [3, pp. 3–7].

In a Galton-Watson branching process, time is divided into generations. We start with one object alive in the 0th generation and at generation i, the number of objects depends on the number of objects in generation $i-1$. Let $f(x)$ denote the probability generating function of this number. The probability generating function for the number of objects in the nth generation is $f_{(n)}(x) = f(f(\cdots f(f(x))\cdots))$. Therefore, the expected number of objects in the nth generation is

$$(f_n(x))'\big|_{x=1} = (f'(1))^n = \varphi^n.$$

This quantity φ acts as a threshold. If $\varphi \leq 1$, the process terminates with probability 1, whereas if $\varphi > 1$, the process has a nonzero probability of surviving forever.

How do we apply this theory to our problem? In Step 2a of the algorithm, an object is a row of weight 1 that disappears and may create new objects of weight 1 for the next generation. The associated value φ (called the *critical product*) of this branching process is given by:

[1]There is no *canonical* algorithm for SGE: from the same idea, details can differ in the implementation and the choice of some parameters.

Theorem 1. *Assuming that the rows and columns are independent, we have*

$$\varphi \approx \left(\frac{\sum_k k(k-1)c_k}{\sum_k kc_k}\right)\left(\frac{2r_2}{\sum_k kr_k}\right),$$

where c_k (resp. r_k) is the probability that a randomly chosen column (resp. row) contains exactly k nonzero entries and the approximation is due to the fact that the matrix is finite.

For our purpose, we see that if $\varphi > 1$, then our algorithm loops forever and the catastrophe occurs.

5. Critical Parameters and their Analysis

5.1. **Probability Model.** Let $M = (m_{i,j})$ denote our $m \times n$ matrix. We make the assumption that $\mathrm{Prob}(m_{i,j} \neq 0) = D/j$ for some fixed parameter D. This sounds realistic since the column j of M is related to the prime $p_j \approx j \log j$ dividing some number, thus with probability $1/p_j \approx D/j$ since log is a slowly increasing function. On the other hand, a reasonable model for the weight of rows is that of a Poisson model. We will let $C = Dm/n$.

5.2. **Effect of the Initial Clean Up.** This step causes $n\alpha_1$ columns (and corresponding rows) of weight 1 and $n\alpha_0$ columns (and no rows) of weight 0 to be eliminated. At the end of this step, one gets a new matrix with $m - n\alpha_1$ rows and $n(1 - \alpha_0 - \alpha_1)$ columns.

Theorem 2. *One has:*

$$\alpha_1 \approx \overline{\alpha}_1 = \frac{CE_1(C)}{1 - D(E_0(C) - E_1(C))}, \qquad \alpha_0 \approx CE_2(C) + DE_1(C) \times \overline{\alpha}_1,$$

where $E_r(C) = \int_C^\infty e^{-t}t^{-r}\,dt$ is the exponential integral.

Numerically, for $m/n = 1.0$ and $D = 3.0$, this yields $\alpha_0 = 0.012$ and $\alpha_1 = 0.044$. More generally, the values of α_0 and α_1 are rather small. Moreover, the new matrix will have the same shape as the original one, meaning that the Poisson model will still apply.

5.3. **Matrix After Reduction.** What happens in our case is that the value of φ increases from one iteration of the algorithm to the other, reaching a value > 1 and thus causing a catastrophe. We are interested in the parameters associated with the matrix when this occurs. We suppose we enter Step 2 of the algorithm with an $m \times n$ matrix $M = (m_{i,j})$. At Step 2b, we suppose that some fraction τ of the columns have been deactivated and eliminated. For simplicity, assume these are the leftmost τn columns of M. We want to relate τ and φ.

We suppose that our model is still valid for M, and in particular the model used for the row weight is again a (truncated, since there are no rows of weight 0 or 1) Poisson model of parameter λ. We first have:

Theorem 3. *With the notations above:*

$$-D\log\tau \approx \lambda\left(\frac{e^\lambda - 1}{e^\lambda - \lambda - 1}\right).$$

From this, one gets:

Theorem 4. *Letting $C = Dm/n$, one has*

$$\varphi \approx \frac{C(1-\tau)}{-\tau\log\tau}\frac{\lambda}{e^\lambda - 1}.$$

This formula enables one to compute the value τ_0 corresponding to $\varphi = 1$, i.e., when a catastrophe occurs. For instance, when $m/n = 1.0$ and $D = 3.0$, $\tau_0 = 0.318$. In any case, τ_0 is always far from 0, which indicates that the SGE algorithm ends up with a matrix of size proportional to that of the original matrix.

5.4. **Final Matrix.** By final, we understand the matrix which is rebuilt after SGE and to which we need apply another linear algebra algorithm. Among the τn columns discarded in Step2 of the algorithm, a fraction δ of them were deactivated (a remaining $\tau - \delta$ having been eliminated), therefore being eligible to the final matrix.

Theorem 5. *With the notations above:*

$$\delta(\tau) \approx \int_0^\tau \left(1 + \frac{C\lambda}{\tau(1-\varphi)(e^\lambda - 1)}\right)^{-1} d\tau.$$

For the same numerical values, $m/n = 1.0$ and $D = 3.0$, one finds $\delta_0 = 0.186$. This again shows that the final matrix is of size proportional to that of the original matrix.

6. Conclusions

The authors have attempted an analysis of the structured Gaussian elimination. With rather crude assumptions, they were able to derive an approximate model that is close, at least qualitatively, to that observed by their own simulations as well as by people who really factor numbers. Going further, that is have a model close to reality in quantity would require more work.

Bibliography

[1] Bender (Edward A.) and Canfield (E. Rodney). – An approximate probabilistic model for structured Gaussian elimination. *Journal of Algorithms*, vol. 31, n° 2, 1999, pp. 271–290.

[2] CABAL. – 211-digit SNFS factorization. – `ftp://ftp.cwi.nl/pub/herman/NFSrecords/SNFS-211`, April 1999.

[3] Harris (T. E.). – *The theory of branching processes.* – Dover Publications, 1989.

[4] LaMacchia (B. A.) and Odlyzko (A. M.). – Solving large sparse linear systems over finite fields. In Menezes (A. J.) and Vanstone (S. A.) (editors), *Advances in Cryptology. Lecture Notes in Computer Science*, vol. 537, pp. 109–133. – Springer-Verlag, 1990. Proceedings Crypto '90, Santa Barbara, August 11–15, 1988.

[5] Lenstra (A. K.) and Lenstra, Jr. (H. W.) (editors). – *The development of the number field sieve.* – Springer, *Lecture Notes in Mathematics*, vol. 1554, 1993.

[6] Montgomery (P. L.). – A block Lanczos algorithm for finding dependencies over GF(2). In Guillou (L. C.) and Quisquater (J.-J.) (editors), *Advances in Cryptology – EUROCRYPT '95*, *Lecture Notes in Computer Science*, vol. 921, pp. 106–120. – 1995. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.

[7] Pomerance (Carl) (editor). – *Cryptology and computational number theory.* – American Mathematical Society, Providence, RI, 1990, xii+171p. Lecture notes prepared for the American Mathematical Society Short Course held in Boulder, Colorado, August 6–7, 1989, AMS Short Course Lecture Notes.

[8] Pomerance (Carl) and Smith (J. W.). – Reduction of huge, sparse matrices over finite fields via created catastrophes. *Experimental Mathematics*, vol. 1, n° 2, 1992, pp. 89–94.

[9] Wiedemann (Douglas H.). – Solving sparse linear equations over finite fields. *IEEE Transactions on Information Theory*, vol. 32, n° 1, 1986, pp. 54–62.

The Probability of Connectedness

Edward A. Bender
Department of Mathematics, University of California, San Diego

November 2, 1998

[summary by Bruno Salvy]

A graph is a set of connected components. Graphs of various kinds are obtained by imposing constraints on these components. If c_n is the number of different components of size n and a_n the number of graphs of size n, then c_n/a_n is the probability that a graph selected uniformly at random among all graphs of size n is connected. The aim of this work is to study to what extent structural properties of the sequence $\{c_n\}$ make it possible to determine the asymptotic probability of connectedness (as the size n tends to infinity).

The asymptotic properties of c_n/a_n are closely related to properties of the generating functions of these sequences. Two cases are to be considered. In the *labelled* case, the generating functions under study are

$$A(x) = \sum_{n\geq 0} a_n \frac{x^n}{n!}, \qquad C(x) = \sum_{n\geq 0} c_n \frac{x^n}{n!}$$

and they are connected by

$$A(x) = \exp(C(x)). \tag{1}$$

In the *unlabelled* case, the generating functions are

$$A(x) = \sum_{n\geq 0} a_n x^n, \qquad C(x) = \sum_{n\geq 0} c_n x^n$$

and they are connected by

$$A(x) = \exp\left(C(x) + C(x^2)/2 + C(x^3)/3 + \cdots\right). \tag{2}$$

(See for instance [3] for a proof.) From the asymptotic point of view, these two identities are sufficiently close to make most of the proofs go through from one case to the other, with technical complications in the unlabelled case.

Example. General labelled rooted trees with n vertices are counted by n^{n-1}. The exponential generating function is the tree function $T(z)$ defined by

$$T(z) = z\exp(T(z)).$$

The corresponding forests have generating function $\exp(T(z)) = T(z)/z$. The dominant singularity of $T(z)$ is $\exp(-1)$ where the singularity is of square root type. Singularity analysis then shows that the asymptotic probability of connectedness is $\exp(-1)$.

	possible values for (ρ_ℓ, ρ_u)
$R = 0$	$[0,1] \times \{1\}$
C divergent at R	$\{0\} \times [0,1]$
C convergent at R	$[0,1) \times (0,1]$ with $\rho_\ell \leq \rho_u$

TABLE 1. Conjectured possibilities for (ρ_ℓ, ρ_u)

Let R be the radius of convergence of the series $C(x)$. In the unlabelled case, since the c_n are integers, $R \leq R_{\max} = 1$, while $R_{\max} = \infty$ in the labelled case. It is useful to distinguish three situations: $R = 0$, C converges at R, or C diverges at R (which can be infinite). Defining

$$\rho_\ell = \liminf_{n\to\infty} c_n/a_n, \qquad \rho_u = \limsup_{n\to\infty} c_n/a_n,$$

the aim of this work is to study when $\rho_\ell = \rho_u$ and to show as much as possible of Table 1.

A first result in this area is the following.

Theorem 1 ([5]). *A necessary and sufficient condition for asymptotic connectedness ($\rho_\ell = \rho_u = 1$) is that $R = 0$ and*

$$\sum_{i=1}^{n-1} h_i h_{n-i} = o(h_n) \tag{3}$$

where h_n is any of a_n or c_n.

Note that (3) is satisfied with $h_n = a_n$ if and only if it is satisfied with $h_n = c_n$.

Example. General undirected graphs with n vertices are enumerated by $a_n = 2^{n(n-1)/2}$ which accounts for all choices of edges. The theorem shows that $c_n \sim a_n$.

The remainder of this summary is devoted to proving parts of Table 1.

1. It is Always Possible that $\rho_\ell = 0$ and $\rho_u = 1$

This is shown by constructing an *ad hoc* sequence c_n which is 1 for most n and very large at rare points. Then a_n tends to infinity so that $\rho_\ell = 0$ and $\rho_u = 1$ because for those large c_n, $a_n \sim c_n$.

This idea might extend to obtain $0 = \rho_\ell < \rho_u < 1$ by taking more frequent large c_n in order to break the last equivalence.

2. Divergent Case: $\rho_\ell = 0$

This is a result of [4], which is proved as follows. If there exists $\delta > 0$ such that $c_n > \delta a_n$ for all n sufficiently large, then we get for $0 \leq z < R$

$$C(z) > \delta e^{C(z)(+\cdots)} + P(z),$$

where P is a polynomial and the dots indicate more positive terms that are present in the unlabelled case. In both cases, this inequality implies that C is convergent at R.

3. **Convergent Case:** $\rho_u > 0$ **and** $\rho_\ell < 1$

The second inequality is a consequence of Wright's theorem.

The first one can be proved as follows in the labelled case. Differentiating (1) and extracting coefficients yields

$$\frac{a_n}{n!} = \frac{1}{n}\sum_{k=0}^{n} k\frac{c_k}{k!}\frac{a_{n-k}}{(n-k)!}.$$

If $c_n = o(a_n)$, then cutting the sum at $n^{1/2}$ and using $c_k \le a_k$ in the first part shows that

$$[x^n]A(x) = o([x^n]A(x)^2),$$

which implies divergence of A at R.

4. **When** $\rho_\ell = \rho_u$

The result is that every time (ρ, ρ) is present in Table 1, then there are sequences a_n and c_n of nonnegative integers making this happen. The first two lines of the table are dealt with by exhibiting appropriate examples: general labelled graphs for the first one; partitions of sets for the other one in view of the asymptotics of Bell numbers.

In the convergent case, an important tool is the following theorem.

Theorem 2. *In the convergent case, if* $\lim c_{n-1}/c_n$ *exists (then it is* R*) and* $\sum_{k=\omega}^{n-\omega} c_k c_{n-k} = o(c_n)$ *for any* $\omega(n) \to \infty$*, then* $\rho_\ell = \rho_u = 1/A(R)$*.*

We first show how this theorem is used to prove that every $\rho \in (0,1)$ is reached in the labelled case. The principle is to construct a sequence of generating functions $C^{[i]}(x)$ such that the coefficients $j![x^j]C^{[i]}(x)$ are nonnegative integers for $0 \le j < i$ and the value of $\lim a_n^{[i]}/c_n^{[i]}$ is ρ. Start with

$$C^{[0]}(x) = \alpha \sum \frac{(x/R)^n}{n^2}.$$

Then by the theorem, $\rho = \exp(-\alpha\pi^2/6)$, which fixes α. To construct $C^{[k+1]}$ from $C^{[k]}$, the coefficient of $k!x^k$ is replaced by its integer part, and the coefficient of x^{k+1} is increased to keep ρ unchanged. The increase is at most $R^{-1}/k!$ which is sufficiently small compared to its original value so that the conditions of the theorem still hold. Therefore the limit $C^{[\infty]}$ also satisfies the theorem. A similar argument gives the unlabelled case.

