Algorithms seminars 1992-1993

Bruno Salvy

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE

Algorithms Seminar 1992-1993

Bruno SALVY
(Editor)

N ° 2130
Décembre 1993
PROGRAMME 2

ISSN 0249-6399

ALGORITHMS SEMINAR,

1992–1993

Bruno Salvy

(Editor)

Abstract

These seminar notes represent the proceedings (some in French) of a seminar devoted to the analysis of algorithms and related topics. The subjects covered include combinatorial models and random generation, symbolic computation, asymptotic analysis, average-case analysis of algorithms and data structures, and some computational number theory.

SÉMINAIRE ALGORITHMES,

1992–1993

Résumé

Ces notes de séminaires représentent les actes, pour la plupart en anglais, d'un séminaire consacré à l'analyse d'algorithmes et aux domaines connexes. Les thèmes abordés comprennent : modèles combinatoires, génération aléatoire, calcul formel, analyse asymptotique, analyse en moyenne d'algorithmes et de structures de données, ainsi qu'un peu de théorie algorithmique des nombres.

ALGORITHMS SEMINAR
1992–1993

Bruno Salvy[1]
(Editor)

Abstract

These seminar notes represent the proceedings (some in French) of a seminar devoted to the analysis of algorithms and related topics. The subjects covered include combinatorial models and random generation, symbolic computation, asymptotic analysis, average-case analysis of algorithms and data structures, and some computational number theory.

This is the second of our series of seminar proceedings. These summaries, usually written by a reporter from the audience, form the content of these proceedings.

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 and asymptotic analysis.

Several articles deal with combinatorial enumerations of classical combinatorial objects or their random generation, useful for simulations and empirical studies.

Computer algebra plays an increasingly important rôle in this area. It provides a collection of tools that permit to analyse complex models of combinatorics and the analysis of algorithms; at the same time, it inspires the quest for developing ever more systematic solutions to the analysis of well characterized classes of problems. In this vein, the notes contain several recent developments regarding the automatic computation of limits and the manipulation of recurrences or their generating function counterparts.

Asymptotic methods include singularity analysis, the saddle point method, functional equations like the ones related to divide–and–conquer recurrences, uniform asymptotic expansions and resummation.

The 39 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 AND RANDOM GENERATION

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 strings, trees, graphs, permutations.

In **[1]** the theory of species is introduced. A variant of the classical problem of Young tableaux is analyzed in **[2]**. Some probabilistic methods in combinatorics are the subject of **[3]** and **[4]**. The last three articles of this part present problems and solutions in random generation of combinatorial structures. A general approach is given in **[6]**, while efficient special cases are described in **[5]** and **[7]**.

[1]This work was supported in part by the ESPRIT III Basic Research Action Programme of the E.C. under contract ALCOM II (#7141).

[1] Enumerations related to automorphisms of rooted tree structures *Gilbert Labelle*
[2] A class of formal power series helps enumerate Young paths *François Bergeron*
[3] Sums of independent random variables and some combinatorial problems *V. Kolchin*
[4] Branching processes, random trees and Brownian excursion *Vladimir Vatutin*
[5] Tirage aléatoire de mots et d'objets combinatoires *Alain Denise*
[6] A Calculus of Random Generation *Philippe Flajolet*
[7] Quelques exemples d'algorithmes de génération aléatoire *Dominique Gouyou-Beauchamps*

PART II. SYMBOLIC COMPUTATION

Most exactly solvable models of combinatorics and analysis of algorithms rest on a suitable algebra of *generating functions*. Once this has been recognized, an important goal is to find decision procedures for these classes of generating functions. Computer algebra systems provide a way of testing and implementing the methods, and the problem of optimizing the corresponding procedures often represents a non trivial problem of symbolic computation.

Several algorithms have already implemented in this domain [8]. One important class of generating function is the class of holonomic functions, that are solutions of linear differential equations with polynomial coefficients. For instance, the analysis of such differential equations naturally gives rise to divergent series that can be exploited [13]. Equivalently, the sequence of coefficients of these generating function is solution to a linear recurrence with polynomial coefficients also known as a P-finite recurrence [9]. Any kind of solution to these recurrence or differential equations can be used to help the analysis, and very nice algorithms exist to find rational solutions [10]. It is also very important to be able to compute the expansion of a function in the neighbourhood of a singularity. A new model for doing this is described in [11]. Symbolic integration is one of the most famous successes of computer algebra, its basics are reviewed in [12]. It is sometimes useful to get numerical estimates of the singularities, and a new algorithm in this context is given in [14]. Computer algebra can also be used in some problems of celestial mechanics [15].

[8] Automatic Asymptotics and Generating Functions *Bruno Salvy*
[9] Symbolic Computation with P-finite Sequences *Marko Petkovšek*
[10] Rational Solutions of Linear Difference and Differential Equations *Sergeï Abramov*
[11] Limit Computation in Computer Algebra *Dominik Gruntz*
[12] Introduction to symbolic integration *Bruno Salvy*
[13] Summation of series solutions of linear differential equations *Michèle Loday-Richaud*
[14] The exclusion algorithm *Jean-Claude Yakoubsohn*
[15] Construction d'intégrateurs symplectiques pour des mouvements kepleriens *Pierre-Vincent Koseleff*

PART III. ASYMPTOTIC ANALYSIS

Asymptotic analysis is an essential ingredient in the interpretation of quantitative results supplied by the resolution of combinatorial models.

An important class of problems involves recovering the asymptotic form of the coefficients of a function from asymptotic properties of the function itself. A survey of analytic methods for this problem is given in [16], with applications to limit distributions. An application of singularity analysis to the localization of roots of families of polynomials is given in [17]. Two articles attack problems where arithmetic properties of the index of the sequence are crucial in the analysis [18,19]. Some questions involving the asymptotics of multiple integrals are the subject of [20]. The technique of uniform asymptotics of integrals is the basis of [21], while rigourous resummation of divergent series is the theme of [22].

PART IV. ANALYSIS OF ALGORITHMS AND DATA STRUCTURES

This part deals with the analysis of algorithms and data structures. Trees have been recognized by various authors as the single most important structure in computer science. Not unnaturally, several analyses found here are devoted to tree structures.

A broad survey of the domain is given by **[23]**. A probabilistic algorithm for finding the height of a random tree is analyzed in **[24]**. New explicit results on quadtrees are presented in **[25]**. A probabilistic analysis of Ziv-Lempel algorithms is provided by **[26]**. Heap-ordered trees lead to divide-and-conquer recurrences whose asymptotic behaviour is related to binary representations of integers, this is the subject of **[27]**.

The other presentations in this part present algorithms and analyses for a variety of application problems. String matching in parallel is investigated in **[28]**. Protocols for regulating access to networks are the subject of **[29]**, where flow control from the emitting source is studied, and of **[30]**, a presentation that surveys an attractive alternative to the Ethernet protocol based on stack/tree resolution algorithms.

In the area of seminumerical algorithms, knowledge regarding number of steps of the Euclidean algorithm is summarized in **[31]**. Grid techniques for dynamic closest-pair problems are analyzed in **[32]**. The last two talks discuss recurrence relations either for the analysis of parallel models of computation **[33]** or for probabilistic divide-and-conquer algorithms **[34]**.

PART V. MISCELLANY

This part contains several problems of computational number theory **[35]**, **[36]**, as well as algebraic geometry **[37]**, plus introductions to computational genetics **[38]** and fractals **[39]**.

[38] Cartographie physique globale du Génome humain *Jean-Jacques Codani Bruno Lacroix*
[39] Géométrie fractale *Jacques Levy Vehel*

Acknowledgements. The lectures summarized here emanate from a seminar attended by a community of researchers in the analysis of algorithms, in the Algorithms Project at INRIA (Ph. Flajolet, F. Morain and B. Salvy are the organizers) and in the greater Paris area—especially École Polytechnique (J.-M. Steyaert), University of Paris Sud at Orsay (D. Gouyou-Beauchamps, D. Gardy) and LITP (M. Soria).

The editor expresses his gratitude to the various persons who supported actively this joint enterprise, most notably: Xavier Gourdon, Dominique Gouyou-Beauchamps, Mireille Régnier, Michèle Soria, Paul Zimmermann. Thanks are due also to the speakers and to the authors of summaries. Many of them have come from far away to attend one seminar and nicely accepted to write the summary.

We are especially indebted to Philippe Dumas for his time, and to Virginie Collette for permanently keeping the wheel in motion.

The Editor
B. SALVY

Part I

Combinatorial Models and Random Generation

Enumerations related to automorphisms of rooted tree structures

Gilbert Labelle
LACIM, UQAM, Montréal

June 7, 1993

[summary by Dominique Gouyou-Beauchamps]

Abstract

The goal of this paper is to present a panorama of the fundamental properties of *cycle index series* and *asymmetry index series* within enumerative combinatorics, as well as a few concrete applications. A given structure is said to be *asymmetric* if its automorphism group reduces to the identity. We introduce an *asymmetry indicator series* $\Gamma_F(x_1, x_2, x_3, \ldots)$ by means of which we study the correspondence $F \to \bar{F}$ in connection with the various operations existing in the theory of species of structures. It is shown that all these operations are automatically computable but this aspect is not developed in the summary.

1. Species and Asymmetry Index Series

Given any finite set U, let us denote by $A[U]$ the set of all *rooted trees* having U as underlying set of vertices. Clearly, every bijection $\beta : U \to V$ between finite sets induces another bijection which we denote by $A[\beta] : A[U] \to A[V]$ and call the *transportation* of rooted trees along β (we replace each vertex u in a by the corresponding vertex $\beta(u)$). Of course, transportation commutes with composition in the following way: given any two successive bijections $\beta : U \to V, \beta' : V \to W$, we have $A[\beta' \circ \beta] = A[\beta'] \circ A[\beta]$ and $A[1_U] = 1_{A[U]}$ (where 1_U denotes, as usual, the identity bijection of a finite set U into itself).

A *combinatorial species* [5] is a functor from the category of finite sets and bijections into itself. In other words, a combinatorial species is a rule F that associates a finite set $F[U]$ to any finite set U and a bijection $F[\beta] : F[U] \to F[V]$ to any bijection $\beta : U \to V$. An element $s \in F[U]$ is called an *F-structure* on the underlying set U. The bijection $F[\beta]$ is called the *transportation* of F-structures *along* β.

In the case of *weighted species* F, each F-structure s is given a weight $w_F(s)$ in a certain commutative ring $\mathcal{R}$ and the transportation $F[\beta]$ must preserve these weights.

Given a species F and two F-structures $s \in F[U]$ and $s' \in F[V]$, an *isomorphism* β from s to s' is a bijection $\beta : U \to V$ such that $F[\beta](s) = s'$. Two isomorphic F-structures are said to be of the same *type*. An *automorphism* of s is an isomorphism from s to s. The automorphisms of any given F-structure s form a group called the *automorphism group* of s. When this group is trivial, the structure s is said to be *asymmetric*.

For each integer n, consider now the set $\underline{n} = \{1, 2, \ldots, n\}$. It is easy to see that any species F induces, by transportation, a countable family of actions of the symmetric group S_n:

$$S_n \times F[\underline{n}] \to F[\underline{n}], \quad n = 0, 1, 2, \ldots.$$

Given a weighted species F, the formal power series

$$F(x) = \sum_{n\geq 0} f_n \frac{x^n}{n!}, \quad \tilde{F}(x) = \sum_{n\geq 0} \tilde{f}_n x^n, \quad \bar{F}(x) = \sum_{n\geq 0} \bar{f}_n x^n,$$

whose coefficients are defined by

$$\begin{aligned}
f_n &= \text{the sum of the weights of the } F\text{-structures on any } n\text{-element set} \\
&= \text{the sum of the weights of the elements of } F[\underline{n}], \\
\tilde{f}_n &= \text{the sum of the weights of the types of } F\text{-structures on any } n\text{-element set} \\
&= \text{the sum of the weights of the orbits of the action } S_n \times F[\underline{n}] \to F[\underline{n}], \\
\bar{f}_n &= \text{the sum of the weights of the types of asymmetric } F\text{-structures on any } n\text{-element set} \\
&= \text{the sum of the weights of the } n!\text{-point orbits of the action } S_n \times F[\underline{n}] \to F[\underline{n}],
\end{aligned}$$

are respectively called the (exponential) *generating series* of F, the *types generating series* of F, and the *asymmetry types generating series* of F.

EXAMPLE. For every $n \geq 0$ let

$$\begin{aligned}
a_n &= \text{the number of rooted trees on } n \text{ given vertices} \\
&= \text{the number of elements of } A[\underline{n}], \\
\tilde{a}_n &= \text{the number of types of of rooted trees on } n \text{ vertices} \\
&= \text{the number of orbits of the action } S_n \times A[\underline{n}] \to A[\underline{n}], \\
\bar{a}_n &= \text{the number of types of asymmetric rooted trees on } n \text{ vertices} \\
&= \text{the number of } n!\text{-point orbits of the action } S_n \times A[\underline{n}] \to A[\underline{n}].
\end{aligned}$$

These sequences of numbers can be "encoded" into the series

$$\begin{aligned}
A(x) &= \sum_{n\geq 0} a_n \frac{x^n}{n!} = x + 2\frac{x^2}{2!} + 9\frac{x^3}{3!} + 64\frac{x^4}{4!} + 625\frac{x^5}{5!} + 7776\frac{x^6}{6!} + 117649\frac{x^7}{7!} + \cdots, \\
\tilde{A}(x) &= \sum_{n\geq 0} \tilde{a}_n x^n = x + x^2 + 2x^3 + 4x^4 + 9x^5 + 20x^6 + 48x^7 + 115x^8 + \cdots, \\
\bar{A}(x) &= \sum_{n\geq 0} \bar{a}_n x^n = x + x^2 + x^3 + 2x^4 + 3x^5 + 6x^6 + 12x^7 + 25x^8 + \cdots.
\end{aligned}$$

Given two species F and G, other species can be constructed: the *sum* $F+G$, the *product* $F \cdot G$, the *substitution* $F(G)$ (also denoted $F \circ G$), and the *derivative* F' (also denoted dF/dX). The generic structures belonging to each of these species are described as follows:

(1) s is an $(F+G)$-structure on U *iff* s is an F-structure on U or a G-structure on U (the "or" is an "exclusive or"),

(2) s is an $(F\cdot G)$-structure on U *iff* $s = (f, g)$ where f is an F-structure on U_1, g is a G-structure on U_2, and $U_1 \cup U_2 = U$, $U_1 \cap U_2 = \emptyset$,

(3) s is an $F(G)$-structure on U *iff* $s = (f, \gamma)$ where γ is a set of G-structures having disjoint underlying sets whose union is U, and f is an F-structure on the set γ (the assumption $G[\emptyset] = \emptyset$ is made in order to have a finite number of $F(G)$-structures on each U),

(4) s is an F'-structure on U *iff* s is an F-structure on the augmented set $U \cup \{\star\}$, where $\star$ denotes a point outside U.

The passage from species to series satisfies the following properties:

- The transformation $F \to F(x)$ commutes with combinatorial sums, products, substitutions, and derivations:

$$(F+G)(x) = F(x) + G(x), \qquad (F\cdot G)(x) = F(x)\cdot G(x),$$
$$(F\circ G)(x) = F(G(x)), \qquad F'(x) = dF(x)/dx.$$

- The transformations $F \to \tilde{F}(x)$ and $F \to \bar{F}(x)$ commute with combinatorial sums and products but do not commute, in general, with substitutions and derivations:

$$\widetilde{(F+G)}(x) = \tilde{F}(x) + \tilde{G}(x), \qquad \overline{(F+G)}(x) = \bar{F}(x) + \bar{G}(x),$$
$$\widetilde{(F\cdot G)}(x) = \tilde{F}(x)\cdot\tilde{G}(x), \qquad \overline{(F\cdot G)}(x) = \bar{F}(x)\cdot\bar{G}(x),$$
$$\widetilde{(F\circ G)}(x) \neq \tilde{F}(\tilde{G}(x)), \qquad \overline{(F\circ G)}(x) \neq \bar{F}(\bar{G}(x)),$$
$$\widetilde{F'}(x) \neq d\tilde{F}(x)/dx, \qquad \overline{F'}(x) \neq d\bar{F}(x)/dx.$$

Consider an infinite sequence $t = (t_1, t_2, t_3, \dots)$ of distinct formal "weights" and, given a finite set U, define an F_t-structure on U as being a couple $s = (f, v)$ where f is an F-structure on U and $v : U \to \{1, 2, 3, \dots\}$ is a function that assigns an arbitrary positive integer to each element of U. Define the t-weight of the structure s by $w(s) = \prod_{u\in U} t_{v(u)}$.

Given a bijection $\beta : U \to V$, define the transportation $F_t[\beta] : F_t[U] \to F_t[V]$ by

$$F_t[\beta](s) = (F[\beta](f), v\circ\beta^{-1}).$$

Of course, the two series $\tilde{F}_t(x)$ and $\bar{F}_t(x)$ can be associated to the weighted species F_t and each series is easily seen to be a symmetric function of the t_i's [11].