Proof of the theorem. In the labelled case, the hypothesis is used in an induction on d to obtain the following asymptotic estimates and bounds on $c_n^{(d)} = [x^n]C(x)^d$:

- $c_n^{(d)} < K^{d-1}c_n$ for some K and sufficiently large n;
- $c_n^{(d)} \sim dC(R)^{d-1}c_n$ uniformly for $d \le D(n)$, where $D(n) \to \infty$.

The conclusion follows from there by extracting the coefficient of x^n in $A(x) = \sum C(x)^d/d!$.

A proof in the unlabelled case is given in [2]. □

5. **Conclusion**

Many properties related to connectedness can be deduced from very little information on the counting sequence of the connected components. Much more than indicated here is known if extra smoothness conditions on the sequence are satisfied. Also, results regarding the limiting distribution are known. We refer to [2] for details. Still, a large part of Table 1 remains unproved, mostly regarding the existence of structures with the announced (ρ_ℓ, ρ_u).

Bibliography

[1] Bender (E. A.), Cameron (P. J.), Odlyzko (A. M.), and Richmond (L. B.). – Connectedness, classes and cycle index. *Combinatorics, Probability and Computing*, vol. 8, 1999, pp. 31–43.

[2] Bender (Edward A.), Cameron (Peter J.), and Richmond (L. Bruce). – Asymptotics for the probability of connectedness and the distribution of number of components, 1999. Preprint.

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

[4] Cameron (Peter J.). – On the probability of connectedness. *Discrete Mathematics*, vol. 167/168, 1997, pp. 175–187.

[5] Wright (E. M.). – A relationship between two sequences. *Proceedings of the London Mathematical Society*, vol. 17, 1967, pp. 296–304.

On Random Combinatorial Structures and the Local Time of some Brownian Functionals

Bernhard Gittenberger
Technische Universität Wien, Austria

May 17, 1999

[summary by Philippe Flajolet]

Two methods are presented in order to derive an integral representation of the multi-dimensional densities of the local times of Brownian excursion and reflected Brownian bridge. One is a direct method based on Kac's formula for Brownian functionals, the other is indirect and it uses the fact that functionals for Galton-Watson trees and random mappings yield corresponding Brownian functionals (on excursions and bridges respectively) as a limit. The latter approach relies on generating functions and singularity analysis. The presentation is based on joint works with Guy Louchard (Brussels).

1. Introduction

Brownian motion (BM) models discrete random walks on the integers upon a time normalization by the walk length n and a space normalization proportional to $\sqrt{n}$. Brownian excursion (BE) models walks constrained to start and end at level 0 and not allowed to become negative. Brownian Bridge (BB) corresponds to the constraint that the initial and final altitudes are the same (0, say). The problem tackled here is that of characterizing the amount of time an excursion or a bridge spends at various altitudes. Technically, the *local time* of the process $x(t)$ at a is

$$T^+(t,a) = \lim_{\epsilon\to 0} \frac{1}{\epsilon} \int_0^t I_{[a,a+\epsilon]}(x(s))\,ds,$$

where $I_P(\cdot)$ is the indicator function of the predicate P.

Two methods are employed here in a complementary manner: (i) Kac's formula for Brownian functionals; (ii) singularity analysis applied to generating functions of simple random walks.

2. Kac's Formula

The starting point here is Kac's formula that relates the expectation of a functional of Brownian motion and the solution of an associated second order differential equation. Consider the functional

$$u_\alpha(a) = \mathbb{E}_a \int_0^\infty e^{-\alpha t} \exp\left(-\int_0^t h[x(s)]\,ds\right) f(x(t))\,dt,$$

that is determined by h and f. (There, $\mathbb{E}_a$ means expectation when the process is conditioned by the initial value $x(0) = a$.) Then, the value $u_\alpha(a)$ is a solution to the second order differential equation

$$(1) \qquad (\alpha - \mathcal{G})u = f, \qquad \mathcal{G}[u](a) = \frac{1}{2}u''(a) - h(a)u(a).$$

For instance setting $h(x) = x$ establishes the connection between area problems and Airy functions.

The main result is established in part by means of Kac's formula and Green functions. It constitutes a powerful generalization to d-dimensional motion of the situation for 1-dimensional Brownian excursion, where

$$f_x(y) = \frac{1}{i\sqrt{2\pi}} \int_{1-i\infty}^{1+i\infty} \frac{we^w}{\sinh^2(x\sqrt{w})} \exp\left(-\frac{y}{\sqrt{2}} \frac{\sqrt{w}e^{x\sqrt{2w}}}{\sinh(x\sqrt{w})} \right) dw$$

is the density function of $T^+(1, x)$. (See [1] and [2] for statements.) What is interesting is the companion use of discrete models in the proof, as discussed below.

3. Random Trees and Discrete Walks

One can also approach properties of Brownian excursion from the discrete version provided by simple random walks, where the steps are only of type ± 1. In that case, useful combinatorial decompositions are available. The problem of the time spent at various altitudes for BE is rephrased as the problem of determining the number of times a fixed set S of levels are traversed by a discrete walk. (If one prefers, the corresponding distribution is also the distribution of the total number of nodes at altitude in S in a "general" random tree, given the usual combinatorial correspondence between trees and simple walks.) First, the discrete model is exactly solvable since one knows the generating function where u_j marks traversal of level j,

$$G(u_0, u_1, \dots; z) = \cfrac{zu_0}{1 - \cfrac{zu_1}{1 - \cfrac{zu_2}{\ddots}}}.$$

Second, upon rescaling, when the levels in S are of the form $x_j\sqrt{n}$, the function G renormalizes nicely for z near the relevant singularity $\frac{1}{4}$. In that case, contour integration in the style of Flajolet and Odlyzko's singularity analysis techniques yields the result. The end product is the formula already alluded to for *the d-dimensional density for the local time of Brownian excursion.*

4. Applications

The results obtained provide information of any algorithm or computer system that is modelled in the limit by Brownian excursions. Naturally, this applies to the $M/M/1$ model of queueing theory fame. It also applies to detailed aspects of tree traversals, to shellsort (in fact, the phase of sorting a 2-ordered permutation), and to the analysis of dynamic data structures under random evolutions (Françon's model of "histories"), especially of the stack variety.

Bibliography

[1] Gittenberger (Bernhard) and Louchard (Guy). – The Brownian excursion multi-dimensional local time density. – Preprint, 1999.

[2] Gittenberger (Bernhard) and Louchard (Guy). – On the local time density of the reflecting Brownian bridge. – Preprint, 1999.

On a Quasi-Optimal Search Algorithm and the Jacobi Theta Function

Philippe Chassaing

Institut Élie Cartan, Nancy

November 23, 1998

Abstract

A. Odlyzko has examined the performance of various strategies for seaching maxima or zeros in an unknown environment. He gave an algorithm which is quasi-optimal in average for finding the maximum of a random walk. In the same context, using an enumeration due to Odlyzko, this works shows that the limit law of the cost of the search is the same one for all quasi-optimal algorithms. This law is characterized in terms of the Jacobi theta functions and of the Brownian motion.

This is joint work with Jean-François Marckert and Marc Yor.

Bibliography

[1] Chassaing (P.), Marckert (J.-F.), and Yor (M.). – A stochastically quasi-optimal algorithm. – Preliminary version available at `http://altair.iecn.u-nancy.fr/ marckert/maxstoch.ps`, 1998.

2D Pattern Matching Image and Video Compression

Wojciech Szpankowski
Purdue University

June 21, 1999

Abstract

We propose a lossy data compression framework based on an approximate two dimensional pattern matching (2D-PMC) extension of the Lempel-Ziv lossless scheme. This framework forms the basis upon which higher level schemes relying on differential coding, frequency domain techniques, prediction, and other methods can be built. We apply the pattern matching framework to image and video compression and report on theoretical and experimental results. Theoretically, we show that the fixed database model used for video compression leads to suboptimal but computationally efficient performance. The compression ratio of this model is shown to tend to the generalized entropy defined in this paper. For image compression we use a growing database model for which we provide an approximate analysis. The implementation of 2D-PMC is a challenging problem from the algorithmic point of view. We use a range of techniques and data structures such as k-d trees, generalized run length coding, adaptive arithmetic coding, and variable and adaptive maximum distortion level to achieve good compression ratios at high compression speeds. We demonstrate bit rates in the range of 0.25-0.5 bpp for high quality images and data rates in the range of 0.15-0.5 Mbps for a baseline video compression scheme that does not use any prediction or interpolation. We also show that this asymmetric compression scheme is capable of extremely fast decompression making it particularly suitable for networked multimedia applications.

This is a joint work with M. Alzina (ENST, France) and A. Grama (Purdue).

Part 4

Probabilistic Methods

On the Width of Labeled Trees

Jean-François Marckert
Université de Nancy 1

April 12, 1999

[summary by Christine Fricker]

Abstract

We consider A_n the set of all rooted labeled trees with n nodes. We denote by Z_i the number of nodes at distance i from the root and by $W_n = \max_{0 \le i \le n} Z_i$ the width of the tree. The aim of the talk is to present results on convergence of moments of W_n (correctly renormalized) to those of the maximum of the normalized Brownian excursion and to give a tight bound for the rate of convergence. For the proof, the connections between especially breadth first search random walk on trees, random walk with Poissonian increment, parking function and empiric process of mathematical statistics are described.

The results presented in this talk were obtained jointly with P. Chassaing.

1. Introduction

A rooted labeled tree with n nodes is a connected graph with n vertices and $n-1$ edges where a vertex, the root, is specified. Tight bounds of the width W_n of rooted labeled trees with n nodes are given, answering an open question of Odlyzko and Wilf [3] that $E(W_n)$ is between $C_1\sqrt{n}$ and $C_2\sqrt{n \log n}$. More precisely, we first present the result of Takacs [6] that $W_n/\sqrt{n}$ converges in distribution to the maximum m of the Brownian excursion, with the well-known theta distribution given by

$$\Pr(m \le x) = \sum_{k \in \mathbb{Z}} (1 - 4k^2x^2)e^{-2k^2x^2}.$$

However weak convergence does not answer completely the question of Odlyzko and Wilf. To fill this gap, we prove that

Theorem 1. *For all $p \ge 1$, $\left|E(W_n^p/n^{p/2}) - E(m^p)\right| \le C_p n^{-1/4}\sqrt{\log n}$ where m is the maximum of the normalized Brownian excursion.*

The moments of m are well-known and given by

$$E(m^p) = p(p-1)\Gamma(p/2)\zeta(p)2^{-p/2}.$$

For this we prove that there exists a sequence of normalized Brownian excursions of maximum m_n such that, for all $p \ge 1$,

$$E(\left|W_n/\sqrt{n} - m_n\right|^p) \le C'_p n^{-p/4}\sqrt{\log n}$$

using that if q is defined by $1/p + 1/q = 1$ and if X and Y are two real random variables in L_p, then by Holder's inequality,

$$|E(X^p) - E(Y^p)| \le p \left\|X - Y\right\|_p \left\|X + Y\right\|_p^{p/q}.$$

2. Relation Between Rooted Labeled Trees and Parking Functions

In hashing with linear probing or parking, we consider n cars c_i ($1 \le i \le n$) arriving in this order at random in $n+1$ places $\{0, 1, \ldots, n\}$, where car c_i is parking on its place h_i if h_i is still empty, otherwise car c_i is trying places $h_{i+1} \bmod n+1, \ldots$. We consider parking functions, i.e. sequences $(h_i)_{1 \le i \le n}$ such that place n is empty. A parking function is alternatively characterized by the sequence $(A_k = \{i, h_i = k\})_{0 \le k \le n}$ of sets of cars that arrive on place k, with $x_k = \operatorname{card} A_k$. If y_k is the number of cars that tried once to park on place k,

$$y_k = y_{k-1} - 1 + x_k, \qquad y_0 = x_0.$$

The fact that place n is the empty place is given by

$$y_k \ge 1 \quad (0 \le k \le n-1), \qquad y_n = 0$$

or equivalently

$$\sum_{i=0}^{k} x_i - k \ge 1 \quad (0 \le k \le n-1), \qquad \sum_{i=0}^{n} x_i - n = 0. \tag{1}$$

A labeled tree with vertices $\{0, 1, \ldots, n\}$ rooted at 0 is also characterized by the sequence of disjoint sets $(A_k)_{0 \le k \le n}$ whose union is $\{1, \ldots, n\}$ and the $x_k = \operatorname{card} A_k$ satisfying (1). Indeed, A_k ($k \ge 1$) (respectively A_0) is defined as the set of new neighbors of the smallest element in A_{k-1} (respectively 0) and (1) is the condition for the tree to be connected and to have root 0. The number of A_k ($k \ge 1$) with cardinality x_k ($k \ge 1$) is proportional to the product of Poisson probabilities $e^{-1}/x_k!$. In other words the corresponding unlabeled tree is a Galton-Watson tree with Poisson(1) progeny, constrained to have $n+1$ nodes. Thus, the sequence $y = (y_k)_{0 \le k \le n}$ is the discrete excursion with length n of a random walk with increments $x_k - 1$. It is well-known that $(y_{\lfloor nt \rfloor}/\sqrt{n})_{0 \le t \le 1}$ converges in distribution to $(e(t))_{0 \le t \le 1}$ where e is a normalized Brownian excursion and $\max_k y_k/\sqrt{n}$ converges in distribution to $m = \max_{0 \le t \le 1} e(t)$, which is theta-distributed.

The random walk (y_k) (introduced in [1] and [5]) gives the profile of the tree (Z_k) as a subsequence of (y_k)

$$Z_{k+1} = y_{l(k)}$$

where $l(k) = \sum_{i=1}^{k} Z_i$ and the width W_n as

$$W_n = \max_k Z_k = \max_k y_{l(k)}.$$

We prove in the following proposition that $W_n = \max_k y_{l(k)}$ has the same behavior as $\max_k y_k$.