Let F be any species and $t = (t_1, t_2, t_3, \dots)$ be a countable sequence of formal variables related to the variables $x_1, x_2, x_3, \dots$ by the equations

$$x_k = t_1^k + t_2^k + t_3^k + \cdots, \quad (k\text{-th power sum}), \quad k = 1, 2, 3, \dots.$$

The *cycle index series* Z_F and the *asymmetry index series* Γ_F are defined by

$$Z_F(x_1, x_2, x_3, \dots) = \text{the expression of the symmetric function } \tilde{F}_t(x)\,|_{x:=1}$$
$$\text{of } t_1, t_2, t_3, \dots \text{ in terms of the variable } x_1, x_2, x_3, \dots,$$
$$Z_\Gamma(x_1, x_2, x_3, \dots) = \text{the expression of the symmetric function } \bar{F}_t(x)\,|_{x:=1}$$
$$\text{of } t_1, t_2, t_3, \dots \text{ in terms of the variable } x_1, x_2, x_3, \dots.$$

It turns out that the cycle index series Z_F is the sum, over n, of the classical Pólya's cycle index polynomials of the family of actions $S_n \times F[\underline{n}] \to F[\underline{n}]$, of the symmetric group S_n, $n \geq 0$. Examples show that Γ_F contains informations independent of Z_F (and vice versa). Using the theory of symmetric functions and collecting monomials in $x_1, x_2, x_3, \dots$, both series can be written in the "standard form"

$$f(x_1, x_2, x_3, \dots) = \sum_{n\geq 0}\sum_{\sigma\vdash n} f_\sigma \frac{x_1^{\sigma_1} x_2^{\sigma_2}\cdots x_n^{\sigma_n}}{1^{\sigma_1}\sigma_1!\,2^{\sigma_2}\sigma_2!\cdots n^{\sigma_n}\sigma_n!},$$

where the coefficients f_σ satisfy

$$f_\sigma \in \mathbb{N} \text{ if } f = Z_F, \qquad \text{while} \qquad f_\sigma \in \mathbb{Z} \text{ if } f = \Gamma_F.$$

Species	**F**	F	$\tilde{F}$	$\bar{F}$	Z_F	Γ_F
singleton	X	x	x	x	x_1	x_1
pair	E_2	$\frac{x^2}{2!}$	x^2	0	$\frac{1}{2}(x_1^2+x^2)$	$\frac{1}{2}(x_1^2-x^2)$
set	E	$\exp(x)$	$\frac{1}{1-x}$	$1+x$	$\exp\left(\sum_{n\geq 1}\frac{x_n}{n}\right)$	$\exp\left(\sum_{n\geq 1}(-1)^{n-1}\frac{x_n}{n}\right)$
subset	$\mathcal{P}$	$\exp(2x)$	$\frac{1}{(1-x)^2}$	$(1+x)^2$	$\exp\left(2\sum_{n\geq 1}(-1)^{n-1}\frac{x_n}{n}\right)$	$\exp\left(2\sum_{n\geq 1}(-1)^{n-1}\frac{x_n}{n}\right)$
list	L	$\frac{1}{1-x}$	$\frac{1}{1-x}$	$\frac{1}{1-x}$	$\frac{1}{1-x_1}$	$\frac{1}{1-x_1}$
cycle	C	$\ln(\frac{1}{1-x})$	$\frac{x}{1-x}$	x	$\sum_{n\geq 1}\frac{\phi(n)}{n}\ln\left(\frac{1}{1-x_n}\right)$	$\sum_{n\geq 1}\frac{\mu(n)}{n}\ln\left(\frac{1}{1-x_n}\right)$
permutation	S	$\frac{1}{1-x}$	$\prod_{n\geq 1}\frac{1}{1-x^n}$	$1+x$	$\prod_{n\geq 1}\frac{1}{1-x_n}$	$\frac{1-x_2}{1-x_1}$

TABLE 1. Basic species and their generating series. Here $\phi(n)$ and $\mu(n)$ respectively denote the classical Euler and Möbius functions of n.

The notation $\sigma \vdash n$ means that $\sigma = (\sigma^1, \sigma^2, \ldots, \sigma^n)$ runs through the partitions of n, and σ_i is the number of parts of size i in σ.

The transformations $F \to Z_F$ and $F \to \Gamma_F$ both commute with combinatorial sums, products, substitutions and derivations:

$$(1) \qquad Z_{F+G} = Z_F + Z_G, \qquad Z_{F\cdot G} = Z_F \cdot Z_G, \qquad Z_{F\circ G} = Z_F \circ Z_G, \qquad Z_{F'} = \frac{\partial Z_F}{\partial x_1},$$

$$(2) \qquad \Gamma_{F+G} = \Gamma_F + \Gamma_G, \qquad \Gamma_{F\cdot G} = \Gamma_F \cdot \Gamma_G, \qquad \Gamma_{F\circ G} = \Gamma_F \circ \Gamma_G, \qquad \Gamma_{F'} = \frac{\partial \Gamma_F}{\partial x_1},$$

where $Z_F \circ Z_G$ (resp. $\Gamma_F \circ \Gamma_G$) denotes the plethystic substitution of the series Z_F and Z_G (resp. Γ_F and Γ_G). The *plethysm* $Z_F \circ Z_G$ of two series $Z_F = f(x_1, x_2, x_3, \ldots)$ and $Z_G = g(x_1, x_2, x_3, \ldots)$ is the series $f(g_1, g_2, g_3, \ldots)$, where $g_k(x_1, x_2, x_3, \ldots) = g(x_k, x_{2k}, x_{3k}, \ldots)$ [2].

The series $F(x)$, $\tilde{F}(x)$, and $\bar{F}(x)$ can be computed from Z_F and Γ_F by making use of the following remarkable formulas:

$$(3) \qquad F(x) = Z_F(x, 0, 0, \ldots) = \Gamma_F(x, 0, 0, \ldots),$$

$$(4) \qquad \tilde{F}(x) = Z_F(x, x^2, x^3, \ldots), \quad \bar{F}(x) = \Gamma_F(x, x^2, x^3, \ldots).$$

The following explicit formulas are direct consequences of (1)–(4):

$$\widetilde{(F \circ G)}(x) = Z_F(\tilde{G}(x), \tilde{G}(x^2), \ldots), \qquad \widetilde{F'}(x) = \frac{\partial Z_F}{\partial x_1}(x, x^2, x^3, \ldots),$$

$$\overline{(F \circ G)}(x) = Z_F(\bar{G}(x), \bar{G}(x^2), \ldots), \qquad \overline{F'}(x) = \frac{\partial \Gamma_F}{\partial x_1}(x, x^2, x^3, \ldots).$$

The series F, $\tilde{F}$, $\bar{F}$, Z_F, and Γ_F have been computed for many elementary species. Table 1 gives a short table.

Given any species F and any integer $n \in \mathbb{N}$ we can extract a subspecies $F_n \subseteq F$ by collecting all those F-structures having an underlying cardinality n. If $F = F_n$ we say that F is *concentrated*,

n	A	$n!Z_A$	$n!\Gamma_A$
1	X	x_1	x_1
2	E_2	$x_1^2 + x_2$	$x_1^2 - x_2$
3	E_3	$x_1^3 + 3x_1x_2 + 2x_3$	$x_1 - 3x_1x_2 + 2x_3$
3	C_3	$2x_1^3 + 4x_3$	$2x_1^3 - 2x_3$
4	E_4	$x_1^4 + 6x_1^2x_2 + 8x_1x_3 + 3x_2^2 + 6x_4$	$x_1^4 - 6x_1^2x_2 + 8x_1x_3 + 3x_2^2 - 6x_4$
4	$E_4^{\pm}$	$2x_1^4 + 16x_1x_3 + 6x_2^2$	$2x_1^4 - 6x_2^2 - 8x_1x_3 + 12x_4$
4	$E_2 \circ E_2$	$3x_1^4 + 6x_1^2x_2 + 9x_2^2 + 6x_4$	$3x_1^4 - 6x_1^2x_2 - 3x_2^2 + 6x_4$
4	P_4^{bic}	$6x_1^4 + 18x_2^2$	$6x_1^4 - 18x_2^2 + 12x_4$
4	C_4	$6x_1^4 + 6x_2^2 + 12x_4$	$6x_1^4 - 6x_2^2$
4	$E_2 \circ X^2$	$12x_1^4 + 12x_2^2$	$12x_1^4 - 12x_2^2$

TABLE 2. Atomic species on less than 4 points and their index and asymmetry index series.

or *lives*, on the cardinality n. In the general situation, we obviously have the following canonical decomposition:

$$F = F_0 + F_1 + F_2 + \cdots + F_n + \ldots . \tag{5}$$

The above canonical decomposition can be further refined by applying sums and products to fundamental 'building blocks' called *atomic species*. We recall that the atomic species constitute a countable set (working up to natural isomorphism)

$$\mathcal{A} = \{X, E_2, E_3, C_3, E_4, E_4^{\pm}, E_2 \circ E_2, P_4^{\mathrm{bic}}, C_4, E_2 \circ X^2, \ldots\}$$

and are defined as being the irreducible species with respect to both sums '+' and products '$\cdot$'. Moreover, $\mathcal{A}$ is a 'graded set'

$$\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3 \cup \cdots \cup \mathcal{A}_n \cup \cdots$$

where $\mathcal{A}_n$ is the finite set consisting of all those atomic species that are concentrated on cardinality n. A complete description of $\mathcal{A}_n$ can be found in [5, 8, 15]. It is well known (by Yeh's Theorem [8, 15]) that each F_n in decomposition (5) can be written in a unique way as a polynomial (with coefficients in $\mathbb{N}$) in the atomic species that live on cardinalities $\leq n$. Stated differently, this means that we have the following half-ring isomorphism

$$\mathrm{Species} \simeq \mathbb{N}[[X, E_2, E_3, C_3, E_4, E_4^{\pm}, E_2 \circ E_2, P_4^{\mathrm{bic}}, C_4, E_2 \circ X^2, \ldots]] = \mathbb{N}[[\mathcal{A}]]$$

where Species denotes the half-ring of all the species (under the operations '+' and '$\cdot$' and where equality '=' means natural isomorphism).

EXAMPLE. For the species Gr of simple graphs, we have the unique atomic decomposition:

$$Gr(X) = 1 + X + 2E_2 + 2X\cdot E_2 + 2E_3 + 2X^2\cdot E_2 + 2X\cdot E_3 + 2E_2\cdot E_2 + 2E_2 \circ E_2 + E_2 \circ X^2 + 2E_4 + \cdots .$$

The universal ring $\mathbf{V}$ containing $\mathbb{N}[[\mathcal{A}]]$ is called the *ring of virtual species*. Every element in $\mathbf{V}$ can be represented as $F - G$ where F and G are two species. The ring $\mathbf{V}$ is isomorphic to $\mathbb{Z}[[\mathcal{A}]]$ and is closed for the combinatorial sums, products, substitutions and derivations.

Table 2 gives the index series and the asymmetry index series (polynomial, in fact) of each atomic species on $n \leq 4$ points.

2. General Explicit and Recursive Formulas

Consider the combinatorial equation $A = X \cdot E(A)$ which characterizes the species A of rooted trees. We get in a purely mechanical way the following classical result [3]

$$A(x) = xe^{A(x)},\ \tilde{A}(x) = x\exp\left(\sum_{n\geq 1}\frac{\tilde{A}(x^n)}{n}\right),\ \bar{A}(x) = x\exp\left(\sum_{n\geq 1}(-1)^{n-1}\frac{\bar{A}(x^n)}{n}\right),$$

$$Z_A = x_1\exp\left(\sum_{n\geq 1}\frac{(Z_A)_n}{n}\right),\ \Gamma_A = x_1\exp\left(\sum_{n\geq 1}(-1)^{n-1}\frac{(\Gamma_A)_n}{n}\right).$$

The fundamental Otter-Robinson-Leroux [12, 14, 10] equation

$$\mathcal{A} + A^2 = A + E_2(A),$$

between the species A of rooted trees and the species $\mathcal{A}$ of ordinary trees, gives the following results

$$\mathcal{A}(x) = A(x) - \frac{1}{2}(A(x))^2,\quad \tilde{\mathcal{A}}(x) = \tilde{A}(x) - \frac{1}{2}(\tilde{A}(x))^2 + \frac{1}{2}\tilde{A}(x^2)\ \text{(Otter [12])},$$

$$\bar{\mathcal{A}}(x) = \bar{A}(x) - \frac{1}{2}(\bar{A}(x))^2 - \frac{1}{2}\bar{A}(x^2)\ \text{(Harary-Prins [3])},$$

$$Z_{\mathcal{A}} = Z_A - \frac{1}{2}(Z_A)^2 + \frac{1}{2}(Z_A)_2\ \text{(Robinson [14])},\quad \Gamma_{\mathcal{A}} = \Gamma_A - \frac{1}{2}(\Gamma_A)^2 - \frac{1}{2}(\Gamma_A)_2.$$

3. R-enriched rooted trees and R-enriched trees

The species A_R of *R-enriched rooted trees* (Labelle 1981) is recursively characterized by the following combinatorial equation (i.e. natural isomorphism between species):

$$A_R = X \cdot R(A_R). \tag{6}$$

Depending on the choice of "enriching species" R, this definition includes : *ordinary rooted trees* ($R = E$), *cyclic rooted trees* ($R = 1 + C$), *binary rooted trees* ($R = 1 + E_2$), *plane rooted trees* ($R = L$), *oriented rooted trees* ($R = E^2$), and *permutation rooted trees* ($R = S$).

A variant to the notion of R-enriched rooted tree is that of *R-enriched tree*. It is a tree in which the set of "immediate neighbours" of each node is equipped with an R-structure. The species of R-enriched rooted trees is denoted by $\mathcal{A}_R$.

LEMMA 1 (LABELLE 1981). *The species $\mathcal{A}_R^\bullet = X\frac{d\mathcal{A}_R}{dX}$ of pointed R-enriched trees satisfies*

$$\mathcal{A}_R^\bullet = XR(A_{R'}),$$

where $R' = \frac{dR}{dX}$ and $A_{R'} = XR'(A_{R'})$ is the species of R'-enriched rooted trees.

LEMMA 2. *The species $\mathcal{A}_R$ of R-enriched trees and the species $A_{R'}$ of R'-enriched rooted trees are related by the combinatorial equation*

$$\mathcal{A}_R + A_{R'}^2 = XR(A_{R'}) + E_2(A_{R'}). \tag{7}$$

THEOREM 1. *From equations (6) and (7) we obtain the following ten formulas:*

$$A_R(x) = xR(A_R(x)), \tag{8}$$

$$\widetilde{A_R(x)} = xZ_R(\widetilde{A_R}(x), \widetilde{A_R}(x^2), \widetilde{A_R}(x^3), \dots), \quad Z_{A_R} = x_1 Z_R(Z_{A_R}), \tag{9}$$

$$\overline{A_R(x)} = x\Gamma_R(\overline{A_R}(x), \overline{A_R}(x^2), \overline{A_R}(x^3), \dots), \quad \Gamma_{A_R} = x_1 \Gamma_R(\Gamma_{A_R}), \tag{10}$$

$$\mathcal{A}_R(x) = xR(A_{R'}(x)) - \frac{1}{2}(A_{R'}(x))^2, \tag{11}$$

$$\widetilde{\mathcal{A}_R}(x) = xZ_R(\widetilde{A_{R'}}(x), \widetilde{A_{R'}}(x^2), \widetilde{A_{R'}}(x^3), \dots) - \frac{1}{2}(\widetilde{A_{R'}}(x))^2 + \frac{1}{2}\widetilde{A_{R'}}(x^2), \tag{12}$$

$$\overline{\mathcal{A}_R}(x) = x\Gamma_R(\overline{A_{R'}}(x), \overline{A_{R'}}(x^2), \overline{A_{R'}}(x^3), \dots) - \frac{1}{2}(\overline{A_{R'}}(x))^2 - \frac{1}{2}\overline{A_{R'}}(x^2), \tag{13}$$

$$Z_{\mathcal{A}_R} = x_1 Z_R(Z_{A_{R'}}) - \frac{1}{2}(Z_{A_{R'}})^2 + \frac{1}{2}(Z_{A_{R'}})_2, \Gamma_{\mathcal{A}_R} = x_1\Gamma_R(\Gamma_{A_{R'}}) - \frac{1}{2}(\Gamma_{A_{R'}})^2 - \frac{1}{2}(\Gamma_{A_{R'}})_2. \tag{14}$$

THEOREM 2. *Let A_R be the species of R-enriched rooted trees. Then, for every partition $\sigma = (\sigma_1, \sigma_2, \dots)$ and every species F,*

$$\operatorname{coeff}_\sigma Z_{A_R} = \operatorname{coeff}_\sigma x_1 \prod_{k\geq 1}\left(1 - \frac{x_1 \partial Z_R/\partial x_1}{Z_R}\right)_k (Z_R)_k^{\sigma_k}, \tag{15}$$

$$\operatorname{coeff}_\sigma Z_{F(A_R)} = \operatorname{coeff}_\sigma Z_F \cdot \prod_{k\geq 1}\left(1 - \frac{x_1 \partial Z_R/\partial x_1}{Z_R}\right)_k (Z_R)_k^{\sigma_k}, \tag{16}$$

$$\operatorname{coeff}_\sigma \Gamma_{A_R} = \operatorname{coeff}_\sigma x_1 \prod_{k\geq 1}\left(1 - \frac{x_1 \partial \Gamma_R/\partial x_1}{\Gamma_R}\right)_k (\Gamma_R)_k^{\sigma_k}, \tag{17}$$

$$\operatorname{coeff}_\sigma \Gamma_{F(A_R)} = \operatorname{coeff}_\sigma \Gamma_F \cdot \prod_{k\geq 1}\left(1 - \frac{x_1 \partial \Gamma_R/\partial x_1}{\Gamma_R}\right)_k (\Gamma_R)_k^{\sigma_k}. \tag{18}$$

THEOREM 3. *Let $\mathcal{A}_R$ be the species of R-enriched trees. Then, for every partition $\sigma = (\sigma_1, \dots)$,*

$$\operatorname{coeff}_\sigma Z_{\mathcal{A}_R} = \begin{cases} \omega_{\sigma_1 - 1, \sigma_2, \sigma_3, \dots} & \text{if } \sigma_1 \neq 0, \\ 2^{(\sum \sigma_{2k}) - 1} b_{\sigma_2, \sigma_4, \dots} & \text{if } 0 = \sigma_1 = \sigma_3 = \cdots, \\ 0 & \text{otherwise,} \end{cases} \tag{19}$$

$$\operatorname{coeff}_\sigma \Gamma_{\mathcal{A}_R} = \begin{cases} \omega^\star_{\sigma_1 - 1, \sigma_2, \sigma_3, \dots} & \text{if } \sigma_1 \neq 0, \\ 2^{(\sum \sigma_{2k}) - 1} b^\star_{\sigma_2, \sigma_4, \dots} & \text{if } 0 = \sigma_1 = \sigma_3 = \cdots, \\ 0 & \text{otherwise,} \end{cases} \tag{20}$$

where

$$\omega_\sigma = \mathrm{coeff}_\sigma\, Z_R \cdot \prod_{k\geq 1} \left(1 - \frac{x_1 \partial^2 Z_R/\partial x_1^2}{\partial Z_R/\partial x_1}\right)_k (\partial Z_R/\partial x_1)_k^{\sigma_k},$$

$$b_\sigma = \mathrm{coeff}_\sigma\, x_1 \prod_{k\geq 1} \left(1 - \frac{x_1 \partial^2 Z_R/\partial x_1^2}{\partial Z_R/\partial x_1}\right)_k (\partial Z_R/\partial x_1)_k^{\sigma_k},$$

$$\omega^\star_\sigma = \mathrm{coeff}_\sigma\, \Gamma_R \cdot \prod_{k\geq 1} \left(1 - \frac{x_1 \partial^2 \Gamma_R/\partial x_1^2}{\partial \Gamma_R/\partial x_1}\right)_k (\partial \Gamma_R/\partial x_1)_k^{\sigma_k}$$

$$b^\star_\sigma = \mathrm{coeff}_\sigma\, x_1 \prod_{k\geq 1} \left(1 - \frac{x_1 \partial^2 \Gamma_R/\partial x_1^2}{\partial \Gamma_R/\partial x_1}\right)_k (\partial \Gamma_R/\partial x_1)_k^{\sigma_k}.$$

4. Examples

Every formula developed above can be implemented on symbolic computation systems such as MAPLE, MATHEMATICA, MACSYMA, or DARWIN (Bergeron 1988). Examples of computation are given in [7]. In the sequence, this paragraph contains concrete applications of some of our results for particular choices of the enriching species R.

($\mathbf{R} = \mathbf{1} + \mathbf{C}$).

\# of types of planes trees on n vertices =

$$\frac{1}{2(n-1)} \sum_{d|(n-1)} \phi\left(\frac{n-1}{d}\right) \binom{2d}{d} - \frac{1}{2} c_{n-1} + \frac{1}{2} \chi_{\mathrm{even}}(n) c_{(n/2)-1},$$

\# of types of asymmetric planes trees on n vertices =

$$\frac{1}{2(n-1)} \sum_{d|(n-1)} \mu\left(\frac{n-1}{d}\right) \binom{2d}{d} - \frac{1}{2} c_{n-1} - \frac{1}{2} \chi_{\mathrm{even}}(n) c_{(n/2)-1},$$

where χ_{even} is the characteristic function of the set of even numbers, $\phi(n)$ and $\mu(n)$ respectively denote the classical Euler and Möbius functions of n, and $c_n = \frac{1}{n+1}\binom{2n}{n}$ are the usual Catalan numbers.

($\mathbf{R} = \mathbf{E}$). In the case $A_R = A_E = A$ (the species of rooted trees), (15) and (17) can be rewritten as

$$\mathrm{coeff}_\sigma\, Z_A = \begin{cases} 0 & \text{if } \sigma_1 = 0, \\ \sigma_1^{\sigma_1 - 1} \prod_{k\geq 2} (\phi_k^{\sigma_k} - k\sigma_k \phi_k^{\sigma_k - 1}) & \text{otherwise,} \end{cases}$$

$$\mathrm{coeff}_\sigma\, \Gamma_A = \begin{cases} 0 & \text{if } \sigma_1 = 0, \\ \sigma_1^{\sigma_1 - 1} \prod_{k\geq 2} (\theta_k^{\sigma_k} - k\sigma_k \theta_k^{\sigma_k - 1}) & \text{otherwise,} \end{cases}$$

where $\phi_k = \sum_{d|k} d\sigma_d$ and $\theta_k = \sum_{d|k} (-1)^{(k/d)-1} d\sigma_d$.

In the case $\mathcal{A}_R = \mathcal{A}_E = \mathcal{A}$ (the species of trees), (19) and (20) can be rewritten as

$$\operatorname{coeff}_\sigma Z_{\mathcal{A}_R} = \begin{cases} a_\sigma/\sigma_1 & \text{if } \sigma_1 \neq 0, \\ 2^{(\sum \sigma_{2k})-1} a_{\sigma_2,\sigma_4,\ldots} & \text{if } 0 = \sigma_1 = \sigma_3 = \cdots, \\ 0 & \text{otherwise,} \end{cases}$$

$$\operatorname{coeff}_\sigma \Gamma_{\mathcal{A}_R} = \begin{cases} a^\star_\sigma/\sigma_1 & \text{if } \sigma_1 \neq 0, \\ 2^{(\sum \sigma_{2k})-1} a^\star_{\sigma_2,\sigma_4,\ldots} & \text{if } 0 = \sigma_1 = \sigma_3 = \cdots, \\ 0 & \text{otherwise,} \end{cases}$$

where $a_\sigma = \operatorname{coeff}_\sigma Z_A$ and $a^\star_\sigma = \operatorname{coeff}_\sigma \Gamma_A$.

For a direct application of (16) and (18), consider the species of *endofunctions* $End = S(A)$, where S is the species of permutations. Taking $F = S$ and $R = E$ in (16) and (18), a few computations give

$$\operatorname{coeff}_\sigma Z_{End} = \sigma_1^{\sigma_1} \prod_{k\geq 2} (\phi_k^{\sigma_k} - k\sigma_k \phi_k^{\sigma_k - 1})$$

$$\operatorname{coeff}_\sigma \Gamma_{End} = \sigma_1^{\sigma_1}(\theta_2^{\sigma_2} - 4\sigma_2\theta_2^{\sigma_2-1} + 4\sigma_2(\sigma_2-1)\theta_2^{\sigma_2-2}) \prod_{k\geq 3} (\theta_k^{\sigma_k} - k\sigma_k\theta_k^{\sigma_k-1}),$$

where $\phi_k = \sum_{d|k} d\sigma_d$ and $\theta_k = \sum_{d|k} (-1)^{(k/d)-1} d\sigma_d$.

($\mathbf{R} = \mathbf{S}$). The A_S-structures are called *permutation rooted trees*. In this case, formula (10) takes the very compact form

$$\overline{A_S}(x) = \sum_{n\geq 0} \bar{a}_n x^n = x \frac{1 - \overline{A_S}(x^2)}{1 - \overline{A_S}(x)},$$

where $\bar{a}_0 = 0$, $\bar{a}_1 = 1$, and $\bar{a}_{n+1} = (\bar{a}_1\bar{a}_n + \bar{a}_2\bar{a}_{n-1} + \cdots + \bar{a}_n\bar{a}_1) - \chi_{\text{even}}(n)\bar{a}_{n/2}$.

($\mathbf{R} = \mathbf{E} - \mathbf{E}_2$). A *topological tree* (also called *homeomorphically irreducible tree*) is a tree that has no node of degree 2. The species $\mathcal{A}_{top}$ of topological trees can be expressed in terms of the species $\mathcal{A}$ and A through the combinatorial equation

$$\mathcal{A}_{top} = \mathcal{A}\left(\frac{X}{1+X}\right) + XA\left(\frac{X}{1+X}\right) - XE_2\left(A\left(\frac{X}{1+X}\right)\right).$$

This equation gives the formulas

$$\begin{aligned} \widetilde{\mathcal{A}_{top}}(x) &= Z_{\mathcal{A}}\left(\frac{x}{1+x}, \frac{x^2}{1+x^2}, \ldots\right) + xZ_A\left(\frac{x}{1+x}, \frac{x^2}{1+x^2}, \ldots\right) \\ &\quad - \frac{x}{2}Z_A^2\left(\frac{x}{1+x}, \frac{x^2}{1+x^2}, \ldots\right) - \frac{x}{2}Z_A\left(\frac{x^2}{1+x^2}, \frac{x^4}{1+x^4}, \ldots\right), \\ \overline{\mathcal{A}_{top}}(x) &= \Gamma_{\mathcal{A}}\left(\frac{x}{1+x}, \frac{x^2}{1+x^2}, \ldots\right) + x\Gamma_A\left(\frac{x}{1+x}, \frac{x^2}{1+x^2}, \ldots\right) \\ &\quad - \frac{x}{2}\Gamma_A^2\left(\frac{x}{1+x}, \frac{x^2}{1+x^2}, \ldots\right) + \frac{x}{2}\Gamma_A\left(\frac{x^2}{1+x^2}, \frac{x^4}{1+x^4}, \ldots\right). \end{aligned}$$

5. Related topics

THEOREM 4. *The number of types of rooted plane trees with degree distribution* $\vec{\imath} = (i_1, i_2, i_3, \ldots)$ *is*

$$\frac{1}{n-1} \sum_{p \in supp\ \vec{\imath}} \quad \sum_{d \mid p, \vec{\imath} - \vec{1}_p} \phi(d) \binom{(n-1)/d}{i_1/d, i_2/d, \ldots, (i_p - 1)/d, \ldots},$$

where $supp\ \vec{\imath} = \{p \mid i_p \neq 0\}$, $d \mid \vec{\imath}$ *iff* $\forall p \ : \ d \mid i_p$, *and* $\vec{\imath} - \vec{1}_p = (i_1, i_2, \ldots, i_p - 1, \ldots)$.

THEOREM 5. *The number of types of bicoloured plane trees with degree distributions* $\vec{\imath} = (i_1, i_2, i_3, \ldots)$ *and* $\vec{\jmath} = (j_1, j_2, j_3, \ldots)$ *is*

$$\begin{aligned}
&\frac{1}{n} \sum_{p \in supp\ \vec{\jmath}} \quad \sum_{d \mid p, \vec{\imath}, \vec{\jmath} - \vec{1}_p} \phi(d) \binom{n/d}{i_1/d, i_2/d, \ldots} \binom{(m-1)/d}{j_1/d, j_2/d, \ldots, (j_p - 1)/d, \ldots} \\
&\quad + \frac{1}{m} \sum_{p \in supp\ \vec{\imath}} \quad \sum_{d \mid p, \vec{\imath} - \vec{1}_p, \vec{\jmath}} \phi(d) \binom{(n-1)/d}{i_1/d, i_2/d, \ldots, (i_p - 1)/d, \ldots} \binom{m/d}{j_1/d, j_2/d, \ldots} \\
&\quad - \frac{n+m-1}{nm} \binom{n}{i_1, i_2, \ldots} \binom{m}{j_1, j_2, \ldots},
\end{aligned}$$

where $supp\ \vec{\imath} = \{p \mid i_p \neq 0\}$, $d \mid \vec{\imath}$ *iff* $\forall p \ : \ d \mid i_p$, *and* $\vec{\imath} - \vec{1}_p = (i_1, i_2, \ldots, i_p - 1, \ldots)$.

Let $B = B(X, Y)$ be the species of rooted trees with internal point of sort X and leaves of sort Y. This species is characterized by the functional equation

$$B = Y + X \cdot E^{\star}(B)$$

where $E^{\star} = E - 1$ stands for species characteristic of nonempty sets.

THEOREM 6. *The species* $A = A(X)$ *and* $B = B(X, Y)$ *are related by the following combinatorial equation*

$$B = Y - X + A(X \cdot E(Y - X))$$

where $E = E(X)$ *is the species of sets.*

Let $\mathcal{B} = \mathcal{B}(X, Y)$ be the species of trees with internal point of sort X and leaves of sort Y.

THEOREM 7. *The species* $\mathcal{A} = \mathcal{A}(X)$ *and* $\mathcal{B} = \mathcal{B}(X, Y)$ *are related by the following combinatorial equation*

$$\mathcal{B} = (Y - X) + E_2(Y - X) + \mathcal{A}(X \cdot E(Y - X))$$

where $E = E(X)$ *is the species of sets and* $E_2 = E_2(X)$ *is the species of sets of cardinality two.*

THEOREM 8. *Let* U *be an* n*-set,* σ *be a permutation of* U *whose cyclic type is* $(\sigma_1, \sigma_2, \ldots, \sigma_n)$. *Then, for* $n \geq 2$, *the expected number of leaves in a random rooted tree (resp. in a random tree) on* U *of which* σ *is an automorphism is given respectively by*

$$\frac{1}{a_\sigma} \sum_{k=1}^{n} k\sigma_k \left(\sum_{d \mid k} d\sigma_d - k \right) \cdot a_{(\sigma_1, \ldots, \sigma_k - 1, \ldots, \sigma_n)}$$

$$\frac{1}{\alpha_\sigma} \sum_{k=1}^{n} k\sigma_k \left(\sum_{d \mid k} d\sigma_d - k \right) \cdot \alpha_{(\sigma_1, \ldots, \sigma_k - 1, \ldots, \sigma_n)}$$

where a_σ (resp. α_σ) is the number of rooted trees (resp. trees) of which σ is an automorphism.

EXAMPLE. The expected number of leaves in a random rooted tree with σ as automorphism is

(1) $n(n-1)^{n-1}/n^{n-1} \sim n/e$ if $\sigma = \mathrm{Id}_n$ (well known),

(2) $\frac{(n-3)^{n-2}}{(n-2)^{n-3}} + 2$ if σ is of type $(n-2, 1, 0, \ldots, 0)$,

(3) 97.89276140 if $n = 186$ and σ is of type $(6, 1, 12, 0, 0, 0, 4, 3, 2, 0, 0, 6)$ (example given after a few seconds, using Maple on a personal computer).

Bibliography

[1] Bergeron (F.), Labelle (G.), and Leroux (P.). – Computation of the expected number of leaves in a tree having a given automorphism. In *Proceedings of the Capital City Conference on Combinatorics and Theoretical Computer Science, Discrete Mathematics*. – 1989.

[2] Bergeron (François). – Une combinatoire du pléthysme. *Journal of Combinatorial Theory, Series A*, vol. 46, 1987, pp. 291–305.

[3] Harary (F.) and Prins (G.). – The number of homeomorphically irreducible trees and other species. *Acta Mathematica*, vol. 101, 1959, pp. 141–162.

[4] Harary (Frank) and Palmer (Edgar M.). – *Graphical Enumeration*. – Academic Press, 1973.

[5] Joyal (André). – Une théorie combinatoire des séries formelles. *Advances in Mathematics*, vol. 42, n° 1, 1981, pp. 1–82.

[6] Labelle (Gilbert). – On the generalized iterates of Yeh's combinatorial K-species. *Journal of Combinatorial Theory, Series A*, vol. 50, 1989, pp. 235–258.

[7] Labelle (Gilbert). – Counting asymmetric enriched trees. *Journal of Symbolic Computation*, vol. 14, 1992, pp. 211–242.

[8] Labelle (Gilbert). – On asymmetric structures. *Discrete Mathematics*, vol. 99, 1992, pp. 141–164.

[9] Labelle (Gilbert). – Sur la symétrie et l'asymétrie des structures combinatoires. *Theoretical Computer Science*, vol. 117, 1993, pp. 3–22.

[10] Leroux (P.) and Miloudi (B.). – Généralisation de la formule d'Otter. *Annales des Sciences Mathématiques du Québec*, vol. 16, 1992, pp. 53–80.