Proposition 1. *For each $p \ge 1$,*

$$\|W_n - \max_k y_k\|_p = O(n^{1/4} (\log n)^{3/4}).$$

This result is based on the slow variation of the sequence $y = (y_k)_{0 \le k \le n}$. Indeed, $\Omega_c(n)$ defined as the set of sequences $y = (y_k)_{0 \le k \le n}$ such that, for all k and m such that $k + m \le n$,

$$|y_{m+k} - y_m| \le c\sqrt{k \log n}$$

satisfies the following lemma.

Lemma 1. *For all $\alpha > 0$, there exists $c > 0$ such that, for all n,*

$$1 - \Pr(\Omega_c(n)) = o(n^{-\alpha}).$$

This can be proved using (see Petrov [4]) that, if (Y_k) is a random walk with increments X_k satisfying $E(X_k) = 0$ and for some $\alpha > 0$, $E(\exp(\alpha|X_k|) < \infty$, then there exists $T, C_1, C_2 > 0$ such that

$$\Pr(|Y_k| \geq x) \leq \begin{cases} 2e^{-\frac{x^2}{4C_1}} & \text{if } 0 \leq x \leq C_1 T, \\ 2e^{-C_2 x} & \text{if } x \geq C_1 T. \end{cases}$$

Then it remains to prove that $E((\max_k y_k/\sqrt{n})^p) \to E(m^p)$ and to estimate the rate of convergence. This is the object of the next section.

3. Parking Functions and Empiric Processes

Consider the sequence $(U_i)_{1\leq i\leq n}$ of n i.i.d. random variables uniformly distributed on $[0,1]$. Let $F_n(t)$ be the empiric distribution for $(U_i)_{1\leq i\leq n}$ i.e.

$$F_n(t) = \frac{\operatorname{card}\{i \in \{1,\dots,n\}, U_i \leq t\}}{n}, \qquad (0 \leq t \leq 1).$$

Process $(F_n(t))$ converges to $(F(t)) = (t)$, the distribution function of the uniform distribution. Especially, the empiric process $(\alpha_n(t)) = (\sqrt{n}(F_n(t) - F(t)))_{0\leq t\leq 1}$ converges in distribution to the Brownian bridge $(b(t))_{0\leq t\leq 1}$.

There is a precise connection between parking functions and empiric processes. Indeed, consider the sequence $(U_i)_{1\leq i\leq n}$ of i.i.d. random variables uniformly distributed on $[0,1]$ and realize parking in the following way: If $U_i \in \left[\frac{k-1}{n+1}, \frac{k}{n+1}\right[$, then car c_i tries to park first on place $h_i = k$. The last empty place V is given in terms of the empiric process.

Proposition 2. *There is a unique $T(n)$ in $\{0,1,\dots,n\}$ such that*

$$\alpha_n(\frac{T(n)}{n+1}) = \min_{1\leq j\leq n} \alpha_n(\frac{j}{n+1}).$$

Moreover, $T(n) = V$.

It is easy to deduce that

$$\left|\frac{\max_k y_k}{\sqrt{n}} - (\sup_{0\leq t\leq 1} \alpha_n(t) - \inf_{0\leq t\leq 1} \alpha_n(t))\right| \leq \frac{1+2\epsilon_n}{\sqrt{n}}$$

where $\epsilon_n = \sqrt{n}\sup_{0\leq t\leq 1} |\alpha_n(\frac{\lfloor (n+1)t\rfloor}{n+1}) - \alpha_n(t)|$ satisfies the following proposition.

Proposition 3. *There exists A, C and K such that for all x and n,*

$$\Pr(\epsilon_n \geq C\log n + x) \leq An^{1-KC}e^{-Kx}. \tag{2}$$

Then $\alpha_n(t)$ is replaced by a Brownian bridge $b_n(t)$ using the following result of Komlos, Major and Tusnady [2].

Theorem 2. *There exists a sequence of Brownian bridges $(b_n)_{n\geq 1}$ and A, M, $\mu > 0$ such that for all n and x*

$$\alpha_n(t) = b_n(t) + \frac{c_n(t)}{\sqrt{n}}$$

where $C_n = \sup_{0\leq t\leq 1} |c_n(t)|$ verifies for all x

$$\Pr(C_n \geq A\log n + x) \leq Me^{-\mu x}. \tag{3}$$

Then

$$\left|\frac{\max_k y_k}{\sqrt{n}} - (\sup_{0\le t\le 1} b_n(t) - \inf_{0\le t\le 1} b_n(t))\right| \le \frac{1+2(\epsilon_n + C_n)}{\sqrt{n}}$$

where C_n is introduced in Theorem 2. Using the fact that, if T is the almost surely unique point such that $b(T) = \min_{0\le t\le 1} b(t)$, then $e = (e(t))_{0\le t\le 1}$, defined by $e(t) = b((T+t) \bmod 1) - b(T)$, is a normalized Brownian excursion independent of T, one has

$$\left|\frac{\max_k y_k}{\sqrt{n}} - \sup_{0\le t\le 1} e_n(t)\right| \le \frac{1+2(\epsilon_n + C_n)}{\sqrt{n}}. \tag{4}$$

Relations (2) and (3) give that $\|\epsilon_n + C_n\|_p$ is bounded by $K_p \log n$ and thus (4) gives the following result.

Theorem 3. *For each $p \ge 1$,*

$$\left\|m_n - \frac{\max_k y_k}{\sqrt{n}}\right\|_p = O(\frac{\log n}{\sqrt{n}}).$$

It is then easy to deduce Theorem 1.

Bibliography

[1] Aldous (David). – Brownian excursions, critical random graphs and the multiplicative coalescent. *The Annals of Probability*, vol. 25, n° 2, 1997, pp. 812–854.

[2] Komlós (J.), Major (P.), and Tusnády (G.). – An approximation of partial sums of independent RV's, and the sample DF. II. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 34, n° 1, 1976, pp. 33–58.

[3] Odlyzko (Andrew M.) and Wilf (Herbert S.). – Bandwidths and profiles of trees. *Journal of Combinatorial Theory. Series B*, vol. 42, n° 3, 1987, pp. 348–370.

[4] Petrov (V. V.). – *Sums of independent random variables.* – Springer-Verlag, New York-Heidelberg, 1975, x+346p. Translated from the Russian by A. A. Brown, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 82.

[5] Spencer (Joel). – Enumerating graphs and Brownian motion. *Communications on Pure and Applied Mathematics*, vol. 50, n° 3, 1997, pp. 291–294.

[6] Takács (Lajos). – Limit distributions for queues and random rooted trees. *Journal of Applied Mathematics and Stochastic Analysis*, vol. 6, n° 3, 1993, pp. 189–216.

Random Walks and Graph Geometry: a Survey

Thierry Coulhon
Université de Cergy-Pontoise

April 12, 1999

[summary by Philippe Robert]

Abstract

If Γ is an infinite graph with bounded degree, this talk analyzes the relations between the asymptotic behavior of a nearest neighbor Markov chain on the graph and some simple geometric characteristics of the graph.

1. Notations

We denote $x \sim y$ if x, $y \in \Gamma$ are neighbors. For $k \in \mathbb{N}$ the quantity $p^k(x,x) = \Pr_x(M_k = x)$ is the probability that the random walk (M_n) starting from $x \in \Gamma$ returns to x at the k-th step. In the case of the simple random walk $p(x,y) = p^1(x,y)$ is $1/\deg(x)$ if $y \sim x$ and and 0 otherwise. Let m be a positive function on Γ such that the relation $m(x)p(x,y) = m(y)p(y,x)$ holds for $x, y \in \Gamma$. In the case of a finite graph, this is a reversibility assumption: m is the equilibrium measure and the random walk run backward is similar to the original random walk. From an analytic point of view this condition gives an Hilbertian setting to some of the questions considered here. The L^p spaces considered here are with the measure m. The quantity $m(x)p(x,y)$ is denoted by μ_{xy}, the matrix (μ_{xy}) is thus symmetrical. In the finite case, μ_{xy} is the throughput between x and y at equilibrium.

The distance d on the graph between two nodes is the minimum number of edges between them, $B(x,r)$ is the ball of center $x \in \Gamma$ and radius $r > 0$ and $V(x,r)$ is the volume of this ball $V(x,r) = \sum_{y \in B(x,r)} m(y)$. The boundary of a subset A of Γ is given by $\partial A = \{x \in A; \exists y \notin A, x \sim y\}$.

Definition 1. The graph Γ associated to μ has the doubling property if there exists $C > 0$ such that for all $x \in \Gamma$ and $r > 0$,

$$\text{(D)} \qquad V(x,2r) \leq CV(x,r).$$

If $c_0(A)$ is the set of functions on Γ with a finite support in the subset A, for f in $c_0(\Gamma)$ the length of the gradient is defined by

$$|\nabla f|(x) = \left(\frac{1}{2}\int_{y\sim x} |f(x) - f(y)|^2 p(x,y)\right)^{1/2},$$

for $x \in \Gamma$. It is easy to verify that the identity $\|\nabla f\|_2^2 = \langle (I-P)f, f\rangle$ holds. The left-hand side is called the Dirichlet form associated to P, in a finite setting this functional is related to the convergence to equilibrium of the Markov chain.

The basic problem considered in this talk is of finding a relation between the asymptotics of $(p^k(x,x))$ as k tends to infinity and the behavior of $(V(x,r))$ as r gets large.

2. Graphs with a Polynomial Growth

The first result on this subject is the following proposition, due to Varopoulos.

Proposition 1. *For $D > 2$, the inequality*

$$p^k(x,x) \le Cm(x)k^{-D/2}, \tag{1}$$

for all $x \in \Gamma$ and $k \ge 1$ is equivalent to the Sobolev inequality for all $f \in c_0(\Gamma)$: $\|f\|_{\frac{2D}{D-2}} \le C\|\nabla f\|_2$.

The relation with the geometry of the graph is as follows. The Sobolev inequality implies that $V(x,r) \le cr^D$ for some constant $c > 0$. On the other hand the *isoperimetric inequality*

$$|A|^{\frac{D-1}{D}} \le C \sum_{x\in A, y\notin A, x\sim A} \mu_{xy},$$

for all finite subsets A, implies relation (1). With only a condition on the volume growth, we have the following theorem.

Theorem 1. *If $cr^D \le V(x,r) \le Cr^D$, for any $x \in \Gamma$ and $r > 0$, there exists c', C' such that*

$$c'k^{-D/2} \le \sup_{x\in\Gamma} p^{2k}(x,x) \le C'k^{-\frac{D}{D+1}},$$

and the bounds are optimal.

3. Upper Bounds: Regular Volume Growth

In this section graphs without prescribed volume assumption are considered.

Definition 2.

$$p^k(x,y) \le C\frac{m(y)}{V(x,\sqrt{K})}\exp\left(-c\frac{d^2(x,y)}{k}\right) \quad \forall x,y\in\Gamma, k\ge 1. \tag{UE}$$

The inequality (DUE) is the above inequality but with $x = y$.

$$p^{2k}(x,y) \ge c\frac{m(y)}{V(x,\sqrt{K})} \quad \forall x\in\Gamma, k\ge 1. \tag{DLE}$$

The graph Γ is said to satisfy a Faber-Krahn inequality if there exists a, $\nu > 0$ such that

$$\inf\left\{\||\nabla f|\|_2^2; f\in c_0(A), \|f\|_2 = 1\right\} \ge \frac{a}{r^2}\left(\frac{V(x,r)}{|A|}\right)^\nu, \tag{FK}$$

for all finite subsets A, $x \in \Gamma$ and $r \ge 1/2$.

With these definitions one has the following equivalences between the asymptotic behavior of $(p^k(x,x))$ and the geometry of Γ.

Theorem 2. *The following properties are equivalent* (i) *the Faber-Krahn inequality (FK);* (ii) *the inequalities (UE) and (D);* (iii) *the inequalities (DUE) and (D). Each of them implies (DLE).*

Bibliography

[1] Coulhon (Thierry). – Heat kernels on non-compact Riemannian manifolds: a partial survey. In *Séminaire de Théorie Spectrale et Géométrie, No. 15, Année 1996–1997*, pp. 167–187. – Université Grenoble I, 1997.

[2] Grigor'yan (Alexander). – Analytic and geometric background of recurrence and non-explosion of the Brownian motion on Riemannian manifolds. *Bulletin of the American Mathematical Society*, vol. 36, n° 2, 1999, pp. 135–249.

[3] Rosenberg (Steven). – *The Laplacian on a Riemannian manifold.* – Cambridge University Press, Cambridge, 1997, x+172p. An introduction to analysis on manifolds.

Asymptotic Bounds for the Fluid Queue Fed by Subexponential on/off Sources

Vincent Dumas
INRIA-Rocquencourt

February 4, 1999

[summary by Jean-Marc Lasgouttes]

This talk presents results from Dumas and Simonian [3] on the tail behaviour of the buffer content of a fluid queue processing the input of several exponential and subexponential sources. While the results in [3] are rather general, the presentation given here uses a simplified setting, for the sake of understandability.

1. Framework

Consider a fluid queue with infinite buffering capacity and outflow rate c. This queue is fed by $N > 1$ independent stationary on/off sources, where source i, $1 \leq i \leq N$ is characterized by:

- silence periods, where it generates no traffic, of length S_{in}, $n \geq 1$, i.i.d. and exponentially distributed;
- activity periods, where it generates traffic at peak rate h_i, of length A_{in}, $n \geq 1$; these variables are i.i.d., but no assumption is made on their distribution for now.

The following notation will be useful later:

$$p_i := \frac{\mathbb{E}[A_{in}]}{\mathbb{E}[A_{in} + S_{in}]}, \quad \rho_i := h_i p_i.$$

To characterize the stationary regime of source i, it is convenient to introduce the time elapsed in the current activity period A_i^*, whose distribution is given by

$$\Pr[A_i^* = 0] = 1 - p_i,$$
$$\Pr[A_i^* > x | A_i^* > 0] = \int_x^\infty \frac{\Pr[A_{in} > y]}{\mathbb{E}[A_{in}]} dy.$$

In what follows, we restrict ourselves to the case where $h_i \equiv h$, $p_i \equiv p$ and $\rho_i \equiv \rho$, for all $1 \leq i \leq N$. If V_t is the volume of fluid in the buffer at time t (with $V_0 = 0$), then the following result is well known:

Theorem 1. *Let $\Omega_i[t]$ be the flow emitted by source i in stationary regime in the interval $]-t, 0]$ and define $\Omega[t] := \sum_{i=1}^N \Omega_i[t]$. Then, assuming $N\rho < C$,*

$$\lim_{t\to\infty} V_t \stackrel{\mathcal{L}}{=} V := \sup_{t\geq 0}(\Omega[t] - ct).$$

It is important to have good estimates for $\Pr[V > x]$, since this can be used to determine loss rate in a finite buffer queue. A typical result in this respect is due to Anick, Mitra and Sondhi [1]: if there exist constants α_i such that $\Pr[A_{in} > x] = O(e^{-\alpha_i x}), 1 \leq i \leq N$, then there exists α such that $\Pr[V > x] = O(e^{-\alpha x})$.

However, recent studies have shown that some sources may have subexponential activity patterns, such as $\Pr[A_{in} > x] = O(x^{-s_i})$, $s_i > 1$. The purpose of this work is therefore to find good estimates for the tail distribution of V when the sources are a mix of exponential and subexponential sources, extending the results of [2, 4, 5].

2. Lower and Upper Bounds

Let I be a subset of $\{1, \dots, N\}$, with cardinal $|I|$, and define

$$A_I^* := \min_{i \in I} A_i^*, \qquad \Omega_{\bar{I}}[t] := \sum_{i \notin I} \Omega_i[t],$$
$$n_0 := \inf\{n \geq 0 | nh + (N - n)\rho > c\}.$$

Then the following bound holds as $x \to \infty$:

$$\Pr[V > x] \geq \max_I \Pr\left[(|I|h + (N - |I|)\rho - c)A_I^* > x\right]$$
$$\geq \max_{|I| = n_0} \prod_{i \in I} \Pr\left[(n_0 h + (N - n_0)\rho - c)A_i^* > x\right].$$

Similarly, defining V_i as

$$V_i := \sup_{t \geq 0} \left(\Omega_i[t] - \rho(1 + \epsilon)t\right),$$

where $\epsilon > 0$ is such that $(n_0 - 1)h + (N - n_0 + 1)\rho(1 + \epsilon) = c$, one has

$$\Pr[V > x] \leq \sum_{|I| = n_0} \prod_{i \in I} \Pr\left[V_i > \frac{x}{N - n_0 + 1}\right].$$

3. Application to a Mix of Exponential and Subexponential Sources

Assume that the queues can be partitioned in two classes for some $N_0 < N$:

$$\Pr[A_{in} > x] = O(x^{-s}), \qquad 1 \leq i \leq N_0,$$
$$\Pr[A_{in} > x] = O(e^{-\alpha_i x}), \qquad N_0 < i \leq N.$$

Then the main result of this study is as follows.

Theorem 2. *The following approximations hold:*
- *if* $N_0 < n_0$, *then* $\Pr[V > x] = O(e^{-\alpha x})$;
- *if* $N_0 \geq n_0$, *then* $\Pr[V > x] = O(x^{-n_0(s-1)})$.

Bibliography

[1] Anick (D.), Mitra (D.), and Sondhi (M. M.). – Stochastic theory of a data-handling system with multiple sources. *The Bell System Technical Journal*, vol. 61, n° 8, 1982, pp. 1871–1894.

[2] Boxma (O. J.). – Regular variation in multi-source fluid queue. In Ramaswami (V.) and Wirth (P. E.) (editors), *Teletraffic Contributions for the Information Age*. pp. 391–402. – North-Holland, Washington DC, 1997. Proceedings ITC-15.

[3] Dumas (V.) and Simonian (A.). – *Asymptotic bounds for the fluid queue fed by sub-exponential On/Off sources.* – Technical Report n° 98028, MAB, Université de Bordeaux 1, 1998.

[4] Jelenovicz (P. R.) and Lazar (A. A.). – Asymptotic results for multiplexing on/off sources subexponential on periods. *Advances in Applied Probability*, vol. 31, n° 2, 1999.

[5] Rolski (Tomasz), Schlegel (Sabine), and Schmidt (Volker). – Asymptotics of Palm-stationary buffer content distributions in fluid flow queues. *Adv. in Appl. Probab.*, vol. 31, n° 1, 1999, pp. 235–253.

Optimal Carrier Sharing in Wireless TDMA

Ed Coffman
New Jersey Institute of Technology

February 4, 1999

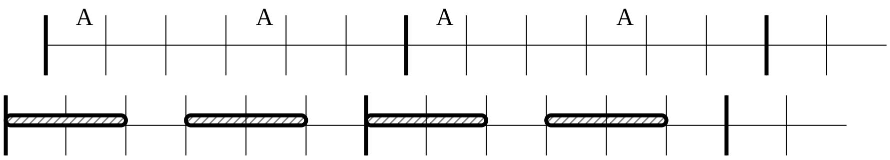
[summary by Philippe Robert]

Abstract

An important design issue in implementing Dynamic Channel Assignment in Time Division Multiple Access (TDMA) wireless networks is whether resource allocation should be done on a per-carrier basis or at the time slot level. Resource allocation at the time slot level is seriously hampered by the lack of synchronization between base stations in distinct cells. We present simple *greedy packing* algorithms which overcome this obstacle by clustering calls. The results suggest that the algorithms are nearly optimal, and that little extra performance can be gained either by allowing the rejection of calls or by repacking.

TDMA (Time Division Multiple Access) systems supply most digital cellular services (GSM for example). The available spectrum is divided into carriers (frequency bands) and each of these is time slotted. A carrier is slotted and up to n calls can be time-multiplexed at one time (for example there are 8 time-slots per carrier for GSM). When n calls are active, call requests are rejected since no queueing is possible.

The calls in a cell A can share any given carrier. A carrier assigned to the cell A will not be assigned to another cell close enough to interfere with its calls. This talk presents algorithms ensuring that a neighboring cell B is allowed to time-share the carrier with cell A. The sharing mechanism must take into account that the slots in cells A and B are not perfectly synchronized. To avoid interference, the slots assigned to cell A are not allowed to overlap slots assigned to cell B.



Clearly, to maximize the acceptance rate of call s, time-slot allocation should try to cluster separately A-calls and B-calls. In the above figure the hatched rectangles indicate time slots which cannot be used by cell B. In this case clustering of A-calls would make 3 slots available instead of 2. The time-slots are represented by a circle with n slots.

Definition 1. An algorithm of slot allocation is *greedy* if a new call is accepted if there is an available slot.

A *repacking* algorithm can reallocate the time-slots (i.e., repack) in order to admit a new call.

Some Examples of Assignment Algorithms.

Clustering algorithms C_n. A call is packed in the first available slot found in a scan of the current state clockwise from slot $(1,2)$ if an A-call and counterclockwise from slot $(2n-2, 2n-1)$ if a B-call. This algorithm tries to separate as much as possible A and B-calls.

Weighting algorithms W_n. Each slot carries a weight. At arrival, the quantity δ_0 is added to the A-slot receiving the new call and δ_1 to neighboring slots, δ_2 to the slots at distance $2, \dots$. The quantity δ_1' is added to the B-slots covered by the slot of the new call, δ_2' to the B-slots at distance 2, etc. An analogous procedure applies to the B-call arrivals. Weight changes are reversed at departure times.

Repacking algorithm R_n. Pack A and B calls in separate clusters whenever necessary.

A stochastic model is considered, the calls in cells A and B arrive according to a Poisson process with parameter λ_A and λ_B respectively. Holding times are independent with rate μ in each cell. For $X = A$, B, $\rho_X = \lambda_X/\mu$ and p_X denotes the probability of rejecting an X-call. The overall probability to be minimized is then

$$\frac{p_A\rho_A + p_B\rho_B}{\rho_A + \rho_B}.$$

The classical method to find the optimal algorithm to minimize the blocking probability is to solve the associated Bellman equation. As usual this equation is very hard to solve explicitly except when the state space is quite small.

Some numerical values are presented and discussed in the case $n = 8$. The main mathematical result is the following theorem.

Theorem 1. *If all optimal algorithms are greedy and if holding times are i.i.d. exponentials, then the algorithm W_n is optimal for $1 \leq n \leq 6$.*

The proof relies on a coupling argument.

Bibliography

[1] Borst (S. C.), Coffman (E. G.), Gilbert (E. N.), Whiting (P. A.), and Winkler (P. M.). – Optimal carrier sharing in wireless TDMA, September 1999.

Explicit Sufficient Invariants for an Interacting Particle System

Yoshiaki Itoh
Institute of Statistical Mathematics, Japan

May 17, 1999

[summary by Philippe Robert]

Abstract

We introduce a new class of interacting particle systems on a graph G. Suppose there are initially $N_i(0)$ particles at each vertex i of G, and that the particles interact to form a Markov chain: at each instant two particles are chosen at random, and if these are at *adjacent* vertices of G, one particle jumps to the other particle's vertex, each with probability $1/2$. The process enters a death state after a finite time when all the particles are in some *independent* subset of the vertices of G, i.e., a set of vertices with no edge between any two of them. The problem is to find the distribution of the death state $\eta_i = N_i(\infty)$ as a function of the numbers $N_i(0)$.

We are able to obtain, for some special graphs, the *limiting* distribution of each N_i if the total number of particles $N \to \infty$ in such a way that the fraction $N_i(0)/N = \xi_i$ at each vertex is held fixed as $N \to \infty$. In particular we can obtain the limit law for the graph $S_2 : \cdot\!-\!\!-\!\cdot\!-\!\!-\!\cdot$ having 3 vertices and 2 edges.

This talk is based on a joint paper with Colin Mallows and Larry Shepp [1]

1. A Particle System

If G is a connected graph, the following particle system is considered. Initially n particles are distributed on the nodes of the graph, at each unit of time two particles are chosen at random if they are on neighboring nodes then one of the two particles jumps to the other one's vertex, each with probability $1/2$. This kind of model has various applications to genetics, to voting and symbolic computation.

It is easily seen that if a vertex has no particles it remains empty and the process lives on a subgraph with this vertex removed. The process continues until all vertices are empty except those of an *independent* subset J of G, i.e., the vertices in J have no edge in common. At that time the process stops since no interaction can occur anymore. We denote by $N(t) = (N_i(t); i \in G)$ the vector of the number of particles on the vertices at time t, τ is the first time the process reaches an independent set; $N(\tau)$ is the terminal state of the process.

Example (The complete graph). The singletons are obviously the independent sets for this graph and by symmetry the terminal distribution is easy to derive, $\Pr(N(\tau) = \delta_i) = N_i(0)/n$.

In general it is difficult to determine the distribution of the final state of the process. The method used here is to find functionals f such that the relation

$$\mathbb{E}(f(N(t))) = \mathbb{E}(f(N(0)))$$

holds for all $t \geq 0$ and for the random time $t = \tau$. If there are sufficiently many functions f then the distribution of $N(\tau)$ may be derived. In a classical dynamical system such a function is an *invariant* of the motion. In a probabilistic context the corresponding notion is the martingale, a function f is *admissible* if $(f(N(t))$ is a martingale, i.e., for all $s \leq t$,

$$\mathbb{E}(f(N(t))|\text{all events before time } s) = f(N(s)),$$

in particular $\mathbb{E}(f(N(t))) = \mathbb{E}(f(N(0)))$ for all $t \geq 0$.

In our case $\left(\sum_{i \in G} N_i(t)\right)$ is a trivial (constant!) martingale. Another example is the process $(N_i(t))$ for $i \in G$, it is also a martingale, hence $\mathbb{E}(N_i(\tau)) = N_i(0)$.

For an admissible f, under mild integrability conditions we shall have $\mathbb{E}(f(N(\tau))) = f(N(0))$, hence if there is a rich class of such f the distribution of $N(\tau)$ will be determined. It turns out that this discrete model does not seem to have sufficiently many admissible functions. The situation is somewhat simpler if one considers a continuous version $(X_i(t); i \in G)$ of the process, it is the solution of the stochastic differential equation

$$dX_i = \sum_{j \in \mathcal{N}_i} \sqrt{X_i X_j}\, dB_{ij}, \tag{1}$$

where $\mathcal{N}_i$ is the set of the neighbors of $i \in G$. The B_{ij}, $i, j \in G$ are Brownian motions such that $B_{ij} = -B_{ji}$, so that if

$$\sum_{i \in G} X_i(t) = 1$$

for $t = 0$ then this relation holds for all $t \geq 0$ (the "number" of particles is constant). Notice that if one of the coordinates is 0 it remains 0 as in the discrete model.

2. Martingales of the Continuous Process

A star graph S_r with $r+1$ vertices is considered, the vertex 0 is supposed to be the center.

Proposition 1. *If $G = S_r$ and $\alpha_1 + \cdots + \alpha_r = 0$, the process $(P_n^\alpha(X_1(t), \ldots, X_r(t)))$ is a martingale, where P_n^α is the polynomial defined by*

$$P_n^\alpha(x_1, \ldots, x_r) = \sum_{\substack{i_1 \geq 1, \ldots, i_r \geq 1 \\ i_1 + \cdots + i_r = n}} \binom{n}{i} \binom{n-r}{i-1} \prod_{k=1}^{r} (\alpha_k x_k)^{i_k},$$

with $i = (i_1, \ldots, i_r)$ and $\binom{n}{i} = n!/i_1! \cdots i_r!$.

The proof is carried out with the help of Itô's equation. In this manner there is a sequence of martingales associated to the stochastic process $(X(t))$.

A similar situation occurs with the Brownian motion (B_t), if h_n is the n-th Hermite polynomial, then

$$(M_n(t)) = \left(t^{n/2} h_n\left(B(t)/\sqrt{t}\right)\right)$$

is a martingale. The appropriate generating function of these processes gives the classical exponential martingale

$$\sum_{n=0}^{+\infty} \frac{c^n}{n!} M_n(t) = \exp\left(cB(t) - \frac{c^2}{2} t\right).$$

The martingales $(M_n(t))$ are not easy to use to get distributions of the Brownian motion functionals. The above exponential martingale is simple, "contains" all the martingales $(M_n(t))$ and many distributions related to the Brownian motion can be directly obtained with it (see Rogers and Williams [3]). In the following a similar method is used to get the terminal distribution of the process. As we shall see the corresponding exponential martingale is not as simple as for Brownian motion but it will give the desired distribution.