[11] Macdonald (I. G.). – *Symmetric Functions and Hall Polynomials*. – Clarendond Press, Oxford, 1979.

[12] Otter (Richard). – The number of trees. *Annals of Mathematics*, vol. 49, n° 3, 1948, pp. 583–599.

[13] Pólya (G.). – Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen. *Acta Mathematica*, vol. 68, 1937, pp. 145–254.

[14] Robinson (R. W.). – Enumeration of nonseparable graphs. *Journal of Combinatorial Theory, Series B*, vol. 9, 1970, pp. 327–356.

[15] Yeh (Y. N.). – The calculus of virtual species and K-species. In Labelle (G.) and Leroux (P.) (editors), *Combinatoire énumérative. Lecture Notes in Computer Science*, pp. 351–369. – Springer-Verlag, 1985.

A class of formal power series helps enumerate Young paths

François Bergeron
LACIM, UQAM, Montréal

April 5, 1993

[summary by Dominique Gouyou-Beauchamps]

Abstract

We study different aspects of the enumeration of standard paths in the poset of compositions of integers. We show that many problems similar to those considered in the poset of partitions of an integer become simpler in this context. We give many explicit formulas for generating functions of standard paths in this poset and interesting subposets.

1. Standard Young Tableaux and Paths in the Young Lattice

A *partition* of a positive integer n is a sequence of integers $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k > 0$ such that $\sum_i \lambda_i = n$. We write $\lambda \vdash n$ to express this fact, and we say that k is the *height* $h(\lambda)$ of λ. The Ferrer diagram of a partition is the set of points $(i,j) \in \mathbb{Z}^2$ such that $1 \leq j < \lambda_i$.

A Young standard tableau T is an injective labelling of a Ferrer diagram by the elements of $\{1, 2, \ldots, n\}$, such that $T(i,j) < T(i+1,j)$, for $1 \leq i < k$, and $T(i,j) < T(i,j+1)$, for $1 \leq j < \lambda_i$. We further say that λ is the *shape* of the tableau T. For a given λ, the number f_λ of tableaux of shape λ is given by the *hook length formula*

$$f_\lambda = \frac{n!}{\prod_c h_c},$$

where $c = c(i,j)$ runs over the set of points in the diagram of λ, and

$$h_c = \lambda_i + \#\{j \mid \lambda_j \geq i\} - i - j + 1.$$

Other classical results in this context are $\sum_{\lambda \vdash n} f_\lambda^2 = n!$, and $\sum_{\lambda \vdash n} f_\lambda =$ coeff of $\frac{x^n}{n!}$ in $e^{x+x^2/2}$.

We are interested in the enumeration of tableaux of height bounded by some integer h. In other words, we want to compute the numbers

$$t_h(n) = \sum_{h(\lambda) \leq h} f_\lambda,$$

and the series

$$y_h(x) = \sum_{n \geq 0} t_h(n) x^n.$$

Closed formulas for $t_h(n)$ are known for $n \leq 5$. Regev [6] has given asymptotic values for these numbers. The series $y_h(x)$ are differentiably finite (see Stanley [7]) (i.e. the $t_h(n)$'s are P-recursive). This means that the $t_h(n)$'s satisfy a recurrence of the form

$$\sum_{k=0}^{m} p_k(n) t_h(n-k) = 0,$$

for some polynomials $p_k(n)$ and some integer m.

Conjecture 1. [1]

(1) *the $t_h(n)$'s satisfy a recurrence of the form*

$$\sum_{k=0}^{\lfloor h/2\rfloor+1} p_k(n)t_h(n-k) = 0, \tag{1}$$

for some polynomials $p_k(n)$ each of degree $\leq \lfloor h/2\rfloor$,

(2) *the coefficient of $t_h(n)$ in (1) is*

$$p_0(n) = \prod_{k=1}^{\lfloor h/2\rfloor} (n + k(h-k)),$$

(3) *for odd h, the coefficient of $t_h(n-1)$ in (1) is*

$$-p_1(n) = np_0(n) - (n-1)p_0(n-1),$$

(4) *for $h = 7$ we have*

$$\begin{aligned}(n+6)(n+10)(n+12)t_7(n) =& (4n^3+78n^2+424n+495)t_7(n-1)\\ &+(n-1)(34n^2+280n+305)t_7(n-2)\\ &-(n-1)(n-2)(76n+290)t_7(n-3)\\ &-105(n-1)(n-2)(n-3)t_7(n-4).\end{aligned}$$

2. Compositions of n

Let us recall that a *composition* P is a sequence of positive integers $(p_i)_{i=1,\ldots,k}$. The p_i's are called *parts* of the composition and k, the number of parts, is said to be the *length* $\ell(P)$ of P and is denoted by $\ell(P)$. The *weight* $|P|$ of a composition P is the sum of its parts

$$|P| = \sum_{i=1}^{k} p_i = n.$$

We often say that P is a composition of n and write $P \models n$. The partition obtained by reordering the parts of a composition P is denoted $\lambda(P)$.

We say that a composition Q covers a composition P, if Q is obtained either by adding 1 to a part of P, or by adding a part of size 1 to P. The partial order obtained by transitive closure of this covering relation is denoted

$$P \prec R,$$

and the poset thus obtained is denoted Γ. For partitions, the analogous order corresponds to the inclusion of Ferrer diagrams. The poset of partitions is denoted Λ and the function $\lambda : \Gamma \longrightarrow \Lambda$, defined above, is a morphism of (graded) posets.

Our first objective will be the enumeration, with some parameters, of "standard" (up-going) paths starting with the composition (1) and finishing at $P \models n$. We also consider this enumeration problem for subposets obtained by restrictions on the compositions. More precisely, a *standard path* is a sequence of compositions

$$(1) = P_1 \prec P_2 \prec P_3 \prec \cdots \prec P_n = P,$$

where $P_i \models i$. Such a path P is said to have *length* n, and we denote it $|\mathcal{P}|$. A standard path $\mathcal{P} = P_1 \prec P_2 \prec P_3 \prec \cdots \prec P_n$ with endpoint P can be encoded by a permutation $\sigma(\mathcal{P})$ in the following way. We form a sequence of words

$$(1) = \omega_1, \omega_2, \ldots, \omega_n = \sigma(\mathcal{P})$$

where ω_i is obtained from ω_{i-1} by insertion of i in position $j = p_1^{(i)} + p_2^{(i)} + \cdots + p_k^{(i)}$ if P_i is obtained from P_{i-1} by adding 1 to the k-th part of P_{i-1}, in position $j = p_1^{(i)} + p_2^{(i)} + \cdots + p_k^{(i)} - 1$ if P_i is obtained by

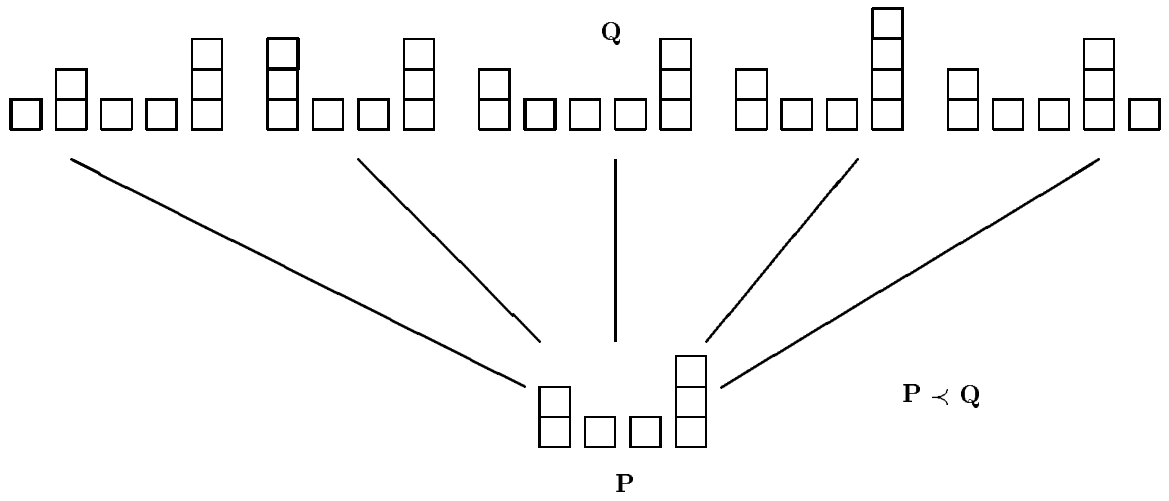


FIGURE 1

adding a part of size 1 to P_{i-1}, just after a part of size > 1, and in first position if the new part is added at the beginning of P_{i-1}.

For example, to the path

$$\mathcal{P} = (1) \prec (1,1) \prec (2,1) \prec (1,2,1) \prec (2,2,1) \prec (2,3,1) \prec (2,4,1) \prec (2,4,2) \prec (2,4,1,2)$$

there corresponds the sequence of words

$$1, 21, 231, 4231, 45231, 452361, 4523671, 45236718, 452369718$$

hence $\sigma(\mathcal{P}) = 452369718$.

Let us denote $P(\omega)$ the composition encoding the descents of a permutation ω

$$P(\omega) = (p_1, p_2, \ldots, p_k).$$

This means that the set $\{i \mid \omega_i > \omega_{i+1}\}$ coincides with the set $\{p_1, p_1 + p_2, p_1 + p_2 + p_3, \ldots\}$. Then

$$P(\sigma(\mathcal{P})) = \mathcal{P}, \qquad \text{and} \qquad \sigma(P(\omega)) = \omega,$$

if $\omega = \sigma(\mathcal{P})$ for some standard path $\mathcal{P}$. In order to unfold our study, we will also need the following alternative encoding of a standard path. First, we may formally define the *diagram* of a composition P to be the set of points $(i, j) \in \mathbb{Z}^2$ such that $1 \leq j \leq p_i$. It is convenient to replace the node (i, j) by the square with corners $(i-1, j-1)$, $(i-1, j)$, $(i, j-1)$ and (i, j). For a standard path ending at P, we label the squares of the diagram of P in the order of their apparition in the path. Thus the step

$$(2,3,1,5) \prec (2,4,1,5)$$

is encoded by the addition of the box labelled 12 in Figure 3.

The labelled diagram obtained in this manner is called the *tableau* of the path, and the underlying diagram (or composition) of a tableau is called its *shape*. This representation suggests that the number of parts of the endpoint P of a standard path $\mathcal{P}$ should be called the *width* of the path, the largest part the *height* of the path, and P the *shape* of the path.

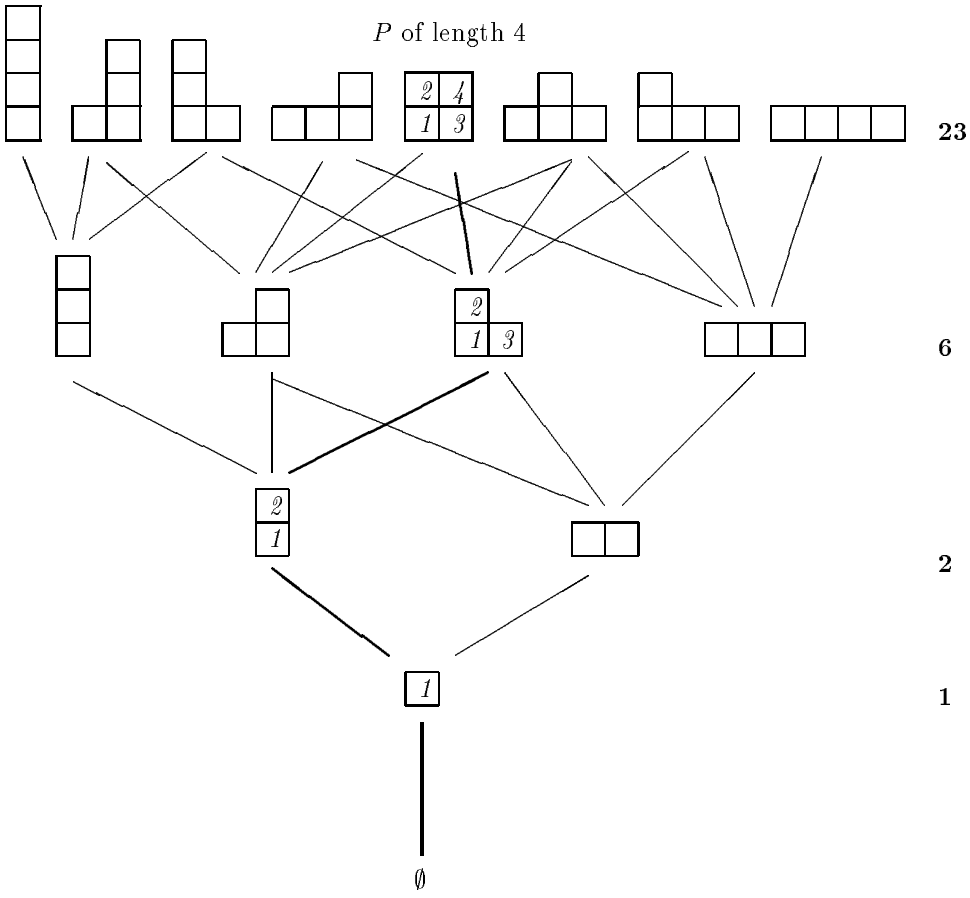


FIGURE 2

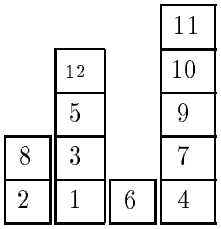


FIGURE 3.

3. Standard paths in the poset Γ

Let $\Gamma_{n,k,d}$ be the set of compositions of length n with k parts of size 1 and d parts of size > 1. Let $\gamma_{n,k,d}$ be the number of standard paths with endpoint in $\Gamma_{n,k,d}$. We would like to derive an explicit expression for the generating function

$$F(u,v,x) = \sum_{n\geq 1} \left(\sum_{k,j} \gamma_{n,k,d} u^k v^d \right) \frac{x^n}{n!}.$$

Examination of the different cases involved in the last step of a standard path gives the following recurrence

$$\gamma_{n+1,k,d} = d\gamma_{n,k,d} + (1+d)\gamma_{n,k-1,d} + (1+k)\gamma_{n,k+1,d-1},$$

with initial conditions $\gamma_{n,n,0} = 1$ and $\gamma_{n,0,1} = 1$, for $n \geq 2$. This recurrence translates into a partial differential equation for F

$$\frac{\partial}{\partial x}F(u,v,x) = (1+u)v\frac{\partial}{\partial v}F(u,v,x) + uF(u,v,x) + v\frac{\partial}{\partial u}F(u,v,x), \tag{2}$$

with initial conditions $F(u,0,x) = \exp(ux)$, and $(\frac{\partial}{\partial v}F(0,v,x))\big|_{v=0} = \exp(x) - 1 - x$. It is straightforward to verify (with the help of Maple) that the following function satisfies equation (2) with the prescribed initial conditions

$$F(u,v,x) = \frac{\alpha^2}{\exp(x)\left((1+u)\sin\left(\frac{\alpha}{2}x\right) - \alpha\cos\left(\frac{\alpha}{2}x\right)\right)^2}, \tag{3}$$

where

$$\alpha = \sqrt{2\,v - (1+u)^2}.$$

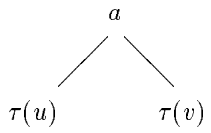
The first few terms of this series in x are

$$1 + ux + (v+u^2)\frac{x^2}{2!} + (v + 4\,vu + u^3)\frac{x^3}{3!} + (v + 4\,v^2 + 6\,vu + 11\,vu^2 + u^4)\frac{x^4}{4!}$$
$$+(v + 14\,v^2 + 34\,uv^2 + 8\,vu + 23\,u^2v + 26\,vu^3 + u^5)\frac{x^5}{5!} + \cdots.$$

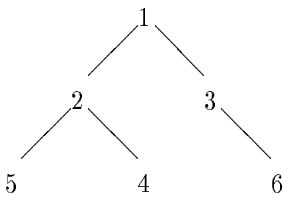
It is not clear how one can come up with an expression such as (3) for the desired generating function. The following combinatorial argument describes one way of finding this expression.

4. Increasing binary trees

First, we describe a classical bijection between permutations and *increasing binary trees*. For any word $w = w_1 w_2 \cdots w_n$ on $n \geq 1$ distinct letters (in an ordered alphabet), we recursively define the binary tree $\tau(w)$ to be

$\tau(w) =$ 

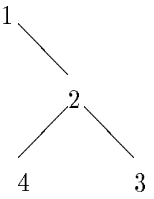
where $a = \min(w)$ is the minimum letter in w, u and v are the factors of w such that $w = uav$, $\tau(u)$ is the left branch of the tree, and $\tau(v)$ is the right branch. If one of these factors is the empty word, we omit the corresponding branch. Hence for the permutation $\omega = 521436$ the corresponding tree is

$\tau(524136) =$ 

It is clear that the labels in such a tree will be in increasing order on any path going from the root to a leaf. Since τ is a bijection, there are $n!$ increasing trees with labels $\{1, 2, \ldots, n\}$.