3. Star Network With Three Nodes

Since the expression of the polynomials P_n^α is rather complicated to derive results on the distribution of $(X(\tau))$, the simpler case $r = 2$ is now considered. In this case the terminal states $(X_0(\tau), X_1(\tau), X_2(\tau))$ are $(1,0,0)$ or $(0,x,1-x)$, $x \in [0,1]$. Taking $\alpha_1 = -1$ and $\alpha_2 = 2$ in the above proposition, we get that, for $n \geq 2$,

$$(Y_n(t)) = \left(\sum_{i=1}^{n-1} \binom{n}{i}\binom{n-2}{i-1}(-1)^i X_1(t)^i X_2(t)^{n-1}\right) \tag{2}$$

is a martingale. The key result of this section is the following identity, for $|v| < 1/4$ and $0 \leq x \leq 1$

$$\sum_{n\geq 2} \frac{v^n}{n} \sum_{i=1}^{n-1} \binom{n}{i}\binom{n-2}{i-1}(-1)^i x^i (1-x)^{n-1} = xv + \frac{1-v}{2}\left(1 - \sqrt{1 + \frac{4xv}{(1-v)^2}}\right), \tag{3}$$

this suggests to sum the expressions (2) as follows

$$Z_u(t) = \sum_{n\geq 2} \frac{u^n}{n} Y_n(t).$$

The process $(Z_u(t))$ is also a martingale, the exponential martingale of $(X(t))$, and the representation (3) gives the following result. If μ is the terminal distribution of $(X_1(t))$ with the initial state $X_i(0) = \xi_i$, $i = 1, \ldots, r$, then for $|u| < 1/4$,

$$\int_0^1 \sqrt{(1-u)^2 + 4ux}\,\mu(dx) = u(\xi_1 + \xi_2 - 1) + \sqrt{1 + 2u(\xi_1 - \xi_2) + u^2(\xi_1 + \xi_2)^2}.$$

The problem is thus reduced to a kind of moment problem (by differentiating with respect to u under the integral). Further analytic manipulations give the density f of μ as

$$\frac{d^2}{dx^2}\frac{2}{\pi}\int_0^x \frac{1}{\sqrt{x-w}} g(w)\,dw,$$

where g is a complicated function but with an explicit expression.

Bibliography

[1] Itoh (Yoshiaki). – Random collision models in oriented graphs. *Journal of Applied Probability*, vol. 16, n° 1, 1979, pp. 36–44.

[2] Itoh (Yoshiaki), Mallows (Colin), and Shepp (Larry). – Explicit sufficient invariants for an interacting particle system. *Journal of Applied Probability*, vol. 35, n° 3, 1998, pp. 633–641.

[3] Rogers (L. C. G.) and Williams (David). – *Diffusions, Markov processes, and martingales. Vol. 2: Itô calculus.* – John Wiley & Sons Inc., New York, 1987, xiv+475p.

Part 5

Number Theory

Continued Fractions from Euclid till Present

Ilan Vardi

IHES, Bures sur Yvette

October 19, 1998

[summary by Philippe Flajolet]

Continued fractions have fascinated mankind for centuries if not millennia. The timeless construction of a rectangle obeying the "divine proportion" (the term is in fact from the Renaissance) and the "self-similarity" properties that go along with it are nothing but geometric counterparts of the continued fraction expansion of the golden ratio,

$$\phi \equiv \frac{1+\sqrt{5}}{2} = \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cdots}}}.$$

Geometry was developed in India from the rules for the construction of altars. The *Sulva Sūtra* (a part of the *Kalpa Sūtra* hypothesized to have been written around 800 BC) provides a rule[1] for doubling an area that corresponds to the near-equality:

$$\sqrt{2} \doteq 1 + \frac{1}{3} + \frac{1}{3\times 4} - \frac{1}{3\times 4\times 34} \qquad \text{(correct to } 2\,10^{-6}\text{)}. \tag{1}$$

Exclusively for these seminar proceedings, we propose the original observation that the third and fourth partial sums in (1), namely $\frac{17}{12}$ and $\frac{577}{408}$, are respectively the fourth and eighth convergents to $\sqrt{2}$.

Accordingly, in the classical Greek world, there is evidence of knowledge of the continued fraction for $\sqrt{2}$ which appears in the works of Theon of Smyrna (discussed in Fowler's reconstruction [6] and in [17]) and possibly of Plato in *Theaetetus*, see [3]. As every student knows, Euclid's algorithm is a continued fraction expansion algorithm in disguise, and Archimedes' Cattle Problem (*circa* 250 BC) most probably presupposes on the part of its author some amount of understanding of quadratic irrationals, Pell's equation, and continued fractions; see [17] for a discussion.

The continued fraction convergent $\pi \approx \frac{355}{113}$ was known to Tsu Ch'ung Chi born in Fan-yang, China in 430 AD. More recently, the Swiss mathematician Lambert proved the 2,000 year conjecture (it already appears in Aristotle) that π is irrational, this thanks to the continued fraction expansion of the tangent function,

$$\tan z = \cfrac{z}{1-\cfrac{z^2}{3-\cfrac{z^2}{5-\cdots}}},$$

[1] "Increase the measure by its third part, and this third part by its own fourth, less the thirty-fourth part of that fourth". See vol. I of Dutt's book [4, p. 272] for context including otherwise rational approximations to $\sqrt{\pi/4}$.

and Apéry in 1979 gave in "a proof that Euler missed" [12] nonstandard expansions like

$$\zeta(3) \equiv \sum_{n=1}^{\infty} \frac{1}{n^3} = 1 + \cfrac{1}{2 \cdot 2 + \cfrac{1^3}{1 + \cfrac{1^3}{2 \cdot 6 + \cfrac{2^3}{1 + \cfrac{2^3}{2 \cdot 10 + \cfrac{3^3}{1 + \cdots}}}}}},$$

from which the irrationality of $\zeta(3)$ eventually derives.

Earlier, Euler had estimated that

$$\sum_{n=0}^{\infty} (-1)^n n! = 0.596\,347\,362\ \ldots$$

by means of a formal continued fraction expansion of the series $\sum_n n!(-z)^n$. A famous memoir of Stieltjes contains many other series identities like

$$\int_0^{\infty} \tanh u\, e^{-zu}\, du = \cfrac{1}{z^2 + \cfrac{1 \cdot 2}{1 + \cfrac{2 \cdot 3}{z^2 + \cfrac{3 \cdot 4}{1 + \cfrac{4 \cdot 5}{z^2 + \cdots}}}}},$$

which, a century later, enabled the author of this summary to provide the first analyses in a dynamic context of some basic data structures of computer science. The fascination continues and in 1985, Gosper found 17 million continued fraction digits of π, which corresponds to about 18 million decimal digits. Such quests are by the way not totally senseless: for instance, from similar data, we can know for sure that, should Euler's constant γ be rational, then its numerator and denominator would have at least 242,080 decimal digits (Papanikolaou, 1997)!

1. **Arithmetica**

This brilliant and erudite talk (see especially [14, 15]) discusses the many facets of standard (or "regular") continued fraction expansions of real numbers, which will be written occasionally as

$$x = [a_0, a_1, \ldots] \quad \text{if} \quad x = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cdots}}.$$

One refers to the a_j as continued fraction digits or partial quotients (thinking of Euclid's algorithm).

The best approximant properties of continued fractions are well-known [7]. Indeed, any convergent p/q (obtained by a finite truncation) of the continued fraction expansion of α approximates α better than any other fraction with a smaller denominator and better even than many with a larger denominator (compare π with $\frac{16}{5}$, $\frac{314}{100}$ against $\frac{22}{7}$).

A fruitful consequence of the best approximation property is the following: let D be a non-square and let p/q be a "good" approximant of $\sqrt{D}$. Then, $p^2 - q^2 D$ is small. In particular, as discovered by Lagrange, the continued fraction expansion of $\sqrt{D}$ hides a solution to Pell's equation,

$p^2 - Dq^2 = 1$. The solutions are essentially powers of a minimal solution that corresponds to a so-called fundamental unit of $\mathbb{Q}(\sqrt{D})$. Archimedes' Cattle Problem can be solved in this perspective, the full solution involving numbers with 206,545 digits! In an entertaining note [17], Vardi even shows that the solution can be enounced with only a few symbols: the total number of cattle is

$$\left\lceil \frac{25194541}{184119152}(109931986732829734979866232821433543901088049 + 50549485234315033074477819735540408986340\sqrt{4729494})^{4658} \right\rceil .$$

Continued fraction algorithms and the Euclidean algorithm are central to many other areas of number theory. For instance, Rademacher observed that the Jacobi symbol $\left(\frac{d}{c}\right)$ (that tells us in essence whether d is a square modulo c) is expressible as

$$\left(\frac{d}{c}\right) = (-1)^{(3-d-(d^{-1} \bmod c)+c\sum(-1)^i a_i)/4}, \tag{2}$$

where $d/c = [0, a_1, \ldots, a_r]$ with r even. In fact, the exponent in (2) is closely related to the Dedekind sum classically defined as

$$s(d,c) := \sum_{h=1}^{c-1} ((hd/c))((h/c)), \tag{3}$$

where the symbol $((x))$ signifies 0 if x is an integer and $x - \lfloor x \rfloor - \frac{1}{2}$ otherwise (see also the last section, especially formula (5)). Zagier discovered that the continued fraction expansion "by excess",

$$\frac{d}{c} = b_0 - \cfrac{1}{b_1 - \cfrac{1}{b_2 - \cfrac{1}{b_3 - \cdots}}}$$

gives rise to an identity related to (2) (and to (5) below),

$$s(d,c) = \frac{1}{12}\left(-6 + \frac{c + (c^{-1} \bmod d)}{d} - \sum_i (b_i - 3)\right). \tag{4}$$

In fine, properties of the type (2) and (4) result from simple matrix algebra, the point being that linear fractional transformations that arise from continued fractions are generated by $S(z) = z + 1$, and $T(z) = -1/z$, and are representable as 2×2 integer matrices of determinant 1, i.e., the group $SL(2, \mathbb{Z})$, while there is exactly one additive character on this group.

Amongst other interesting connections, we find Cornacchia's deterministic algorithm (1908) that makes it possible to write a prime as a sum of two squares directly from the Euclidean algorithm. (Legendre and Hermite had already introduced continued fractions for this problem.) Continued fraction algorithms are discussed in the celebrated HAKMEM ("Hackers' Memorandum") document [2], a text well worth reading.

2. **Statistica**

Examination of large slices of digits in continued fraction expansions of real constants (like $\pi, \gamma, \zeta(3)$ and many others, but unlike ϕ or e) reveals that the digits $1, 2, 3, \ldots$ tend to occur with a frequency that shows little deviation from the values 41%, 17%, 9%, ... , respectively. Such observations belong to the "metric" or "statistical" theory of continued fractions. They are essentially related to properties of the continued fraction transformation $T(x) = \{1/x\}$ (with $\{\cdot\}$ the fractional part function) under iteration.

Gauss first observed around 1800 that the probability density

$$\psi(x) = \frac{1}{\log 2} \frac{1}{1+x},$$

is invariant under the transformation T, as a simple computation based on partial fractions shows. The corresponding measure is called Gauss' measure. It was then natural to conjecture (and so did Gauss) that iteration of T on random data that obey a probability density, for instance a uniform $(0,1)$ density, produces distributions that converge to the invariant ψ.

Nowadays, we know two approaches to such problems: one, more qualitative, is based on ergodic theory, while the other, more precise, is based on functional analysis (following Kuzmin, Lévy, Wirsing) and transfer operators (following Ruelle, Babenko, Mayer, Hensley, Vallée). Indeed, the ergodic theorem grants us that properties of trajectories of real numbers under x are governed (almost surely) by Gauss' measure, while functional analysis identifies ψ with the dominant eigenfunction of the transfer operator $\mathcal{G}_1$, where

$$\mathcal{G}_s[f](x) = \sum_{m=1}^{\infty} \frac{1}{(m+x)^{2s}} f(\frac{1}{m+x}).$$

Properties of Gauss' measure give access to properties of continued fraction digits. For instance, the limit frequency of digit k in the continued fraction expansions of a random real number is (with probability 1) equal to

$$\varpi_k = \int_{1/k}^{1/(k+1)} \psi(x)\, dx = \log_2\left(1 + \frac{1}{k(k+2)}\right),$$

so that $\varpi_k = O(k^{-2})$ has a "soft" tail (and infinite expectation). From this type of argument, one can characterize expected properties of continued fractions of real numbers. One has, almost surely, for any function f that is not too wild,

$$\lim_{n\to+\infty} \frac{1}{n}\left(f(a_1(x)) + \cdots + f(a_n(x))\right) = K_f = \sum_{k=1}^{\infty} f(k) \log_2\left(1 + \frac{1}{k(k+2)}\right).$$

For instance, the geometric and harmonic means of partial quotients satisfy (almost surely)

$$\sqrt[n]{a_1 \cdots a_n} \to e^{K_{\log}}, \qquad e^{K_{\log}} = \prod_{k=1}^{\infty} \left(1 + \frac{1}{k(k+2)}\right)^{\log_2 k}$$

$$\frac{n}{\frac{1}{a_1} + \cdots + \frac{1}{a_n}} \to \frac{1}{K_{\text{inv}}}, \qquad K_{\text{inv}} = \sum_{k=1}^{\infty} \frac{1}{k} \log_2\left(1 + \frac{1}{k(k+2)}\right).$$

Such constants can be evaluated systematically by the "zeta-function trick" discussed in Vardi's book [13]. One finds the values

$$e^{K_{\log}} \doteq 2.68554, \qquad \frac{1}{K_{\text{inv}}} \doteq 1.74540,$$

where the first one is known as Khinchine's constant and the second one is the harmonic mean constant [1]. See Finch's beautiful site on Constants [5] for details and pointers to original sources. For instance, the harmonic mean of the 17 million continued fraction digits of π, as computed by Gosper, is 1.74594, a fact that that brings additional credibility to the conjecture that the continued fraction expansion of π is "normal" (that is, random-looking).

A similar type of question is: *How much information does a continued fraction digit convey?* This conduces to Lévy's constant that is related to the entropy of the continued fraction map. For x a number of the interval $(0, 1)$, let us write

$$\frac{P_n(x)}{Q_n(x)} = [0, a_1(x), \dots, a_n(x)].$$

Lévy proved that (almost surely)

$$\lim_{n\to\infty} \frac{1}{n} \log Q_n(x) \to \frac{\pi^2}{12 \log 2},$$

by making use of an approximation of the type

$$\log Q_n(x) \approx \sum_{k=1}^{n} \log T^k(x),$$

to which ergodic theory can be applied. Since the fundamental interval[2] of rank n that is determined by x has length about $1/Q_n(x)^2$, there results that very roughly,

$$Q_n(x)^{-2} \approx \left(e^{\pi^2/(6 \log 2)}\right)^n \doteq 10^{-1.03064n}.$$

In other words, n continued fraction digits discriminate a number as well as about $1.03064n$ decimal digits. (This is again consistent with Gosper's data on the number π.) Refinements on Lévy's estimates are due to Philipp (who first proved that the distribution of $\log Q_n(x)$ is asymptotically Gaussian) and many others. Lévy's constant also appears (for good reasons, see Vallée's works, e.g., [11]) in the mean number of iterations of Euclid's algorithm which, for rational numbers p/q with $1 \le p < q \le n$, is

$$\frac{12 \log 2}{\pi^2} \log n + O(1).$$

This last estimate is due to Heilbronn and Dixon around 1969. A companion Gaussian limit distribution further holds, which is a "hard" result due to Hensley, 1994.

Arithmetic means of partial quotients take us to a different circle of ideas and the probabilistic phenomena at stake become now quite irregular. Define the sum-of-digits function,

$$S_n(x) = \sum_{k=1}^{n} a_k(x).$$

The point is that the mean value of a continued fraction digit satisfies

$$\sum_{k=1}^{\infty} k \log\left(1 + \frac{1}{k(k+2)}\right) = +\infty.$$

Thus, the arithmetic means S_n/n do not behave at all like their geometric or harmonic counterparts: exceptionally large values of partial quotients a_n and of sums S_n are to be encountered not too infrequently.

---

[2]The fundamental interval of rank n determined by x is defined by all the numbers whose representation starts with $[0, a_1(x), \dots, a_n(x)]$.

This part of the discussion aims at understanding the finesses of large fluctuations in continued fraction digits. First, a Borel-Cantelli argument shows that, given any function $\phi(n)$, then (with λ the Lebesgue measure)

$$\lambda\{x \in (0,1) \ : \ a_n(x) > \phi(n) \text{ (infinitely often)}\} = 1 \quad \Longleftrightarrow \quad \sum \frac{1}{\phi(n)} = +\infty.$$

Thus, we should expect $a_n > n \log n \log\log n$ infinitely often, but $a_n < n \log n (\log\log n)^2$ only at a finite number of places. In fact, Khinchine proved that

$$\lambda\left\{x \ : \ \left|\frac{S_n(x)}{n \log_2 n} - 1\right| > \epsilon\right\} \underset{n\to\infty}{\longrightarrow} 0,$$

for any ϵ. In other words, the arithmetic mean of n digits is "typically" close to $\log_2 n$.

Heinrich [8] obtained a more precise limiting distribution result: for any $x \in \mathbb{R}$ and with μ the Gauss measure:

$$\left|\mu\left\{x \ : \ \frac{1}{n}\sum_{k=1}^{n} a_k(x) - \frac{\log n - \gamma}{\log 2} < t\right\} - G_{1,1}\left(t, \frac{\pi}{2\log 2}\right)\right| = O\left(\frac{(\log n)^2}{n}\right).$$

There γ denotes Euler's constant and $G_{1,1}(t,\lambda)$, is the stable distribution function whose characteristic function equals

$$\exp(-\lambda|u|(1 + 2i \log|u| \operatorname{sgn} u/\pi)).$$

Diamond and Vaaler further established, in a precise sense, that for almost all x's, there is at most one large partial quotient $a_n(x)$: one has

$$\left(S_n(x) - \max_{k\geq n} a_k(x)\right) \sim n \log_2 n,$$

with probability 1. Finally, the St. Petersburg game (play head-and-tails and double the stake till you win) is a well-known example of a sequence of i.i.d. random variables with infinite expectation and was considered as a paradox since no single 'fair' entry fee exists. In relation with the discussion of arithmetic means, Vardi's note [16] shows how the sequence of continued fraction digits of a random real number makes a reasonable choice of entry fees.

In the discrete world, these results indicate that the running time of the subtractive Euclidean algorithm (equal to the sum of the continued fraction digits) should be about $\log n \log\log n$, in the sense that if $S(p/q)$ is the running time, then $S(p/q)/(\log q \log\log q)$ should have a limiting distribution (consistent with Heinrich's result). This would imply that typically, the subtractive algorithm is more expensive than the standard algorithm by a factor of $\log\log n$. Knuth and Yao showed that, on average, the sum of all the partial quotients of all the regular continued fractions for m/n, with $1 \leq m \leq n$, is

$$\frac{6}{\pi^2} n(\log n)^2 + O(n \log n (\log\log n)^2),$$

where Lévy's constant pokes its nose again. (See Vallée's recent works [11] for the light shed by transfer operators on such phenomena.) This tells us that the *average* behavior of the subtractive algorithm is much different from its *typical* behaviour. Such results are not uncommon in number theory, e.g., in divisor problems; see [10].

3. Analytica

The last part of the talk is based on Vardi's paper [15]. The aim is to characterize the distribution of the *alternating sum-of-digits*

$$T_n(x) := \sum_{k=1}^{n} (-1)^k a_k(x),$$

for the continuous case, and of the discrete counterpart

$$T(d/c) = T_r(d/c), \quad \text{where} \quad d/c = [0, a_1, \ldots, a_r].$$

The mathematics go deeper and involve the hyperbolic Laplacian, Kloosterman sums, modular forms, and Eisenstein series. (See Sarnak's introductory lectures [9] for some related background.) The motivation comes largely from the need to understand the distribution of Dedekind sums defined in (3) that also satisfy a formula of Dean Hickerson (compare with Zagier's formula (4)), namely

$$s(d,c) = \frac{1}{12}\left(-3 + \frac{d + (d^{-1} \bmod c)}{c} - \sum_{i=1}^{r} (-1)^i a_i\right), \tag{5}$$

where the regular continued fraction expansion of $d/c = [0, a_1, \ldots, a_r]$ is normalized in such a way that r is even. This formula shows that Dedekind sums should really be thought of as alternating sums of regular continued fraction coefficients.

First, in the continuous case, the distribution of T_n is likely to resemble the difference between two random variables of the S_n type, themselves each distributed according to a $G_{1,1}$ stable law as discussed earlier (Heinrich's theorem). Now the difference of two $G_{1,1}$ is a Cauchy distribution, so that we are led to expect

$$\lim_{n\to\infty} \lambda\{x \ : \ T_n(x) < yn\} = \frac{1}{\pi}\int_{-\infty}^{y} \frac{\xi}{\xi^2 + x^2}\, dx, \tag{6}$$

with $\xi = \pi/(2\log 2)$.

In the discrete case, Vardi [15] has succeeded in proving that an analogue of (6) holds. In the language of Dedekind sums, the main result of [15] is then

$$\begin{aligned} \lim_{n\to\infty} \frac{\#\{0 < d < c < n, (d,c) = 1, s(d,c) < x\log c\}}{\#\{0 < d < c < n, (d,c) = 1\}} &= \frac{1}{\pi}\int_{-\infty}^{x} \frac{(2\pi)^{-1}}{(2\pi)^{-2} + s^2}\, ds \\ &= \frac{1}{\pi}\arctan(2\pi x) + \frac{1}{2}. \end{aligned} \tag{7}$$

(By Hickerson's formula (5), this gives the very same limiting distribution result for the alternating sum of continued fraction coefficients.) The proof uses the full machinery of modular forms and harmonic analysis on $SL(2,\mathbb{Z})$, see [9]. It would be of interest to find a simpler proof, as this would very likely have the advantage of providing the limiting distribution for the sum of continued fraction coefficients. The fact that there is a unique additive character for $SL(2,\mathbb{Z})$ makes it unlikely that this could be obtained using harmonic analysis.

Bibliography

[1] Bailey (David H.), Borwein (Jonathan M.), and Crandall (Richard E.). – On the Khintchine constant. *Mathematics of Computation*, vol. 66, n° 217, 1997, pp. 417–431.

[2] Beeler (M.), Gosper (R. W.), and Schroeppel (R.). – *HAKMEM*. – Memorandum n° 239, M.I.T., Artificial Intelligence Laboratory, February 1972. Available on the WorldWide Web at `http://www.inwap.com/pdp10/hbaker/hakmem/hakmem.html`.

[3] Caveing (J.). – *L'irrationalité, dans les mathématiques grecques jusqu'à Euclide.* – Presses Universitaires du Septentrion, Paris, 1998.

[4] Dutt (Romesh Cunder). – *A History of Civilisation of Ancient India Based on the Sanskrit Literature.* – Vishal Publishers, Delhi, 1972. A reprint of the original edition, 1888.

[5] Finch (Steven). – Favorite mathematical constants. – Available on the World Wide Web at the URL `http://www.mathsoft.com/asolve/constant/constant.html`, 1995.

[6] Fowler (D. H.). – *The Mathematics of Plato's Academy: A New Reconstruction.* – Clarendon Press, Oxford, 1987.

[7] Hardy (G. H.) and Wright (E. M.). – *An Introduction to the Theory of Numbers.* – Oxford University Press, 1979, fifth edition.

[8] Heinrich (Lothar). – Rates of convergence in stable limit theorems for sums of exponentially ψ-mixing random variables with an application to metric theory of continued fractions. *Mathematische Nachrichten*, vol. 131, 1987, pp. 149–165.

[9] Sarnak (Peter). – *Some Applications of Modular Forms.* – Cambridge University Press, 1990, *Cambridge Tracts in Mathematics*, vol. 99.

[10] Tenenbaum (Gérald). – *Introduction to analytic and probabilistic number theory.* – Cambridge University Press, Cambridge, 1995, xvi+448p. Translated from the second French edition (1995) by C. B. Thomas.

[11] Vallée (Brigitte). – A unifying framework for the analysis of a class of Euclidean algorithms. – Preprint, 2000. To appear in *Proceedings of LATIN'2000*, *Lecture Notes in Computer Science*, in press.

[12] Van der Poorten (Alfred). – A proof that Euler missed ... Apéry's proof of the irrationality of $\zeta(3)$. *Mathematical Intelligencer*, vol. 1, 1979, pp. 195–203.

[13] Vardi (Ilan). – *Computational Recreations in Mathematica.* – Addison Wesley, 1991.

[14] Vardi (Ilan). – The distribution of Dedekind sums. – Preprint, October 1992. 20 pages.

[15] Vardi (Ilan). – Dedekind sums have a limiting distribution. *International Mathematics Research Notices*, n° 1, 1993, pp. 1–12.

[16] Vardi (Ilan). – The St. Petersburg game and continued fractions. *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique*, vol. 324, n° 8, 1997, pp. 913–918.

[17] Vardi (Ilan). – Archimedes' cattle problem. *The American Mathematical Monthly*, vol. 105, n° 4, 1998, pp. 305–319.

An Introduction to Analytic Number Theory

Ilan Vardi
IHES, Bures-sur-Yvette

December 14, 1998

[summary by Cyril Banderier and Ilan Vardi]

1. Introduction

> "Le plus court chemin entre deux vérités dans le domaine réel passe par le domaine complexe.[1] "
>
> J. Hadamard.

The above quote captures the depth analysis can bring when one is confronted by number theoretic questions. The oldest and most fundamental of such questions is the study of prime numbers. The first question to be answered is: Are there an infinite number of primes? This can be answered by a number of simple proofs (several other proofs are given in [7]):

- Euclid: Assume there are a finite number of primes $p_1, \ldots, p_n$, then $p_1 p_2 \cdots p_n + 1$ is not divisible by any of the p_i's, so any of its prime divisors yields a new prime number (Euclid only considered the case $n = 3$).
- Pólya: The Fermat numbers $F_n = 2^{2^n} + 1$ are pairwise relatively prime, so the set of their prime divisors must be infinite.
- Erdős: Fix x and consider the primes $p_1, \ldots, p_n \leq x$. Since every integer is the product of a perfect square and a squarefree number, one can write every integer $m \leq x$ as $m = p_1^{e_1} \cdots p_n^{e_n} Q^2$, where $e_i \in \{0, 1\}$ and $Q^2 \leq x$. There are 2^n choices for the e_i and $\sqrt{x}$ choices for Q, so it follows that $n \geq \frac{\ln(x)}{2\ln(2)}$.
- Euler: One has the formal identity

$$\sum_n \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \tag{1}$$

which in fact holds for $\Re(s) > 1$. As $s \to 1$, the left hand side of (1) tends to ∞ since the harmonic series diverges, so there must be an infinite number of factors on the right.

This proof can be modified by noting that $\zeta(2) = \pi^2/6$, where $\zeta(s) = \sum 1/n^s$. If there were only a finite number of primes, then (1) would imply that π^2 is rational, proved false by Legendre in 1797, see also [6].

A stronger version of this is due to Mertens: The finite version of (1) gives

$$\prod_p \frac{1}{1 - p^{-1}} > \sum_{n<x} \frac{1}{n} \sim \ln(x),$$

[1] "The shortest path between two truths in the real domain passes through the complex domain."

and taking logs will give

$$\sum_{p<x} \frac{1}{p} \sim \ln\ln(x), \tag{2}$$

and so there are an infinite number of primes.