We can characterize the increasing trees $T = \tau(\sigma(\mathcal{P}))$ corresponding to the permutation encoding $\sigma(\mathcal{P})$ of standard paths $\mathcal{P}$ by the condition that for any node ν appearing in the left subtree of another node, when ν has two sons the label of its left son is inferior to that of the right one.

The smallest increasing tree that is excluded with this condition is



Using this characterization and the results of [5], it is easy to check that $F = F(x)$ satisfies the following system of differential equations

$$F' = F(1+G), \qquad F(0) = 1, \qquad G' = 1 + 2\,G + G^2/2, \qquad G(0) = 0. \tag{4}$$

This is how we first obtained the generating function (3) (with $u = v = 1$). A finer study of the properties of these trees allows for the generalization of (4) accounting for the parameters u and v. We obtain

$$F' = F(1+G), \qquad F(u,v,0) = 1, \qquad G' = v + (1+u)G + G^2/2, \quad G(u,v,0) = 0, \tag{5}$$

where $F'(x) = \frac{\partial}{\partial x} F(u,v,x)$.

The particular form of system (5) underlines that F is a *constructible differentially algebraic* series in the sense of [2]. Recall that a series $y = y(x)$, with coefficients in K, is said to be constructible differentially algebraic (CDF for short) if for some $k \geq 1$, there exist k series $y_1, \ldots, y_k$ with $y_1 = y$ and polynomials $P_1, \ldots, P_k$ (with coefficients in K) such that

$$\begin{aligned} y_1' &= P_1(y_1, \ldots, y_k) \\ &\vdots \\ y_k' &= P_k(y_1, \ldots, y_k) \end{aligned}$$

The class of CDF series contains polynomials, algebraic series, and the series expansion around 0 of the usual functions such as e^x, $\log(1+x)$, or the trigonometric functions and their inverse. It is closed for the usual operations on series: sum, product, composition, derivation, integration, inversion ($1/y(x)$), and inversion for composition. However it is not closed under Hadamard product (term-wise product). All CDF series are analytic around 0, hence $\sum_n n! x^n$ is not CDF which shows that this class does not contain the class of D-finite series (see [7, 8]). The series expansion around 0 of $1/\cos(x)$ is not D-finite, but is CDF. Thus the class CDF is not contained in the class of D-finite series.

5. Standard paths of bounded height

In the sequel of this paper, we denote $\Gamma_{(k)}$ the subposet of compositions of width $\leq k$, and $\Gamma^{(k)}$ the subposet of compositions of height $\leq k$.

The story is very similar for the poset $\Gamma^{(2)}$. Let, once again, $\Gamma^{(2)}_{k,d}$ be the set of compositions with k parts of size 1 and d parts of size 2. Clearly this implies that the length of the path is $n = k + 2\,d$. As before, let $\gamma^{(2)}_{k,d}$ be the number of standard paths with endpoint in $\Gamma^{(2)}_{k,d}$. The basic recurrence in this case is

$$\gamma^{(2)}_{k,d} = (1+d)\gamma^{(2)}_{k-1,d} + (1+k)\gamma^{(2)}_{k+1,d-1}. \tag{6}$$

We could proceed as in the derivation of (3) to deduce from (6) that

$$F^{(2)}(u,v) = \frac{\beta^2}{\left(u\,\sin(\frac{\beta}{2}) - \beta\,\cos(\frac{\beta}{2})\right)^2},$$

where $\beta = \sqrt{2\,v - u^2}$.

For a general k, the study of $\Gamma^{(k)}$ becomes quite intricate. We do not know at this time what are the generating functions for the enumeration of standard paths in those instances. In the case $k = 3$ the first terms of the corresponding generating function are

$$1 + x + 2\frac{x^2}{2!} + 6\frac{x^3}{3!} + 22\frac{x^4}{4!} + 98\frac{x^5}{5!} + 514\frac{x^6}{6!} + 3086\frac{x^7}{7!} + 20890\frac{x^8}{8!} + 157398\frac{x^9}{9!} + \cdots.$$

6. Standard paths of given width

The (ordinary) generating functions for the number of paths of *width* at most 2 is the rational function

$$F_{(2)}(x) = \frac{x^2 + x^3}{(1-x)(1-2\,x)}.$$

Bibliography

[1] Bergeron (François), Favreau (Luc), and Krob (Daniel). – Conjectures on the enumeration of tableaux of bounded height. – Preprint, 1992.

[2] Bergeron (François) and Reutenaeur (Christophe). – Combinatorial resolution of systems of differential equations III. A special class of differentiably algebraic series. *European Journal of Combinatorics*, vol. 11, 1990, pp. 501–512.

[3] Favreau (Luc). – *Combinatoire des tableaux oscillants et des polynômes de Bessel.* – PhD thesis, Université de Bordeaux I, 1991.

[4] Fomin (S. V.). – Generalized Robinson-Schensted-Knuth correspondence. *Soviet Mathematical Doklady*, vol. 41, 1988, pp. 979–991.

[5] Leroux (P.) and Viennot (G. X.). – Combinatorial resolution of systems of differential equations I: Ordinary differential equations. In Labelle (G.) and Leroux (P.) (editors), *Combinatoire Énumérative. Lecture Notes in Mathematics*, pp. 210–245. – Springer-Verlag, 1986.

[6] Regev (A.). – Asymptotic values for degrees associated with strips of Young diagrams. *Advances in Mathematics*, vol. 41, n° 2, 1981, pp. 115–136.

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

[8] Zeilberger (Doron). – A holonomic systems approach to special functions identities. *Journal of Computational and Applied Mathematics*, vol. 32, 1990, pp. 321–368.

Sums of independent random variables and some combinatorial problems

V. Kolchin
Steklov Mathematical Institute

September 17, 1992

[summary by Philippe Robert]

1. Introduction

Consider n independent random variables uniformly distributed on the set $\{1, 2, \ldots, N\}$ and denote by η_i the number of occurrences of i, $1 \leq i \leq N$. For any N-tuple of integers $n_1, n_2, \ldots, n_N$ such that $\sum_1^N n_i = n$, then

$$P(\eta_1 = n_1, \ldots, \eta_N = n_N) = \frac{n!}{n_1! \cdots n_N! N^n}.$$

In the language of allocation of particles into cells (or balls into urns): n particles are put at random into N cells, η_i is the number of particles in the i-th cell.

If $\xi_1, \ldots, \xi_N$ are independent Poisson random variables with parameter λ,

$$p_k = P(\xi_1 = k) = \frac{\lambda^k e^{-\lambda}}{k!}, \quad k = 0, 1, \ldots$$

it is easy to check that

$$P(\eta_1 = n_1, \ldots, \eta_N = n_N) = P(\xi_1 = n_1, \ldots, \xi_N = n_N / \xi_1 + \cdots + \xi_N = n). \tag{1}$$

Let $\mu_r(n, N)$ be the number of cells with exactly r particles and $\eta_{(N)} = \max\{\eta_1, \ldots, \eta_N\}$. If $\xi_1^{(r)}, \ldots, \xi_N^{(r)}$ are independent identically distributed (i.i.d.) random variables such that

$$P(\xi_1^{(r)} = k) = P(\xi_1 = k / \xi_1 \neq r),$$

and $\bar{\xi}_1^{(r)}, \ldots, \bar{\xi}_N^{(r)}$ i.i.d variables with

$$P(\bar{\xi}_1^{(r)} = k) = P(\xi_1 = k / \xi_1 \not\leq r),$$

then using the relation (1), one gets

$$\begin{aligned} P(\eta_{(N)} \leq r) &= (P(\xi_1 \leq r))^N \, \frac{P(\bar{\xi}_1^{(r)} + \cdots + \bar{\xi}_N^{(r)} = n)}{P(\xi_1 + \cdots + \xi_N = n)}, \\ P(\mu_r(n, N) = k) &= \binom{N}{k} p_r^k (1 - p_r)^{N-k} \frac{P(\xi_1^{(r)} + \cdots + \xi_{N-k}^{(r)} = n - kr)}{P(\xi_1 + \cdots + \xi_N = n)}. \end{aligned}$$

Definition 1. An N-tuple $\eta_1, \ldots, \eta_N$ of random variables is a generalized scheme of allocating particles if there exist random variables $\xi_1, \ldots, \xi_N$ such that (1) is satisfied.

EXAMPLE. We consider the partitions of integers n into N non-negative integer summands, $n = n_1 + \cdots + n_N$. There are $\binom{n-N+1}{N-1}$ such partitions; if they are equally likely, then $n = \eta_1 + \cdots + \eta_N$. If we take independent geometrically distributed random variables $\xi_1, \ldots, \xi_N$,

$$P(\xi_1 = k) = p^k(1-p), \qquad k \in \mathbb{N}, \quad 0 < p < 1,$$

then relation (1) is satisfied.

2. A general model of application of the generalized scheme of allocation

Let

- $\Gamma_n(R)$ be the set of all graphs with n vertices which satisfy some property R,
- $\Gamma_{n,N}(R)$ the set of the elements of $\Gamma(R)$ with N connected components,
- $\bar{\Gamma}_{n,N}(R)$ the set of objects which consists of ordered collections on N components.

Take the uniform distribution on $\bar{\Gamma}_{n,N}(R)$ and denote by $\eta_1, \ldots, \eta_N$ the sizes of the components of a random element from $\bar{\Gamma}_{n,N}(R)$. Denote by $a_n, a_{n,N}, \bar{a}_{n,N}$ the respective cardinalities of $\Gamma_n(R), \Gamma_{n,N}(R), \bar{\Gamma}_{n,N}(R)$, b_n the number of connected graphs in $\Gamma_n(R)$ and let $\xi_1, \ldots, \xi_N$ be i.i.d. random variables such that

$$P(\xi_1 = k) = \frac{b_k x^k}{k! B(x)}, \qquad k \in \mathbb{N},$$

where $B(x) = \sum_1^{+\infty} \frac{b_k x^k}{k!}$ and x is in the domain of convergence of this series. Then relation (1) is valid:

$$a_{n,N} = \frac{\bar{a}_{n,N}}{N!} = \frac{1}{N!} \sum_{n_1 + \cdots + n_N = n} \frac{n!}{n_1! \cdots n_N!} b_1 \cdots b_{n_N},$$

$$\begin{aligned} P(\xi_1 + \cdots + \xi_N = n) &= \sum_{n_1 + \cdots + n_N = n} \prod_{i=1}^{N} \frac{b_{n_i} x^{n_i}}{n_i! B(x)} \\ &= \frac{x^n}{B(x)^N} \sum_{n_1 + \cdots + n_N = n} \prod_{i=1}^{N} \frac{b_{n_i}}{n_i!}, \end{aligned}$$

hence

$$a_{n,N} = \frac{n!(B(x))^N}{N! x^n} P(\xi_1 + \cdots + \xi_N = n). \tag{2}$$

EXAMPLE. 1) Random permutations from S_n.

$$a_n = n!, \quad b_n = (n-1)!,$$

$$P(\xi_1 = k) = \frac{-x^k}{k \log(1-x)}, \qquad k \in \mathbb{N}, \quad 0 < x < 1.$$

2) Random mappings from Σ_n.

$$a_n = n^n, \quad b_n = (n-1)! \sum_{k=0}^{n-1} \frac{n^k}{k!},$$

$$P(\xi_1 = k) = \frac{b_k x^k}{k! B(x)}, \qquad 0 < x < 1.$$

3) Random partitions from the set unordered partitions of the set $\{1, \ldots, n\}$.

$$b_n = 1,$$

$$a_n = \sum_{N=1}^{n} a_{n,N} = \sum_{N=1}^{n} \frac{n!}{N!} \sum_{n_1+\cdots+n_N=n} \frac{1}{n_1!\cdots n_N!},$$

$$P(\xi_1 = k) = \frac{x^k}{k!(e^x - 1)}, \qquad k \in \mathbb{N}, \quad 0 < x < +\infty.$$

4) Random forest from the set of all forests of N non-rooted trees with n total number of vertices.

$$b_n = n^{n-2}, \quad B(x) = \sum_{1}^{+\infty} \frac{n^{n-2}x^n}{n!}, \qquad 0 < x < e^{-1},$$

$$P(\xi_1 = k) = \frac{k^{k-2}x^k}{k!B(x)}, \qquad k \in \mathbb{N}.$$

The complete investigation of $a_{n,N}$ was carried out by Britikov in 1990,

$$E(\xi_1) = \frac{1}{B(x)} \sum_{1}^{+\infty} \frac{k^{k-1}x^k}{k!} = \frac{\theta(x)}{B(x)},$$

$$\sigma^2 E(\xi_1^2) = \frac{1}{B(x)} \sum_{1}^{+\infty} \frac{k^k x^k}{k!} = \frac{A(x)}{B(x)},$$

where

$$A(x) = \frac{\theta(x)}{1-\theta(x)}, \quad B(x) = \frac{1}{2}(1-(1-\theta(x))^2)$$

and $\theta(x)$ is the root of $x = \theta e^{-\theta}$ in the interval $[0,1]$.

As a consequence of the local central limit theorem (see [1] p. 233),

$$P(\xi_1 + \cdots + \xi_N = k) = \frac{1}{\sigma\sqrt{2\pi N}} e^{-u^2/2}(1 + o(1)),$$

uniformly on the integers k such that $u = \frac{(k - NE(\xi_1))}{\sigma\sqrt{N}}$ is in a finite interval.

The number of edges in the forest is $T = n - N$, if $\theta = \frac{2T}{n}$, then $E(\xi_1) = \frac{n}{N}$,

$$P(\xi_1 + \cdots + \xi_N = n) = \frac{1}{\sigma\sqrt{2\pi N}}(1 + o(1)).$$

Finally if $n, N \to +\infty$ such that $\theta = \frac{2T}{n}$ is constant, then using (2) one gets

$$a_{n,T} = \frac{n^{2T}\sqrt{1-\theta}}{2^T T!}(1 + o(1))$$

Bibliography

[1] Gnedenko (B. V.), Kolmogorov (A. N.), and Chung (K. L.). – *Limit Distributions for Sums of Independent Random Variables.* – Addison-Wesley, 1968.

Branching processes, random trees and Brownian excursion

Vladimir Vatutin
Steklov Mathematical Institute (Moscow)

September 17, 1992

[summary by Guy Louchard]

Abstract

Using bijections between genealogical trees arising from branching processes, plane trees and classical random walks, one can derive asymptotic distributions of random variables such as tree height, distances related to the nearest mutual ancestor and labelled trees properties.

1. A few definitions

– $\mathcal{K}_N :=$ the set of all plane trees K with $N+1$ vertices

$$|\mathcal{K}_N| = \frac{1}{N+1}\binom{2N}{N} \qquad \text{(Catalan number)}$$

– Let $A \subset \{0,1,\dots\}$,

$$\mathcal{K}_N^{(A)} := \{K \in \mathcal{K}_N\text{: the degree of any non-rooted vertex of K belongs to } A\}.$$

– $\mathcal{F}_N :=$ the set of all rooted labelled trees with N non-rooted vertices

$$|\mathcal{F}_N| = (N+1)^{N-1}.$$

To any plane tree $K \in \mathcal{K}_{N+1}$ having m_r vertices of degree r, there corresponds $\frac{N!}{\prod_r (r!)^{m_r}}$ rooted labelled trees, with

$$\begin{cases} m_1 + 2m_2 + \cdots + Nm_N = N, \\ m_0 + m_1 + \cdots + m_N = N+1. \end{cases}$$

2. Branching processes

Let $f(s)$ be the generating function of the number ξ of direct descendants of an individual in a Galton-Watson branching process: $f(s) := \sum_k P(\xi = k)s^k$ and let $Z(n)$ be the number of individuals at time n.

There is an obvious bijection δ between any genealogical tree G and the corresponding plane tree K.

If Ω_G is the set of all genealogical trees, $f(s)$ generates a probability measure on the set of subsets of Ω_G and also a corresponding measure on the set of subsets of Ω_K (the set of all plane trees). If $\nu(G)$ is the total number of individuals in G then

$$P[G = G_N | \nu(G) = N] = \frac{p_0^{m_0} \cdots p_{N-1}^{m_{N-1}}}{P[\nu(G) = N]} \tag{1}$$

and by the bijection δ, this is equivalent to $P_\delta[K = K_N | K \in \mathcal{K}_N]$.

A few particular cases of $f(s)$ are given by:

– $f_1(s) = \frac{1}{2-s}$. Then (1) gives $\frac{1}{|\mathcal{K}_N|}$.

– $f_2(s) = \sum_{k\in A} c\alpha^k s^k$ with $f(1) = 1$, $f'(1) = 1$. Then (1) leads to

$$P_\delta[K = K_n | K \in \mathcal{K}_N^{(A)}] = \frac{1}{|\mathcal{K}_N^{(A)}|}.$$

– $f_3(s) = e^{s-1}$. Then (1) leads to

$$\frac{N!}{\prod_r (r!)^{m_r}} \frac{1}{(N+1)^{N-1}}. \tag{2}$$

3. Labelled trees

If $T_N \in \mathcal{F}_N$, set $\gamma :=$ the operation of removing labels and adding a root, so $K_{N+1} = \gamma(T_N) \in \mathcal{K}_{N+1}$. One can prove that $P[T \in \mathcal{F}_N : \gamma(T) = K_{N+1}] \equiv (2)$. So one can investigate the properties of T_N which are invariant with respect to relabelling by investigating the branching process with $f(s) = f_3(s)$. The same analysis holds with $f_4(s) = \sum_{k\in A} \frac{c}{k!} s^k$ and for $\mathcal{F}_N^{(A)}$.

4. Trees height

Let $\tau(G) = \min[n : Z(n) = 0]$ (extinction time). Then the height of K, $H(K)$ is given by $H(K) = \tau[\delta^{-1}(K)]$. One can prove that, if $f'(1) = 1, 0 \le f''(1) = B$, then

$$\lim P\left[\frac{\tau}{\sqrt{N}} \ge x | \nu = N\right] = P\left[\max_{0\le t\le 1} W_0^+(t) \ge \frac{x}{2}\sqrt{B}\right] \tag{3}$$

where $W_0^+(t)$ is the standard Brownian Excursion (B.E.) on $[0, 1]$.

For example $f_1(s)$ leads to $B = 2$. If we set $n = x\sqrt{N}$, (3) gives $P[H(K) \ge n]$. An equivalent of the density can also be derived.

If one analyzes the standard random walk (R.W.) until the next return to 0, the local time at height j is equivalent in probability to the branching process $Z(j)$ with $f_1(s)$. Also f_1 leads to the Catalan statistic for plane trees and to the classical relation between asymptotic height and maximum of the B.E.

However, if $\frac{n}{\sqrt{N}} \to \infty$, with $\frac{n}{N} \le a < 1$, (3) is no longer true. It is however possible to find a function $h(n, N)$ such that

$$P[H(K) \ge n | K \in \mathcal{H}_N] \sim 4\frac{n^2}{N} \frac{\exp[-h(n, N)]}{1 - n^2/N^2}.$$

5. Nearest mutual ancestor

Let $\lambda(n, G)$ be the distance to the nearest mutual ancestor of all individuals living at time $n - 1$ (given that $Z(n - 1) > 0$). Let us condition on $\nu(G) = N$ and use $f_1(s)$. Call $\zeta(n, K)$ the corresponding quantity in the tree K.

One can derive $P[\zeta(n, K)/\sqrt{N} \le a | K \in \mathcal{K}_{n,N}]$ if $\frac{n}{\sqrt{N}} \to \beta$. Also $\zeta(n, K) \le na$ iff the number of upcrossings of the strip $[(n - 1)a, n]$ in the corresponding R.W. is given by (1). The same arguments can be generalized to the total number of subtrees of K having their roots on level $(1 - a)n$ and containing all vertices of given height n of K.

6. Generalizations

One can consider generation dependent branching processes, processes with some life length distribution, etc.

Tirage aléatoire de mots et d'objets combinatoires

Alain Denise
LABRI
Université de Bordeaux I

8 Février 1993

[résumé par Loÿs Thimonier]

Résumé

On propose ici une généralisation de la méthode florentine [1, 2] de génération aléatoire de certains mots : pour une grande classe, les *fg-langages*, la complexité moyenne de la méthode peut être obtenue simplement au moyen de la série génératrice du langage. L'intérêt de cette approche est son application à l'étude d'objets combinatoires associés par des bijections à de tels langages, en particulier les objets de grande taille : si le nombre des objets de taille n croît exponentiellement, leur génération exhaustive devient vite impossible ; il s'agit alors de pouvoir en temps raisonnable en générer un nombre suffisant pour une étude statistique.

1. Introduction

Soient L_n l'ensemble des mots de longueur n d'un langage L et l_n le cardinal de L_n : la génération aléatoire et uniforme de mots de L consiste, n étant donné à tirer au hasard de façon équiprobable (probabilité : $1/l_n$) un mot de L_n. Cette génération aléatoire est très utile pour l'étude de familles d'objets combinatoires, souvent associées avec des langages par des bijections ; chaque famille admet un paramètre taille, le nombre d'objets de taille $f(n)$ étant égal au nombre l_n de mots de longueur n associés par la bijection ; le nombre d'objets de taille n croît souvent exponentiellement : la génération exhaustive est vite irréalisable, une étude statistique n'est possible que par génération aléatoire et uniforme d'un nombre suffisamment important d'objets de taille n.

Comme les tailles sont grandes, la complexité de la méthode de génération doit être raisonnable en fonction de la longueur des mots. Les algorithmes déterministes permettent le calcul de la complexité dans le pire des cas ; l'algorithme le plus général [3] permet la génération aléatoire et uniforme des mots de tout langage algébrique non ambigu : sa complexité bien que polynomiale fait cependant intervenir l_n, ce qui exclut la génération efficace des très longs mots.

Les méthodes "à tirages" utilisent une suite d'essais-erreurs, entraînant un nombre non borné d'opérations nécessaires pour engendrer un mot : on ne peut prendre en compte qu'une complexité moyenne ; Barcucci, Pinzani et Sprugnoli présentent une telle méthode, avec une complexité linéaire, pour générer les mots de Motzkin ainsi que les chemins sous-diagonaux qui les généralisent [1].

C'est cette méthode qui est généralisée ici à un ensemble plus vaste, les *fg-langages*, avec une complexité moyenne obtenue simplement à l'aide de la série génératrice.

2. Génération de mots

2.1. Méthodes naïve et optimisée : modélisation par des langages. Soient : Random(A) la procédure consistant, dans l'alphabet A de cardinal k, à tirer une lettre de A de façon équiprobable ; ϵ le mot vide ; $|w|$ la longueur de w.

méthode naïve :

entrée : L, n

algorithme :

$w \leftarrow \epsilon$;
tant que $w \notin L_n$:
$w \leftarrow \epsilon$;
tant que $|w| \prec n$:
$a \leftarrow \text{Random}(A)$;
$w \leftarrow wa$;

sortie : un mot w de L_n

L'idée pour optimiser [1] est de repérer aussitôt si la construction peut continuer, grâce à un test de "maintien" : le mot en cours doit appartenir alors au langage $FG(L_n)$ des facteurs gauches des mots de L_n ; d'où :

méthode optimisée :

entrée : L, n
algorithme :

$w \leftarrow \epsilon$;
tant que $w \notin L_n$:
$w \leftarrow \epsilon$;
tant que $(|w| \prec n) \wedge (w \in FG(L_n))$:
$a \leftarrow \text{Random}(A)$;
$w \leftarrow wa$;

sortie : un mot w de L_n

On remarque que si w ne franchit pas le test de maintien, alors : $w \in R_n$, où R_n est l'ensemble des mots de $FG(L_n)A \setminus FG(L_n)$ de longueur inférieure ou égale à n, donc à la fin le mot ω obtenu après tous les tirages de lettres jusqu'à production d'un mot de L_n appartient à $G \stackrel{def}{=} L_n \cup (\cup_{i \geq 1} {R_n}^i L_n)$ vérifiant $G = L_n \cup R_n G$.

2.2. Uniformité de la génération aléatoire des mots de L_n. On doit vérifier qu'un mot v de L_n est généré avec une probabilité $p = 1/l_n$; soit $\sharp L$ le cardinal d'un langage L.

Méthode naïve. $p = \sum_{i>=0} \Pr_i(v)$, où $\Pr_i(v)$ est la probabilité d'obtenir v après la génération de i mots w de $A^n \setminus L_n$: $\Pr(w \in A^n \setminus L_n) = (k^n - l_n)/k^n \Longrightarrow \Pr_i(v) = [(k^n - l_n)/k^n]^i \cdots 1/k^n$, et $p = 1/l_n$.

Méthode optimisée. $p = \sum_{i>=0} \Pr_i(v)$, où $\Pr_i(v)$ est la probabilité d'obtenir v après la génération de i mots w de R_n ; si $R_{n,j} \stackrel{def}{=} R_n \cap A^j$, alors $\Pr(w \in R_n) = \sum_{j=1}^{n} \Pr(w \in R_{n,j}) = \sum_{j=1}^{n} \sharp R_{n,j}/k^j$; de $A^n = L_n \cup (\cup_{j=1}^{n} R_{n,j} A^{n-j})$, on tire : $k^n = l_n + k^n \Pr(w \in R_n)$, ce qui permet de terminer avec $\Pr_i$(v) et p comme pour le cas naïf.

2.3. Complexité moyenne.

2.3.1. Rapport avec le nombre moyen l de lettres tirées

Pour la méthode optimisée, le test de maintien est effectué à chaque lettre tirée, alors que par la méthode naïve il n'y a de test que quand on a tiré un multiple de n lettres : le temps de test de maintien doit être négligeable par rapport à celui de la méthode naïve ; on ne considère ici que des langages avec test de maintien en temps constant : la complexité moyenne est proportionnelle au nombre moyen l de lettres tirées pour produire un mot de L_n.

2.3.2. Rapport entre l et le nombre moyen m de mots générés pour obtenir un mot de L_n

LEMME 1. *Pour les 2 méthodes,* $m = k^n/l_n$.

PREUVE. Il s'agit de $E[X]$, où X suit une loi géométrique de paramètre l_n/k^n. Par la méthode naïve, $l = mn$ (chaque mot généré a n lettres) ; par la méthode optimisée, $m - 1 + n < l < mn$ (chacun des $(m-1)$ premiers mots a 1 lettre dans le meilleur des cas, n lettres dans le pire des cas). □

2.3.3. Méthode optimisée : nombre moyen de tirages de lettres pour obtenir un premier mot de L_n et fonctions génératrices

LEMME 2. *Si* $G_i \stackrel{def}{=} \sharp(G \cap A^i)$, $G(t) \stackrel{def}{=} \sum_j G_j t^j$ *alors* $l = (1/k)G'(1/k)$.

PREUVE. Soit X le nombre de lettres à tirer ; alors

$$l = E[X] = \sum_{j>=n} G_j/k^j = (1/k)\sum_j jG_j/k^{j-1} = (1/k)G'(1/k).$$

□

THÉORÈME 1. *Si* $R_{n,j} \stackrel{def}{=} R_n \cap A^j$, $r_{n,j} \stackrel{def}{=} \sharp R_{n,j}$, $R_n(t) \stackrel{def}{=} \sum_{j=1}^n r_{n,j}t^j$, *alors :*

$$l = n + (k^{n-1}/l_n)R'_n(1/k).$$

PREUVE. $G = L_n \cup R_nG \Longrightarrow G(t) = l_nt^n/(1 - R_n(t)$, d'où $P(t) \stackrel{def}{=} G(t/k) = l_nt^n/k^n(1 - R_n(t/k))$; l=P'(1) (lemme) $=nl_n/k^n(1 - R_n(1/k)) + l_nk^{n-1}R'_n(1/k)/k^{2n}(1 - R_n(1/k))^2$;
$A^n = L_n \cup (\cup_{j=1}^n R_{n,j}A^{n-j}) \Longrightarrow k^n = l_n + \sum_{j=1}^n r_{n,j}k^{n-j}$,
d'où $l_n = k^n(1 - R_n(1/k)$: ainsi $l = n + (k^{n-1}/l_n)R'_n(1/k)$. □

3. Fg-langages

3.1. complexité moyenne et fonction génératrice d'un fg-langage L**.** On souhaite exprimer simplement $R'_n(1/\mathrm{k})$ en fonction de L et n, ce qui va être possible quand L est un fg-langage.

DEFINITION 1. L est *préfixiel* si $FG(L) \subset$ L.

DEFINITION 2. L est *préfixe-complet* si $\forall u \in L, \exists v \neq u, v \in L$, tel que u soit un préfixe (propre) de v.

DEFINITION 3. L est un *fg-langage* s'il est préfixiel et préfixe-complet.

PROPOSITION 1. *Si* L *est un fg-langage, alors* $\forall u \in L, \forall n \succ |u|, \exists v \in L_n$ *tel que* u *soit préfixe de* v.

La preuve est aisée.

LEMME 3. *Si* L *est un fg-langage et* $Q(t) \stackrel{def}{=} R_n(t/k)$, *alors* $Q'(1) = \sum_{i=0}^{n-1} l_i/k^i - nl_n/k^n$.

PREUVE. Avec la proposition précédente, le caractère préfixiel de L, et la définition de R_n. □

LEMME 4. *Si* L *est un fg-langage,*

$$l = (\sum_{i=0}^{n-1} l_i/k^i)/[t^n]L(t/k).$$

PREUVE. $l = n + (k^n/l_n)(R'_n(1/k)/k)$ (théorème 1) ; L est un fg-langage : $R'_n(t/k)/k = Q'(t)$, et on remplace $R'_n(1/k)/k$ par l'expression de $Q'(1)$ résultant du lemme 3. L'expression obtenue se simplifie en $(\sum_{i=0}^{n-1} l_i/k^i)k^n/l_n$, et $l_n/k^n = [t^n]L(t/k)$. □

THÉORÈME 2. *Si* L *est un fg-langage, par la méthode optimisée*

$$l = \frac{[t^n](tL(t/k)/(1-t))}{[t^n](L(t/k))}.$$

PREUVE. On manipule une somme double en utilisant la formule du lemme 4. □

3.2. Cas où L est un fg-langage déterministe. Le codage d'objets combinatoires fait souvent intervenir un langage algébrique L ; quand L est en plus déterministe, il est reconnu par états d'acceptation d'un automate à pile déterministe.

THÉORÈME 3. *Si L est un fg-langage algébrique déterministe, alors le test de maintien dans $FG(L)$ peut être effectué en temps constant.*

PREUVE. On parcourt l'automate à pile précédent au fur et à mesure de la construction de w ; $w \in FG(L_n)$ si et seulement si le parcours mène à un état d'acceptation. □

COROLLAIRE 1. *La complexité moyenne de la méthode optimisée pour un fg-langage L algébrique déterministe sur un alphabet A à k lettres est proportionnelle à*

$$\frac{[t^n](tL(t/k)/(1-t))}{[t^n](L(t/k))}.$$

PREUVE. On a déjà vu que pour un langage avec test de maintien en temps constant la complexité moyenne était proportionnelle à l, et on utilise le théorème 2. □

3.3. Applications. On retrouve de façon simple à l'aide d'un logiciel de calcul formel comme $\Lambda\Upsilon\Omega$ les résultats de Barcucci, Pinzani et Sprugnoli pour des fg-langages algébriques comme les facteurs gauches de Motzkin et les chemins sous-diagonaux. Les résultats de ce travail sont en cours d'application à d'autres fg-langages (facteurs des suites de Sturm, chemins arborescents, préfixes de Dyck ...).

Bibliographie

[1] Barcucci (E.), Pinzani (R.), et Sprugnoli (R.). – *The Random Generation of Directed Animals.* – Rapport technique n° 11, Lacim, Université du Québec à Montréal, 1992. Actes de l'atelier Franco-Québécois de Combinatoire Algébrique, Eds. P. Leroux et Ch. Reutenauer.

[2] Barcucci (E.), Pinzani (R.), et Sprugnoli (R.). – The random generation of underdiagonal walks. *In : Séries formelles et combinatoire algébrique*, éd. par Leroux (P.) et Reutenauer (C.). pp. 17–32. – Université du Québec à Montréal, 1992. Proceedings of FPSAC'4, Montréal (Canada).

[3] Cohen (Jacques) et Hickey (Timothy). – Uniform random generation of strings in a context-free language. *SIAM Journal on Computing*, vol. 12, n° 4, novembre 1983, pp. 645–655.

A Calculus of Random Generation

Philippe Flajolet
INRIA Rocquencourt

February 1, 1993

[summary by Xavier Gourdon]

Abstract

A systematic approach to the random generation of labelled combinatorial objects is presented. It applies to structures that are decomposable, *i.e.*, formally specifiable by grammars involving union, product, set, sequence, and cycle constructions.

This work started with a question arising in statistical classification theory: How can one generate a random "hierarchy"? In combinatorial terms, the generation problem simply amounts to drawing uniformly at random a tree with internal nodes of degree at least 2 and with leaves (external nodes) labelled by distinct integers, the number n of leaves being fixed. The need arises in statistics as one would like to generate at random such hierarchies and compare their characteristics to hierarchical classifications obtained from real-life data.

There are well-known methods for coping with this type of tree generation problems, the general strategy relying on a divide-and-conquer principle: Generate the root with the suitable probability distribution, then recursively generate the root subtrees. Several of the basic principles of this recursive top-down approach have been formalized by Nijenhuis and Wilf in their reference book on combinatorial algorithms [7], by Hickey and Cohen in the case of context-free languages [5], and under a fairly general setting by Greene within the framework of labelled grammars [4]. This work is in many ways a systematization and a continuation of the pioneering research of these authors.

The original article can be found in [2].