Which of these is the "best" proof? One argument would say that it is the one which allows the best generalisation. For example, Euclid's proof easily shows that there are an infinite number of primes of the form $4k+3$ (consider $4p_1 \cdots p_n - 3$), but seems to fall flat when trying to prove that the same holds for primes of the form $4k+1$ (one has to consider $4(p_1 \cdots p_n)^2 + 1$). In general, one wants to demonstrate Dirichlet's assertion (that he proved in 1837, in [3]) "there are an infinite number of primes of the form $ak+b$, where a and b are relatively prime." It turns out that the proof of this deep fact uses a generalisation of Euler's method, i.e., equation (2):

$$\sum_{p \equiv a \bmod q} \frac{1}{p} = \infty \Leftrightarrow \text{there are an infinite number of primes in } ak+q.$$

2. Dirichlet's Theorem

Let χ be a multiplicative character, with period q, that it is to say a complex valued function $\chi(n)$ satisfying $\chi(mn) = \chi(m)\chi(n)$, $\chi(1) = 1$ and $\chi(0) = 0$ (this implies that if $\chi(n) \neq 0$, then it is a root of unity and so has norm one). An example is the Legendre (or Jacobi if q is not a prime) symbol

$$\chi(n) := \left(\frac{n}{q}\right) = \begin{cases} 0 & \text{if } q|n, \\ 1 & \text{if } x^2 \equiv n \bmod q \text{ for some } x, \\ -1 & \text{otherwise.} \end{cases}$$

In fact, for any q power of an odd prime number, there are exactly $\phi(q)$ multiplicative characters with period q, all given by $\chi(n) := e^{2ik\pi\nu(n)/\phi(q)}$ for $0 \le k \le \phi(q) - 1$ and where $\nu(n)$ is such that $n \equiv g^{\nu(n)} \bmod q$ for any generator of the group of invertible elements of $\mathbb{Z}/q\mathbb{Z}$. When q is a power of 2, the definition is little more cumbersome (linked to the "factorisation" $n \equiv (-1)^{\nu_1(n)} 5^{\nu_2(n)} \bmod q$), and for general q, it is the product of characters of the factors of q. The importance of characters is seen by the following *orthogonality relation*:

$$\frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \chi(n) = \begin{cases} 1 & \text{whenever } n \equiv a \bmod q, \\ 0 & \text{otherwise,} \end{cases} \tag{3}$$

where the sum is over all the characters (the two real ones and the other complex characters). The *orthogonality relation* allows one to pick out an arithmetic progression. For his proof, Dirichlet introduced what are nowadays called Dirichlet L-functions, defined by

$$L(s,\chi) := \sum_{n \ge 1} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}.$$

Taking logarithm leads to $\ln L(s,\chi) = \sum_p - \ln(1 - \chi(p)p^{-s})$, thus one has

$$\begin{aligned} \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \ln L(s,\chi) &= \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \sum_p - \ln(1 - \chi(p)p^{-s}) \\ &= \sum_p \sum_{k \ge 1} \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \frac{\chi(p^k) p^{-sk}}{k} \end{aligned}$$

and a simple application of relation (3) gives

$$(4)\qquad \frac{1}{\phi(q)}\sum_{\chi}\overline{\chi(a)}\ln L(s,\chi)=\sum_{p}\sum_{\substack{k\geq 1\\ p^k\equiv a \bmod q}}\frac{p^{-sk}}{k}=\sum_{p\equiv a \bmod q}p^{-s}+O(1),\quad s\to 1^+.$$

Then, by splitting the sum in real and complex characters, one gets

$$(5)\qquad \sum_{p\equiv a \bmod q}p^{-1}=\frac{1}{\phi(q)}\left(\sum_{\chi=\chi_0}+\sum_{\chi=\left(\frac{n}{q}\right)}+\sum_{\chi\text{ complex}}\right)\overline{\chi(a)}\ln L(1,\chi)+O(1).$$

χ_0 is called the principal character and equals 1 whenever $n\not\equiv 0 \bmod q$ and 0 otherwise. The first sum (over χ_0) is $+\infty$, as $L(s,\chi_0)=\zeta(s)\prod_{p|q}(1-p^{-s})$. This infinite term should imply that there are an infinite number of primes in the arithmetic progression. The only problem is that one of the other terms could cancel this one by being $-\infty$ at $s=1$. The Abel summation criterion shows that $L(1,\chi)$ is finite. One therefore has to show that $L(1,\chi)\neq 0$.

This is definitely true for complex characters since otherwise, by setting $a=1$ and taking the exponential in (4), one has $\prod_\chi |L(1,\chi)|>1$ which is incompatible with a zero of order at least 2 (coming from $L(1,\chi)=0$ and $L(1,\overline{\chi})=0$) versus a single pole in $s=1$. Hence the last sum in relation (5) is bounded.

The real problem is then to bound the middle sum in relation (5), that is to say to show that $L(1,(\cdot/q))\neq 0$. Dirichlet proved this result by a very ingenious method: He evaluated this number in closed form! This is now known as Dirichlet's class number formula:

$$0\neq L\left(1,(\cdot/q)\right)=\begin{cases}\frac{\pi h}{w\sqrt{q}} & \text{when } q\equiv 1 \bmod 4\\ \frac{2h\ln\epsilon}{\sqrt{q}} & \text{when } q\equiv 3 \bmod 4\end{cases}$$

where h is the class number of $\mathbb{Q}(\sqrt{(-1)^{(q+1)/2}q})$ and ϵ its fundamental unit and w the number of roots of unity in this field (see the canonical reference [2]). Since each of these quantities counts something, they are positive, the result now follows:

$$\sum_{p\equiv a \bmod q}p^{-1}=+\infty.$$

Simpler proofs using only complex analysis are also possible. The idea is to use Landau's theorem that a Dirichlet series with positive terms has a pole at its abscissa of convergence and apply it to $\prod_\chi L(s,\chi)$ which has just been shown to have positive coefficients.

3. **Prime Number Theorem**

The distribution of primes is quite irregular, so it is easier to study their statistical behaviour. In this direction, let $\pi(x)$ be the number of primes $\leq x$. Gauss conjectured that $\pi(x)\sim\int_2^x\frac{dt}{\ln t}=:\mathrm{Li}(x)$. This assertion simply says: "the probability that n is prime is about $1/\ln n$." This result was finally proved by Hadamard and La Vallée Poussin in 1896. Both of them used fundamental ideas of Riemann who was the first to introduce complex analysis in the study of the distribution of prime numbers.

Using Perron's formula, namely

$$\sum_{p^n\leq x}\ln(p)=\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{-\zeta'(s)}{\zeta(s)}\frac{x^s ds}{s}$$

and using residues, Riemann essentially found what is perhaps the most important formula in analytic number theory (the von Mangoldt explicit formula):

$$(6)\qquad \sum_{p^n\le x}\ln(p)=x-\frac{\zeta'(0)}{\zeta(0)}-\sum_{\zeta(\rho)=0}\frac{x^\rho}{\rho}=x-\ln(2\pi)-\sum_{\Re(\rho)>0}\frac{x^\rho}{\rho}-\frac{1}{2}\ln(1-x^{-2}),$$

where sum on the right is over the zeroes of the Riemann ζ function. These zeroes can be split up into two types: The *trivial* zeroes at $-2,-4,-6,\dots$, and the zeroes with $0\le\Re\le 1$ (the right hand side of (6) reflects this dichotomy). This formula has many interesting properties and reflects the following principles of analytic number theory:

1. Primes should always be counted with weight $\ln(p)$;
2. Primes and prime powers should be counted together;
3. There are much less prime powers than primes;
4. The zeroes of the ζ function are the "fundamental frequencies" of the primes, and in this sense are dual to the primes.

Following Chebyshev, one defines $\theta(x)=\sum_{p\le x}\ln(p)$ and $\psi(x)=\sum_{p^n\le x}\ln(p)=\sum_{n\le x}\Lambda(n)$, where $\Lambda(n)=\ln(p)$ when $n=p^m$, and zero otherwise. A fairly straightforward partial summation shows that the prime number theorem is equivalent to $\psi(x)\sim x$ (note that trivially, $\psi(x)=\theta(x)+O(\sqrt{x})$), and that more generally,

$$\psi(x)=x+R(x)\Longleftrightarrow\pi(x)\sim\mathrm{Li}(x)+O(R(x)/\ln(x)).$$

One can then see from the explicit formula (6) that the prime number theorem would follow if one can bound $\Re\rho<1$, since each error term would then be of order $<x$. The prime number theorem would then be equivalent to showing that $\zeta(1+it)\ne 0$ for $t\ne 0$. In fact, this is an equivalence (as was later shown by Wiener) and Hadamard and La Vallée Poussin were able to prove that $\zeta(1+it)\ne 0$ using some ingenious trigonometric identities. We will give a proof due to Mertens, in 1898. Set $\rho=1+it$, then $\zeta(\rho)=0\Longrightarrow\Re\ln\zeta(\sigma+it)\to-\infty$ when $\sigma\to 1$ (we restrict to $\Re(\sigma)>1$). But, by the Euler identity, one has $\ln\zeta(s)=\sum_p\sum_{m\ge1}m^{-1}p^{-m\sigma}\exp(-itm\ln(p))$ and so

$$\Re\ln\zeta(s)=\sum_p\sum_{m\ge1}m^{-1}p^{-m\sigma}\cos(-tm\ln(p)).$$

Mertens' trick consists in noticing that $2(1+\cos\beta)^2=3+4\cos\beta+\cos 2\beta\ge 0$, thus $3\ln\zeta(\sigma)+4\Re\ln\zeta(\sigma+it)+\Re\ln\zeta(\sigma+2it)\ge 0$, hence $\zeta^3(\sigma)|\zeta^4(\sigma+it)\zeta(\sigma+2it)|\ge 1$.
But, as $\sigma\to 1$, one has $\zeta(\sigma)\sim(\sigma-1)^{-1}$ and $|\zeta(\sigma+it)|\sim A(\sigma-1)$ for a some constant A (by analyticity). So one should have $\zeta(\sigma+2it)\to\infty$, this contradicts the fact that $\zeta(1+2it)$ is bounded (by the Abel summation criterion). In conclusion, the ζ function has no zero with $\Re(\rho)=1$, the PNT is proved. Note that by mixing his proof of the PNT and the proof of Dirichlet's theorem, La Vallée Poussin proved also that there is asymptotically $\pi(x)/\phi(q)$ primes of the shape $a+qn$ less than x. An elementary (i.e. without complex analysis) proof of the PNT was subsequently found by Erdős and Selberg in 1949 (see [4] and [9]).

4. **Chebyshev's Bias**

All numerical evidence shows that $\pi(x)<\mathrm{Li}(x)$ and it was long believed that this would be true for all x. Similarly, Chebyshev noted that the number of primes of the form $4k+3$ seemed to be more abundant than the primes of the form $4k+1$, more precisely, let $\pi_{q,a}(x)=|\{p\le x:p\equiv a \bmod q\}|$ then $\pi_{4,3}(x)\ge\pi_{4,1}(x)$.

In fact, Littlewood proved in 1914 that $\pi(x) - \mathrm{Li}(x)$ changes sign infinitely often and the same is true for $\pi_{4,3}(x) - \pi_{4,1}(x)$. In 1957 Leech showed that $\pi_{4,1}(x) > \pi_{4,3}(x)$ is first true for $x = 26861$. That the similar inequality $\pi_{3,1}(x) > \pi_{3,2}(x)$ is first true for $x = 608981813029$ was shown by Bays and Hudson in 1978. No example of $\pi(x) > \mathrm{Li}(x)$ is known. Skewes first gave an upper bound $e^{e^{e^5}}$ which was later reduced by Sherman-Lehman and then te Riele [10] who gave an upper bound of 10^{370}.

This behaviour can easily be explained using explicit formulas. In the case of $\pi(x)$, the point is the following: The explicit formula (6) expresses $\psi(x)$ as a sum of powers x^ρ. Assuming the Riemann Hypothesis, one can write this as

$$\psi(x) = x - x^{1/2}\left(\sum_{\zeta(1/2+i\gamma)=0} \frac{x^{i\gamma}}{1/2+i\gamma}\right) + o(x^{1/2}).$$

One can now see the reason for the bias: The function $\psi(x)$ does not count primes but prime powers so what one really wants is the behaviour of $\theta(x)$ which is given by

$$\theta(x) = \psi(x) - \theta(\sqrt{x}) + O(x^{1/3}),$$

so that

$$\theta(x) = x - x^{1/2}\left(1 + \sum_{\zeta(1/2+i\gamma)=0} \frac{x^{i\gamma}}{1/2+i\gamma}\right) + o(x^{1/2}).$$

The function

$$\sum_{\zeta(1/2+i\gamma)=0} \frac{e^{i\gamma\ln(x)}}{1/2+i\gamma},$$

is a very slowly oscillating trigonometric series which should be zero on average, so the extra term biases $\theta(x)$ to be smaller than x on average. A simple description is that $\mathrm{Li}(x)$ counts the number of prime powers $\leq x$, so the number of primes should be slightly less since the number of prime squares is of the same order as the error term.

There is a similar explanation for the bias in arithmetic progressions. There is an explicit formula

$$\sum_{p^n \leq x} \chi(n)\ln(p) = -x^{1/2}\left(\sum_{L(1/2+i\gamma_\chi,\chi)=0} \frac{x^{i\gamma_\chi}}{1/2+i\gamma_\chi}\right) + o(x^{1/2}),$$

where the *Generalised Riemann Hypothesis* has been assumed (there is no x term since $L(1,\chi)$ is no longer a pole if $\chi \neq \chi_0$). As before one has

$$\psi_{q,a}(x) = \sum_{\substack{p^n \equiv a \bmod q \\ p^n \leq x}} \ln(p) = \frac{x}{\phi(q)} - \frac{x^{1/2}}{\phi(q)} \sum_\chi \overline{\chi(a)} \sum_{L(1/2+i\gamma_\chi)=0} \frac{x^{i\gamma_\chi}}{1/2+i\gamma_\chi}$$

but one really wants to look at

$$\theta_{q,a}(x) = \sum_{\substack{p \equiv a \bmod q \\ p \leq x}} \ln(p) = \psi_{q,a}(x) - \sum_{\substack{p^2 \equiv a \bmod q \\ p^2 \leq x}} \ln(p) + O(x^{1/3}) = \psi_{q,a}(x) - c_{q,a}x^{1/2} + O(x^{1/3}),$$

where $c_{q,a}$ is the number of solutions of $y^2 \equiv a \bmod q$. In particular, the same argument shows that there will always be fewer primes in the progression $qn + a$ when a is a residue than when a is a nonresidue. Simply put, the "balanced" count is the set of prime powers $\equiv a \bmod q$ so there are fewer primes $\equiv a \bmod q$ when a is quadratic residue since the number of prime squares congruent to a is of the same order as the error term in the analytic formulas.

In 1994, Rubinstein and Sarnak [8] were able to make Chebyshev's bias precise. Assuming GRH (if this is false, then there is no bias) and also the Grand Simplicity Hypothesis (GSH: All the ordinates of zeroes of L-function are linearly independent over $\mathbb{Q}$), then

$$\frac{1}{\ln(x)} \sum_{\substack{\pi(n)>\mathrm{Li}\, n \\ n\leq x}} \to .00000026, \qquad \frac{1}{\ln(x)} \sum_{\substack{\pi_{4,3}(n)>\pi_{4,1}(n) \\ n\leq x}} \to .9959.$$

Bibliography

[1] Daboussi (Hédi). – Sur le théorème des nombres premiers. *Comptes Rendus des Séances de l'Académie des Sciences. Série I. Mathématique*, vol. 298, n° 8, 1984, pp. 161–164.

[2] Davenport (Harold). – *Multiplicative Number Theory.* – Springer-Verlag, New York, 1980, second edition, xiii+177p. Revised by Hugh L. Montgomery.

[3] Dirichlet (L.). – Beweis des Satzes, das jede unbegrenzte arithmetische Progression... *Abh. König. Preuss. Akad.*, vol. 34, 1837, pp. 45–81.

[4] Erdős (P.). – On a New Method in Elementary Number Theory which leads to an Elementary Proof of the Prime Number Theorem. *Proceedings of the National Academy of Sciences. U.S.A.*, vol. 35, 1949, pp. 374–384.

[5] Friedlander (John) and Iwaniec (Henryk). – Using a Parity-Sensitive Sieve to Count Prime Values of a Polynomial. *Proceedings of the National Academy of Sciences. U.S.A.*, vol. 94, n° 4, 1997, pp. 1054–1058.

[6] Niven (Ivan). – A Simple Proof that π is Irrational. *Bulletin of the American Mathematical Society*, vol. 53, 1947, p. 509.

[7] Ribenboim (Paulo). – *The New Book of Prime Number Records.* – Springer-Verlag, New York, 1996, xxiv+541p.

[8] Rubinstein (Michael) and Sarnak (Peter). – Chebyshev's Bias. *Experimental Mathematics*, vol. 3, n° 3, 1994, pp. 173–197.

[9] Selberg (Atle). – An Elementary Proof of the Prime-Number Theorem. *Annals of Mathematics (2)*, vol. 50, 1949, pp. 305–313.

[10] te Riele (Herman J. J.). – On the Sign of the Difference $\pi(x) - \mathrm{Li}(x)$. *Mathematics of Computation*, vol. 48, n° 177, 1987, pp. 323–328.

[11] Tenenbaum (Gérald) and Mendès France (Michel). – *Les nombres premiers.* – Presses Universitaires de France, Paris, 1997, 128p.

Premiers chiffres significatifs et nombres algébriques

Ilan Vardi
IHES

December 10, 1998

[summary by M.-J. Bertin]

Abstract

Let α and β, $1 \le \alpha < \beta$ and define $\log_\beta(\alpha) = \frac{\log \alpha}{\log \beta}$. Denote by $\{z\}$ the fractional part of z i.e. $\{z\} = z - \lfloor z \rfloor$. The main result is the analytic continuation in $\mathbb{C}$ of the L-series $L(s,\alpha,\beta) = \sum_{n\ge 1}\{\log_\beta \frac{n}{\alpha}\}\frac{1}{n^s}$ if and only if β is a Pisot number, α belonging to the number field generated by β and the second largest conjugate of β being real or the corresponding conjugate of α being positive.

1. Introduction

La motivation de ce travail est la "loi" probabiliste de Benford, disant que les entiers rationnels n satisfaisant

$$\beta^h \le n < \alpha\beta^h$$

pour α et β vérifiant $1 \le \alpha < \beta$, apparaissent parmi les entiers rationnels avec une probabilité $\log_\beta(\alpha) = \log \alpha / \log \beta$. En réalité, cette "loi" est fausse car $\log_{10} n$ n'est pas une suite équirépartie modulo 1.

Cependant, la loi est vraie en moyenne harmonique d'après le théorème de Duncan prouvant que

$$\frac{\sum_{n<x}^{*} \frac{1}{n}}{\sum_{n<x} \frac{1}{n}} \underset{x\to\infty}{\longrightarrow} \log_\beta(\alpha),$$

la sommation $\sum^*$ étant faite sur les entiers n satisfaisant les inégalités

$$\beta^h \le n < \alpha\beta^h.$$

2. Les résultats

D'après un résultat de Diaconis, la limite précédente est équivalente à la formule

$$\lim_{s\to 1^+} (s-1)\zeta_{\alpha,\beta}(s) = \log_\beta(\alpha),$$

où

$$\zeta_{\alpha,\beta}(s) = \sum_{n\ge 1}^{*} \frac{1}{n^s}.$$

Par ailleurs, $\zeta_{\alpha,\beta}(s)$ peut s'écrire

$$\zeta_{\alpha,\beta}(s) = L(s,\alpha,\beta) - L(s,1,\beta) + \zeta(s)\log_\beta(\alpha),$$

où

$$L(s,\alpha,\beta) = \sum_{n\geq 1} \{\log_\beta \frac{n}{\alpha}\} \frac{1}{n^s}$$

et $\zeta(s)$ désigne la fonction dzêta de Riemann.

Il est naturel de s'intéresser au prolongement analytique dans $\mathbb{C}$ des séries $L(s,\alpha,\beta)$ et $\zeta_{\alpha,\beta}(s)$. En effet, en 1997, Kuba a montré le lien entre la série $L(s,\alpha,\beta)$ et le nombre de points d'un réseau situés sous une courbe logarithmique. Auparavant, Hecke avait montré que la fonction $\sum_{n\geq 1}\{\theta n\}n^{-s}$ possède un prolongement analytique à $\mathbb{C}$ si θ est un irrationnel quadratique. De même, Hardy et Littlewood ont montré que le prolongement admet une frontière naturelle si θ admet une bonne approximation par des rationnels.

Avant de présenter les résultats d'I. Vardi, rappelons qu'un nombre de Pisot (resp. Salem) est un entier algébrique supérieur à 1 dont tous les autres conjugués ont un module strictement inférieur à 1 (resp. inférieur ou égal à 1 avec au moins un conjugué de module 1).

Théorème 1. *La fonction $L(s,\alpha,\beta)$ admet un prolongement analytique dans le demi-plan $\sigma = \Re s > 0$. Ou bien la droite $\sigma = 0$ est une frontière naturelle pour la fonction L ou bien la fonction L est méromorphe dans $\mathbb{C}$.*

Si L est méromorphe dans $\mathbb{C}$, alors β est un nombre de Pisot ou de Salem et $\alpha \in \mathbb{Q}(\beta)$.

En outre, si $\alpha \in \mathbb{Z}[1/\beta]/f'(\beta)$, où f désigne le polynôme minimal de β, le prolongement analytique dans $\mathbb{C}$ est équivalent au fait que le deuxième plus petit conjugué de β soit réel (par suite β est un nombre de Pisot).

Si $\alpha \notin \mathbb{Z}[1/\beta]/f'(\beta)$ et si β est un nombre de Pisot, l'existence du prolongement analytique dans $\mathbb{C}$ est équivalente à l'existence d'un entier m ne divisant pas la trace de $m\alpha\beta^k$ pour k assez grand. Si β est un nombre de Salem, il n'y a pas équivalence, cette dernière condition étant seulement nécessaire.

Corollaire 1. *La fonction $\zeta_{\alpha,\beta}(s)$ admet un prolongement méromorphe dans $\sigma = \Re s > 0$ et ou bien la droite $\sigma = 0$ est une frontière naturelle ou bien le prolongement est méromorphe dans tout le plan.*

L'existence d'un prolongement méromorphe est équivalente au fait que β soit un nombre de Pisot, α appartenant au corps de nombres engendré par β et ou bien le deuxième plus grand conjugué de β est réel ou bien $\alpha \in \mathbb{Z}[1/\beta]/f'(\beta)$ et le conjugué de α correspondant au deuxième plus grand conjugué de β est positif.

Proposition 1. *Pour tout nombre de Pisot ou de Salem β, il existe une infinité de α appartenant au corps de nombres engendré par β tels que $L(s,\alpha,\beta)$ possède un prolongement analytique dans $\mathbb{C}$.*

Bibliography

[1] Amara (Mohamed). – Ensembles fermés de nombres algébriques. *Annales Scientifiques de l'École Normale Supérieure*, vol. 83, n° 3, 1966, pp. 215–270.

[2] Berend (Daniel) and Frougny (Christiane). – Computability by finite automata and Pisot bases. *Mathematical Systems Theory. An International Journal on Mathematical Computing Theory*, vol. 27, n° 3, 1994, pp. 275–282.

[3] Bertin (M.-J.), Decomps-Guilloux (A.), Grandet-Hugot (M.), Pathiaux-Delefosse (M.), and Schreiber (J.-P.). – *Pisot and Salem numbers.* – Birkhäuser Verlag, Basel, 1992, xiv+291p. With a preface by David W. Boyd.

[4] Diaconis (Persi). – *Weak and strong averages in probability and the theory of numbers.* – PhD thesis, Department of Statistics, Harvard University, 1974.

[5] Duke (William). – Lattice points in cones. – Preprint, 1990.

[6] Duncan (R. L.). – A note on the initial digit problem. *Fibonacci Quarterly*, vol. 7, 1969, pp. 474–475.

[7] Fel'dman (N. I.). – Estimation of a linear form in the logarithms of algebraic numbers. *Matematicheskiĭ Sbornik. Novaya Seriya.*, vol. 76, n° 118, 1968, pp. 304–319. – (Russian).

[8] Gupta (Rajiv) and Murty (M. Ram). – A remark on Artin's conjecture. *Inventiones Mathematicae*, vol. 78, n° 1, 1984, pp. 127–130.

[9] Hardy (G. H.) and Littlewood (J. E.). – Some problems of diophantine approximation. *Transactions of the Cambridge Philosophical Society*, vol. 22, 1923, pp. 519–533.

[10] Heath-Brown (D. R.). – Artin's conjecture for primitive roots. *The Quarterly Journal of Mathematics. Oxford. Second Series*, vol. 37, n° 145, 1986, pp. 27–38.

[11] Hecke (E.). – Über analytische Funktionen und die Verteilung von Zahlen mod Eins. *bhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 1, 1921, pp. 54–76.

[12] Hill (Theodore P.). – Base-invariance implies Benford's law. *Proceedings of the American Mathematical Society*, vol. 123, n° 3, 1995, pp. 887–895.

[13] Hill (Theodore P.). – Le premier chiffre significatif fait sa loi. *La Recherche*, 1999, pp. 72–75.

[14] Hooley (Christopher). – On Artin's conjecture. *Journal für die Reine und Angewandte Mathematik*, vol. 225, 1967, pp. 209–220.

[15] Kahane (Jean-Pierre) and Salem (Raphaël). – *Ensembles parfaits et séries trigonométriques.* – Hermann, Paris, 1994, second edition, 245p.

[16] Knuth (Donald E.). – *The art of computer programming.* – Addison-Wesley Publishing Co., Reading, Mass., 1973, 2nd edition, xi+722 pp.p. Volume 3. Sorting and searching.

[17] Kuba (G.). – The number of lattice points below a logarithmic curve. *Archiv der Mathematik*, vol. 69, n° 2, 1997, pp. 156–163.

[18] Lang (Serge). – *Algebraic numbers.* – Addison-Wesley Publishing Co., Reading, Mass., 1964, ix+163p.

[19] Meyer (Yves). – *Algebraic numbers and harmonic analysis.* – North-Holland Publishing Co., Amsterdam, 1972, x+274p.

[20] Mignotte (Maurice). – Sur les conjugués des nombres de Pisot. *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique*, vol. 298, n° 2, 1984, p. 21.

[21] Pólya (G.). – Sur les séries entières à coefficients entiers. *Proceedings of the London Mathematica Society*, vol. 21, 1923, pp. 22–38.

[22] Salem (R.). – Power series with integral coefficients. *Duke Mathematical Journal*, vol. 12, 1945, pp. 153–172.

[23] Salem (Raphaël). – *Algebraic numbers and Fourier analysis.* – D. C. Heath and Co., Boston, Mass., 1963, x+68p.

[24] Serre (Jean-Pierre). – *Abelian l-adic representations and elliptic curves.* – A K Peters Ltd., Wellesley, MA, 1998, 199p. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[25] Shanks (Daniel). – Fibonacci primitive roots. *Fibonacci Quarterly*, vol. 10, n° 2, 1972, pp. 163–168, 181.

[26] Stevenhagen (P.) and Lenstra, Jr. (H. W.). – Chebotarëv and his density theorem. *The Mathematical Intelligencer*, vol. 18, n° 2, 1996, pp. 26–37.

[27] Tenenbaum (G.). – Communication personnelle, 1998.

[28] Vardi (Ilan). – Premiers chiffres significatifs et nombres algébriques. *Comptes Rendus de l'Académie des Sciences. Série I. Mathématique*, vol. 328, n° 9, 1999, pp. 749–754.

Algorithms in Classical Cryptanalysis

François Morain

LIX, École polytechnique

November 23, 1998

Abstract

Till the end of World War I, cryptographic methods required only paper and pencil. Since this glorious period, machines first and then computers replace man in complicated cyphering and decyphering processes. It is interesting to consider this period with an algorithmic viewpoint and seek computer algorithms to break those old cyphers.

This talk describes algorithmic tools that can be used to break as automatically as possible cryptosystems based on mono- or polyalphabetical substitutions as well as transpositions. In particular, the talk will focus on combinatorial optimization methods, such as genetic algorithms. New ideas are also presented, that make it possible to break some systems with ease.

Contents

Part 1. Combinatorics

Part 5. Number Theory

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