1. Combinatorial structures and constructions

We consider *labelled objects*. We start from the *initial objects* $\mathbf{1}$ that designates the "empty" structure of size 0 that bears no label, and Z that generically designates a single labelled node of size 1. We operate with the usual collection of labelled *constructions*,

$$+,\ \cdot\ ,\ \mathit{sequence}(\,),\ \mathit{set}(\,),\ \mathit{cycle}(\,). \tag{1}$$

We deal with the following structures, similar to the ones considered in [1].

Definition 1. Let $\mathbf{T} = (T_0, T_1, \ldots, T_m)$ be an $(m+1)$-tuple of classes of combinatorial structures. A *specification* of $\mathbf{T}$ is a collection of $m+1$ equations, with the ith equation being of the form

$$T_i = \Psi_i(T_0, T_1, \ldots, T_m) \tag{2}$$

where Ψ_i is a term built from $\mathbf{1}$, Z, and the T_j, using the standard constructions listed in (1).

We also say, for short, that the system (2) is a specification of T_0. A structure that admits a specification is called *decomposable*. The framework of specifications resembles that of context-free grammars for formal languages, but enriched with additional constructions.

From the usual transformation rules on the exponential generating functions (egf), it is possible to derive from (2) a set of equations which specify the corresponding egf. A consequence is that given a specification, the corresponding enumerating sequences up to size n are all computable in $\mathcal{O}(n^2)$ arithmetic operations.

2. Standard specifications

In this section, we consider reduction of specifications to standard form. The standard specifications constitute the basis of the random generation procedures to be developed in the paper.

Besides the transformation into standard form, we need the pointing operator, defined as follows. Given a class A of structures, the pointing of A is a class denoted ΘA, $\Theta A = \bigcup_{n=1}^{\infty} (\mathcal{A}_n \times [1\,..\,n])$, where $\mathcal{A}_n$ is the subclass of objects in A having size n and $[1\,..\,n]$ is the integer interval $\{1, 2, \ldots, n\}$. In other words, an object in the class ΘA can be viewed as an object of A with the additional property that one of the labels, corresponding to the field in $[1\,..\,n]$, is distinguished. From the definition we have that $C = \Theta A$ implies $C_n = nA_n$. Thus, the egfs are still computable by the added rule

$$C = \Theta A \qquad \Longrightarrow \qquad C(z) = \Theta A(z), \text{ where } \Theta f(z) = z \cdot \frac{d}{dz} f(z).$$

Developments in this section are inspired by Joyal's elegant theory [6] and by Greene's work [4].

Definition 2. Let $\mathbf{T} = (T_0, T_1, \ldots, T_m)$ be a tuple of classes of combinatorial structures. A *standard specification* of $\mathbf{T}$ is a collection of $m+1$ equations, the ith equation being of one of the forms

$$T_i = \mathbf{1};\ T_i = Z;\ T_i = U_j + U_k;\ T_i = U_j \cdot U_k;\ \Theta T_i = U_j \cdot U_k,$$

where each $U_j \in \{\mathbf{1}, Z, T_0, \ldots, T_m, \Theta T_0, \ldots, \Theta T_m\}$.

Theorem 1 (Standardization algorithm). *Every decomposable structure admits an equivalent standard specification.*

The proof is actually a conversion algorithm. For example, the transformation rule for the sequence construction $B = \mathit{sequence}(A)$ is $B = \mathbf{1} + A \cdot B$. As for the set construction $B = \mathit{set}(A)$, the transformation is $\Theta B = B \cdot \Theta A$, this being understood as a fundamental combinatorial isomorphism: Pointing at a node in a set individuates the component containing the node and the component becomes pointed; this leaves aside a set of components, the non-marked ones. The cycle construction $B = \mathit{cycle}(A)$ can be translated into $\Theta B = C \cdot \Theta A$, $C = \mathit{sequence}(A)$. Similar combinatorial principle apply to the reduction of sequences, sets, and cycles under cardinality constraints.

As an illustration, a standard form for hierarchies defined by $H = Z + \mathit{set}(H, \text{card} \geq 2)$ is

$$\{H = Z + U_1,\ \Theta U_1 = U_2 \cdot \Theta H,\ \Theta U_2 = U_3 \cdot \Theta H,\ \Theta U_3 = U_3 \cdot \Theta H\}.$$

3. Basic generation schemes

From the preceding section, it is sufficient to exhibit generation routines for standard specifications. This goal is achieved by means of a set of translation rules or "*templates*", inspired by existing technology of random generation [4, 5, 7]. A *preprocessing stage* furnishes, once and for all in time $\mathcal{O}(n^2)$ and in storage $\mathcal{O}(n)$ the enumerating sequences, up to size n, of structures intervening in a specification.

Given any class C, recall that $c_n = C_n/n!$ is its normalized counting sequence, from now on assumed to be available. We let gC denote a random generation procedure relative to class C. The general strategy is based on the *divide-and-conquer* principle.

$\mathbf{T}_0$. *Initial structures.* The generation procedures corresponding to $\mathbf{1}$ and Z are trivial.

$\mathbf{T}_1$. *Unions.* If $C = A + B$, the probability that a C-structure of size n arises from A is simply a_n/c_n. The random generation procedure uses a variate U drawn uniformly from the real interval $[0, 1]$ to effect the choice.

$\mathbf{T}_2$. *Products.* If $C = A \cdot B$, the probability that a C-structure of size n has an A-component of size k and a B-component of size $n-k$ is

$$\binom{n}{k} \frac{A_k \cdot B_{n-k}}{C_n} \equiv \frac{a_k \cdot b_{n-k}}{c_n}.$$

The random generation procedure results from this equation.

$\mathbf{T}_3$. *Pointing.* Generating A and ΘA are clearly equivalent processes.

THEOREM 2 (SEQUENTIAL RANDOM GENERATION). *The templates* $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$, *and* $\mathbf{T}_3$ *produce from any standard specification* Σ_0 *a collection of random generation routines* $g\Sigma_0$. *Each routine of* $g\Sigma_0$ *uses precomputed tables consisting of* $\mathcal{O}(n)$ *integers; its worst case time complexity is of* $\mathcal{O}(n^2)$ *arithmetic operations.*

4. Boustrophedonic random generation

The standardization theory implies that all the complexity lies in the random generation of products. More precisely, when measured in the number of while-loops executed, the cost of generating (α, β) by the sequential method is the size of the first component, $|\alpha|$. In fact, a worst-case complexity of $\mathcal{O}(n \log n)$ can be achieved for all decomposable structures. The principle is simply a *boustrophedonic*[1] search. Given a product $C = A \cdot B$, we let K be the random variable denoting the size of the A-component of a C-structure. Amongst C-structures of size n, we have

$$\pi_{n,k} := \Pr\{K = k\} = \frac{a_k \cdot b_{n-k}}{c_n}.$$

The idea is to appeal to a special search for the drawing of K with the probability distribution $\{\pi_{n,k}\}_{k=0}^{n}$. Instead of the order of increasing values of k, we explore the possibilities of K in the boustrophedonic order

$$\pi_{n,0}, \pi_{n,n}, \pi_{n,1}, \pi_{n,n-1}, \ldots,$$

that sweeps alternatively from left to right and back. The recurrence translating the cost admit $\mathcal{O}(n \log n)$ solutions (see [3, Sec. 2.2]), leading to the following result.

THEOREM 3 (BOUSTROPHEDONIC RANDOM GENERATION). *Any* decomposable *structure has a random generation routine that uses precomputed tables of size* $\mathcal{O}(n)$ *and achieves* $\mathcal{O}(n \log n)$ *worst case time complexity.*

The purpose of the next sections is to come up with adequate specifications that permit to attain a complexity of $\mathcal{O}(n \log n)$ involving low multiplicative factors by exploiting "natural" regularities present in combinatorial structures. To algorithms designers, the situation resembles that of heapsort —which has guaranteed $\mathcal{O}(n \log n)$ complexity— versus quicksort —which is $\mathcal{O}(n \log n)$ only on average but with small constants—, so that quicksort is often preferred in practice.

5. The cost algebra of sequential generation

It is possible to examine the cost structure underlying the random generation procedures of the *sequential* group. This can be achieved thanks to a cost algebra, developed in [2], and corresponding to that of *complexity descriptor* in [1]. For example, it can be proved that the generation algorithm for binary plane trees corresponding to the standard specification $\{B = Z + U_1;\ U_1 = B \cdot B\}$ has average case complexity $\gamma B_n = \frac{1}{2}\sqrt{\pi} n^{3/2} + \mathcal{O}(n)$.

[1] Boustrophedonic: turning like oxen in ploughing (Webster).

6. The analysis of cost generating functions

The cost algebra we mentioned in the previous section attains its full dimension when we examine it in the light of asymptotic properties of combinatorial structures. This means that orders of growth of coefficients should be taken into account. Consideration of asymptotic properties of structures using the classical arsenal of complex analysis does provide, in all cases of practical interest, valuable guidelines regarding the design of generation algorithms.

Let's see what happens on the family of non-plane trees, whose specification is $A = Z \cdot set(A)$. It furnishes a first example where two random generation algorithms derived from combinatorially equivalent specifications lead to rather different complexity behaviours. We make use of the general principles of the standardization method, our starting point being the pair of combinatorially equivalent specifications

$$\Theta A \cong A + (\Theta A \cdot A) \cong A + (A \cdot \Theta A).$$

Applying our cost algebra leads to the following theorem.

THEOREM 4 (NON PLANE TREES). *(i). The random generation algorithm for labelled trees corresponding to the standard specification* $\Theta A = A + (\Theta A \cdot A)$ *has average cost*

$$\gamma A_n = \sqrt{\frac{\pi}{2}} n^{3/2} + \mathcal{O}(n).$$

(ii). The generation algorithm for labelled trees corresponding to the specification $\Theta A = A + (A \cdot \Theta A)$ *has average cost*

$$\gamma A_n = \frac{1}{2} n \log n + \mathcal{O}(n).$$

This result suggests optimization transformations. The pointed trees are much more numerous than the basic trees, the ratio being $\Theta A_n / A_n = n$. Accordingly, the mark tends to fall on larger portions of the tree, thus leading to the complexity $\mathcal{O}(n \log n)$.

In order to make this discussion precise, we introduce a formal definition.

DEFINITION 3. Given two generating functions F and G, F *dominates* G, in symbols $F \gg G$, if

$$\frac{f_n}{g_n} \to \infty \qquad \text{as} \quad n \to +\infty.$$

The considerations regarding labelled trees then suggest a simple heuristic:

> **Big-endian heuristic.** Given a standard specification Σ_0, reorganize all comparable pairs in products each time $A \gg B$ using the isomorphism transformation
>
> $$(A \cdot B) \hookrightarrow (B \cdot A).$$

This heuristic applied to the two specifications of non-plane trees leads to the "good choice" with an $\mathcal{O}(n \log n)$ behaviour. A further optimization that this discussion suggests consists in obtaining, as much as possible, specifications where products are *imbalanced* so as to take full advantage of the big-endian heuristic. To that purpose, the Θ operator can be employed. For instance, let us re-examine the binary trees, $B = Z + B \cdot B$. Consider the induced relation obtained by differentiation,

$$\Theta B = Z + \Theta B \cdot B + B \cdot \Theta B.$$

Let K designate the size of the first component in $B \cdot B$, and K' denote the size of the first component in $B \cdot \Theta B$. The expectation of K is $n/2$ while that of K' turns out to be $\mathcal{O}(\sqrt{n})$, so that a global gain of order close to $\mathcal{O}(\sqrt{n})$ is to be anticipated if the big endian heuristic is employed. This dictates a new heuristic:

> **Differential heuristic.** Replace in specifications polynomial relations by differential relations.

For binary trees, the differential algorithm corresponding to the specification

$$\Theta B = Z + (B + B) \cdot \Theta B$$

leads to the average behaviour $\frac{1}{2} n \log n + \mathcal{O}(n)$.

Thanks to these optimization transformations, all polynomial families of trees as well as functional graphs can be generated in time asymptotic to $\frac{1}{2} n \log n$. Furthermore, the class of iterative structures admits $\mathcal{O}(n)$ random generation algorithms.

7. Numerical data

The generation method for decomposable structures has been implemented in the symbolic manipulation system MAPLE by P. Zimmermann. The complete programme tests specifications for well-foundedness, puts them in standard quadratic form, and compiles two sets of procedures from standard specifications: the counting routines that implement the convolution recurrences, and the random generation routines based on the templates. The whole set, in its current stage, represents some 1500 lines of Maple code. The random generation procedures produced are in the Maple language itself, and they take advantage of the multiprecision arithmetic facilities available in MAPLE.

The version of the Maple programme that was written furthermore compiles random generation routines by automatically implementing a version of the big-endian heuristic based on "probing". As an outcome, all our eleven reference structures are generated in time between 2 and 9 seconds on a machine of 20 Mips for size $n = 400$. Gains involving a factor of about 10 for $n = 400$ result from optimizations dictated by the cost calculus.

8. Unlabelled structures

Many important structures of computer science and combinatorics are *unlabelled*.

Work currently under redaction shows that the framework presented here extends to unlabelled combinatorial structures. (The treatment is only made more complex because of the occurrence of Pólya operators.) As a result: (*i*) all unlabelled decomposable structures including context-free languages and term trees of symbolic computation can be generated in worst-case time $\mathcal{O}(n \log n)$; (*ii*). Wilf's `RANRUT` Algorithm [8] has expected case complexity which is $\sim \frac{1}{2} n \log n$.

Bibliography

[1] Flajolet (P.), Salvy (B.), and Zimmermann (P.). – Automatic average-case analysis of algorithms. *Theoretical Computer Science, Series A*, vol. 79, n° 1, February 1991, pp. 37–109.

[2] Flajolet (Philippe), Zimmerman (Paul), and Van Cutsem (Bernard). – *A Calculus for the Random Generation of Labelled Combinatorial Structures.* – Research Report n° 1830, Institut National de Recherche en Informatique et en Automatique, January 1993. 29 pages. To appear in *Theoretical Computer Science*.

[3] Greene (D. H.) and Knuth (D. E.). – *Mathematics for the analysis of algorithms.* – Birkhauser, Boston, 1981.

[4] Greene (Daniel Hill). – *Labelled formal languages and their uses.* – PhD thesis, Stanford University, June 1983.

[5] Hickey (T.) and Cohen (J.). – Uniform random generation of strings in a context-free language. *SIAM Journal on Computing*, vol. 12, n° 4, 1983, pp. 645–655.

[6] Joyal (André). – Une théorie combinatoire des séries formelles. *Advances in Mathematics*, vol. 42, n° 1, 1981, pp. 1–82.

[7] Nijenhuis (Albert) and Wilf (Herbert S.). – *Combinatorial Algorithms.* – Academic Press, 1978, second edition.

[8] Wilf (Herbert S.). – *Combinatorial Algorithms: An Update.* – Society for Industrial and Applied Mathematics, Philadelphia, 1989, *CBMS-NSF Regional Conference Series.*

Quelques exemples d'algorithmes de génération aléatoire

Dominique Gouyou-Beauchamps
LRI, Université d'Orsay

1er Février 1993

[résumé par Michèle Soria]

Résumé

La génération aléatoire est un outil important pour l'étude expérimentale d'objets combinatoires. Étant donnée la spécification d'une classe de structures combinatoires, il s'agit d'engendrer *uniformément* une structure de taille n (i.e. toutes les structures de taille n ont la même probabilité d'être engendrées).

Cet exposé présente un certain nombre d'algorithmes performants parmi lesquels : les algorithmes de génération d'arbres les plus classiques, l'algorithme de Hickey et Cohen pour générer des mots d'un langage context-free, l'algorithme florentin pour la génération d'animaux dirigés, les algorithmes de L. Alonso pour la génération d'arbres unaire-binaires.

1. Génération de mots de Dyck

Le langage de Dyck sur l'alphabet $\{x, \bar{x}\}$ est engendré par la grammaire $D = \epsilon + xD\bar{x}D$. Les mots de Dyck de taille $2n$ sont en bijection avec les arbres binaires de taille n. Il existe un certain nombre d'algorithmes de génération de mots de Dyck dont le *coût est linéaire* en la taille du mot :

L'algorithme de Rémy. [5] est un algorithme incrémental de génération uniforme d'arbres binaires, fondé sur la relation

$$(n+2)C_{n+1} = 2(2n+1)C_n \ ,$$

où le nombre de Catalan $C_n = \frac{1}{n+1}\binom{2n}{n}$ est le nombre d'arbres binaires de taille n. La construction d'un arbre aléatoire de taille $n+1$ à partir d'un arbre aléatoire de taille n se fait en choisissant une arête (parmi $2n+1$) pour faire l'extension, puis une orientation (gauche ou droite) pour cette arête. Chaque arbre de taille $n+1$ est ainsi obtenu avec multiplicité $n+2$.

L'algorithme de Arnold et Sleep. Il permet d'engendrer efficacement un mot de Dyck aléatoire de taille fixée $2n$. À chaque étape on engendre un x ou un $\bar{x}$ selon un tirage aléatoire dépendant de la fin de mot qu'il reste à construire. Ce tirage est fonction de l'expression du nombre $d_{h,l}$ de suffixes de chemins de Dyck de hauteur initiale h et de taille l :

$$d_{h,l} = \frac{h+1}{l+1}\binom{l+1}{\frac{l+h}{2}+1}.$$

À l'étape i, si le chemin construit est à hauteur h et s'il reste l lettres à engendrer pour former le mot, il suffit de calculer le produit $p = \frac{h+2}{l}\frac{l-h}{2n}$, et l'on engendre x avec probabilité p, et $\bar{x}$ avec probabilité $1-p$.

La factorisation de Raney. Cette factorisation [4] permet d'engendrer des mots de Lukaciewicz. Le langage de Lukaciewicz sur l'alphabet $A = \{x, \bar{x}\}$ est l'ensemble des mots f de A^* tels que $\delta(f) = -1$ et pour tout f' facteur gauche de f, $\delta(f') \geq 0$, (δ est le morphisme défini sur A^* par $\delta(x) = 1$ et $\delta(\bar{x}) = -1$).

D'après le *lemme cyclique* de Raney, tout mot g de A^* vérifiant $\delta(g) = -1$ a une factorisation unique (g_1, g_2) telle que le mot $g_2 g_1$ est dans le langage de Lukaciewicz.

L'algorithme de Raney consiste alors à construire un mot aléatoire formé de n lettres x—pas montants—et $(n+1)$ lettres $\bar{x}$—pas descendants—sans contrainte sur les facteurs gauches, puis à le factoriser par le lemme cyclique (g_2 est le plus grand facteur droit de hauteur minimale).

La factorisation de Catalan. Cette factorisation [4] permet d'engendrer des mots de Dyck à partir de mots formés d'un nombre égal de x et de $\bar{x}$, sans contraintes. Elle reflète la relation

$$(n+1)C_n = \binom{2n}{n}.$$

Soit w un mot ayant même nombre de x et de $\bar{x}$; sa réduction par la relation $x\bar{x} \equiv 1$ donne le mot résiduel $v = \bar{x}^k x^k$. Ayant placé une barre devant le premier x de v (ou au debut du mot si $k = 0$), on échange les lettres résiduelles ($x \leftrightarrow \bar{x}$) dans le mot initial w. Le résultat de cette transformation est un mot de Dyck w' avec une barre devant un $\bar{x}$ ($n+1$ possibilités). Et pour revenir en arrière, on réduit w' par $x\bar{x} \equiv 1$, sans chevaucher la barre, ce qui donne le mot $v' = x^k|\bar{x}^k$, et l'on échange ($x \leftrightarrow \bar{x}$) les lettres de v'.

2. Génération de mots d'un langage algébrique

Hickey et Cohen [3] ont donné une méthode de génération aléatoire des mots d'un langage algébrique défini par une grammaire non ambiguë, sans cycle et sans production vide. Cet algorithme est de complexité $O(n^2 \log^2 n)$, avec un précalcul de complexité $O(n^2 \log n)$ en temps, et $O(n)$ en place.

Étant donnée la grammaire $G = (N, T, A, P)$, où $N = \{N_1, \ldots, N_r\}$ est l'ensemble des non terminaux, T l'ensemble des symboles terminaux, A l'axiome, et P l'ensemble des règles de production $P = \{\pi_{i,j} : N_i \rightarrow \alpha_{i,j} | i = 1, \ldots, r \; ; j = 1, \ldots, s_i\}$, les mots sont engendrés par dérivation gauche.

Soit β un mot de $(N \cup T)^*$ de longueur inférieure à n, et N_i le non terminal le plus à gauche de β. La probabilité de poursuivre la génération en utilisant la règle $\pi_{i,j}$, pour obtenir un mot de longueur n est

$$p_{i,j}(\beta, n) = \frac{g_\gamma(n)}{g_\beta(n)},$$

où γ est le mot dérivé de β par $\pi_{i,j}$, et $g_\delta(n)$ représente le nombre de mots de T^n obtenus par dérivations à partir de δ.

Le noyau de la méthode vient de ce que tout $g_\delta(n)$ s'exprime comme convolution des $g_{N_i}^{(a_i)}(n)$, si le non terminal N_i apparaît a_i fois dans δ.

L'algorithme précalcule les $g_{N_i}(n)(i = 1, \ldots, r)$ en temps $O(n^2 \log n)$: la grammaire étant acyclique, pour chaque n il y a un nombre constant de convolutions à calculer (ce qui se fait en temps $O(n \log n)$ par transformée de Fourier rapide). Ce précalcul nécessite un espace $O(n)$ pour le stockage des $g_{N_i}(n)$.

Le calcul des $g_\delta(n)$ se fait ensuite en temps $O(n \log^2 n)$: $O(\log n)$ pour calculer les puissances des $g_{N_i}(n)$, et $O(n \log n)$ pour calculer les convolutions par FFT.

La génération d'un mot de longueur n, nécessitant $O(n)$ dérivations, se fait donc en $O(n^2 \log^2 n)$ opérations arithmétiques. Et dans le cas des grammaires linéaires, la génération est linéaire, puisqu'il n'y a pas de convolutions.

3. Génération de mots de Motzkin

Le langage des mots de Motzkin sur l'alphabet $B = \{a, x, \bar{x}\}$ est engendré par la grammaire $M = \epsilon + aM + xM\bar{x}M$. Et le langage des facteurs gauches de mots de Motzkin est engendré par la grammaire $F = M + MxF$.

Les mots de Motzkin sont en bijection avec les arbres unaire-binaires, et les facteurs gauches de mots de Motzkin sont en bijection avec les animaux dirigés.

De l'expression des grammaires, on déduit les équations vérifiées par les séries génératrices de dénombrement

$$M(t) = \sum_{n\geq 0} m_n t^n \qquad \text{et} \qquad F(t) = \sum_{n\geq 0} f_n t^n \ ,$$

où m_n (resp. f_n) est le nombre de (facteurs gauches de) mots de Motzkin formés de n lettres :

$$M(t) = 1 + tM(t) + t^2M^2(t) \qquad \text{d'où} \qquad M(t) = \frac{1 - t - \sqrt{(1-3t)(1+t)}}{2t^2} \ ,$$

$$F(t) = M(t) + tM(t)F(t) \qquad \text{d'où} \qquad F(t) = \frac{\sqrt{1+t}}{2t\sqrt{(1-3t)}} - \frac{1}{2t}.$$

La valeur asymptotique des coefficients se déduit par analyse de singularités [6] :

$$m_n \sim \frac{\sqrt{3}}{2\sqrt{\pi}} 3^{n+1} n^{-\frac{3}{2}} \qquad \text{et} \qquad f_n \sim \frac{\sqrt{3}}{\sqrt{\pi}} 3^n n^{-\frac{1}{2}}.$$

Récemment plusieurs algorithmes ont été proposés pour la génération des facteurs gauches de Motzkin d'une part, et des mots de Motzkin d'autre part, avec une complexité moyenne linéaire (même si la complexité maximale est infinie).

3.1. L'algorithme florentin. L'algorithme de Barcucci, Pinzani et Sprugnoli [2] engendre un facteur gauche de Motzkin lettre par lettre, chacune des lettres a, x et $\bar{x}$ apparaissant avec la même probabilité $1/3$. Si au cours de la génération d'un mot on engendre un préfixe qui contient un $\bar{x}$ de plus que de x, on recommence tout le processus. Ainsi chaque mot de B^* a la même probabilité d'être tiré, et donc chaque mot de F apparaît avec la même probabilité $1/f_n$.

Le coût $c(f)$ du tirage d'un mot $f \in F$ est le nombre total de lettres tirées (y compris les échecs) pour engendrer f. Et le coût moyen pour engendrer un préfixe de Motzkin de longueur n est donné par

$$C_n = \frac{1}{f_n} \sum_{f\in B^n} c(f) \ .$$

Or

$$\sum_{f\in B^n} c(f) = \sum_{f\in B^n\cap F} c(f) + \sum_{f\in B^n\cap \bar{F}} c(f)$$

La première somme, coût des essais réussis, est égale à nf_n. La seconde somme, correspondant au coût des essais avec échec, vaut $S_n = \sum_{k=1}^{n} k m_{k-1} 3^{n-k}$, puisqu'un échec à la k-ième lettre implique que l'on avait engendré un mot de Motzkin avec les $(k-1)$ lettres précédentes. Or S_n est le coefficient de t^{n-1} dans $\frac{1}{1-3t}\frac{d}{dt}\big(tM(t)\big)$, qui vaut asymptotiquement $\sqrt{\frac{3}{\pi}} 3^n n^{1/2}$.

Et l'on obtient donc l'expression asymptotique du coût moyen de génération d'un facteur gauche de Motzkin :

$$C_n = \frac{1}{f_n}(nf_n + S_n) \sim 2n.$$

L'algorithme florentin est cependant peu performant pour la génération de mots de Motzkin, puisque son coût moyen est alors quadratique (provenant du terme S_n/m_n).

3.2. Les algorithmes de L. Alonso. L. Alonso a proposé dans sa thèse [1] deux algorithmes pour engendrer des mots de Motzkin avec un coût moyen linéaire. Le premier est fondé sur une subtile méthode d'urnes, et le second est une extension de l'algorithme florentin.

La méthode des urnes. L'algorithme est le suivant ; on répartit les mots de Motzkin de taille n dans v urnes, en plaçant dans l'urne i les N_i mots de Motzkin ayant $i-1$ lettres x. Puis on ajoute dans chacune des urnes un certain nombre de *mots blancs* (mots qui ne sont pas de Motzkin), de façon que l'urne i contienne en tout D_i mots. On choisit alors au hasard l'urne k avec la probabilité $D_k/\sum D_i$ (étape 1). Puis on tire un mot dans l'urne k (étape 2) ; si ce mot n'est pas un mot blanc (*bon choix*) on engendre un mot de Motzkin de taille n ayant k lettres x (étape 3), et sinon on reprend le processus à l'étape 1, jusqu'à ce qu'on fasse un *bon choix*.

Notons $D = \sum_i D_i$ et $N = \sum_i N_i$.

LEMME 1. *La probabilité de faire un bon choix sur l'urne i est $P_i = N_i/N$.*

En effet la probabilité de faire un bon choix sur l'urne i est $\frac{D_i}{D}\frac{N_i}{D_i} = \frac{N_i}{D}$, et la probabilité de faire les étapes 1–2 "pour rien" est $R = 1 - N/D$. Le processus se répétant jusqu'à obtenir un bon choix, on a donc

$$P_i = \frac{N_i}{D}(1 + R + R^2 + \cdots) = \frac{N_i}{N}.$$

LEMME 2. *Le nombre moyen d'étapes 1–2 pour faire un bon choix sur une urne est D/N.*

En effet il y a j étapes 1–2 si les $j-1$ premières sont "pour rien", et la dernière donne un bon choix. Donc le nombre moyen d'étapes 1–2 vaut $\sum_j jR^{j-1}(1-R) = \frac{1}{1-R} = D/N$.

COROLLAIRE 1. *La complexité moyenne de l'algorithme par méthode d'urnes est*

$$\frac{D}{N}(F+G) + H,$$

où F est la complexité moyenne de l'étape 1, G est la complexité moyenne de l'étape 2, et H la complexité moyenne pour construire un mot de Motzkin, étant donné son nombre de x—étape 3.

Il reste donc à déterminer les valeurs de F, G, H et D/N. La complexité moyenne pour construire un mot de Motzkin de taille n ayant k lettres x est linéaire, pour tout k, donc $H = O(n)$. Par ailleurs, un choix judicieux des D_i permet de montrer que F et G sont en $O(n)$, et D/N est en $O(1)$.

Les valeurs de N_i (nombre de mots de Motzkin ayant $i-1$ lettres x) sont connues :

$$N_i = 0 \quad \text{pour} \quad i > 1 + \lfloor n/2 \rfloor, \quad \text{et} \quad N_i = \binom{n}{2i}\frac{1}{i+1}\binom{2i}{i} \quad \text{pour} \quad 1 \le i \le 1 + \lfloor n/2 \rfloor.$$

Les D_i sont choisis légèrement supérieurs aux N_i de façon que la méthode de rejet soit linéaire en moyenne :

$$D_i = \frac{1}{n+1}\binom{n+1-\lfloor\frac{n+1}{3}\rfloor}{i}\binom{n+1}{\lfloor\frac{n+1}{3}\rfloor}.$$

– Pour tout i, N_i/D_i se met sous la forme $\binom{a}{c}/\binom{b}{c} \le 1$.
– L'étape 1, choix de l'urne i avec la probabilité D_i/D peut se faire en engendrant une suite de $n+1-\lfloor\frac{n+1}{3}\rfloor$ bits et en faisant la somme des bits engendrés (et donc $F = O(n)$), puisque

$$\frac{D_i}{D} = \binom{n+1-\lfloor\frac{n+1}{3}\rfloor}{i}/2^{n+1-\lfloor\frac{n+1}{3}\rfloor}.$$

– L'étape 2, validation du choix de l'urne i avec la probabilité N_i/D_i peut se faire en choisissant c entiers dans $[1,b]$ et en vérifiant qu'ils sont tous inférieurs à a, et donc $G = O(n)$.
– L'évaluation asymptotique de D donne $D \sim \frac{1}{2\sqrt{\pi}}3^{n+2}n^{-3/2}$, et donc $D/N \sim \sqrt{3}$.

On obtient donc finalement

THÉORÈME 1. *La complexité de génération aléatoire de mots de Motzkin par méthode d'urnes est en moyenne linéaire.*

Extension de l'algorithme florentin. En utilisant une bijection entre les mots de Motzkin et le sous-ensemble des facteurs gauches de Motzkin qui contiennent au moins un pas horizontal à hauteur 0, L. Alonso montre que l'algorithme florentin peut être étendu à la génération aléatoire de mots de Motzkin avec une complexité moyenne linéaire.

La méthode se déroule en quatre étapes :

– Génération d'un facteur gauche de Motzkin p, de taille $n+1$ qui n'est pas un mot de Motzkin sans pas horizontal à hauteur 0.

– Transformation de p en un facteur gauche p' de hauteur finale impaire.

– Transformation de p' en un mot m, de taille $n+1$ sur $\{x, \bar{x}, a\}^*$, ayant un $\bar{x}$ de plus que de x.

– Transformation de m en un mot de $M\bar{x}$, de taille $n+1$, par application du lemme cyclique.

Le coût moyen de la première étape, en utilisant l'algorithme florentin avec retirage lorsque le facteur gauche tiré est un mot de Motzkin sans pas horizontal à hauteur 0, est linéaire, car la probabilité d'avoir à faire un retirage est en $O(1/n)$. Les deux étapes suivantes sont des transformations bijectives de coût $O(n)$. Enfin l'application du lemme cyclique est aussi en $O(n)$.

L'algorithme est donc de complexité moyenne linéaire, et de plus la génération est uniforme : chaque mot de Motzkin est engendré avec probabilité $1/m_n$.

Bibliographie

[1] Alonso (Laurent). – *Structures arborescentes, algorithmes de génération, problème de l'inclusion, relations maximin.* – Thèse de PhD, Université de Paris-Sud, Orsay, novembre 1992.

[2] Barcucci (E.), Pinzani (R.), et Sprugnoli (R.). – *The Random Generation of Directed Animals.* – Rapport technique n° 11, Lacim, Université du Québec à Montréal, 1992. Actes de l'atelier Franco-Québécois de Combinatoire Algébrique, Eds. P. Leroux et Ch. Reutenauer.

[3] Hickey (T.) et Cohen (J.). – Uniform random generation of strings in a context-free language. *SIAM Journal on Computing*, vol. 12, n° 4, 1983, pp. 645–655.

[4] Lothaire (M.). – *Combinatorics on Words.* – Addision-Wesley, 1983, *Encyclopedia of Mathematics and its Applications*, vol. 17.

[5] Rémy (J.-L.). – Un procédé itératif de dénombrement d'arbres binaires et son application à leur génération aléatoire. *RAIRO Theoretical Informatics and Applications*, vol. 19, n° 2, 1985, pp. 179–195.

[6] Vitter (Jeffrey Scott) et Flajolet (Philippe). – Analysis of algorithms and data structures. *In : Handbook of Theoretical Computer Science*, éd. par van Leeuwen (J.), Chapitre 9, pp. 431–524. – North Holland, 1990.

Part II

Symbolic Computation

Automatic Asymptotics and Generating Functions

Bruno Salvy
INRIA Rocquencourt

September 16, 1992

[summary by Bruno Salvy]

Abstract

Computer algebra systems can be of help in the asymptotic analysis of combinatorial sequences. Several algorithms are presented, most of which have been implemented in Maple.

Introduction

We assume a sequence is given, either by its first terms or by a combinatorial description of a class of objects it enumerates. The main tool we use is the *generating function* of the sequence. The idea is to consider this formal power series as an analytic function. When the series has a non-zero radius of convergence, Cauchy's theory makes it possible to find an asymptotic estimate of the sequence we started with.

1. From the sequence to the series

The preferred method naturally depends on the available information concerning the sequence.

Empirical method. When only the first few terms of the sequence are known, there are *a priori* an infinite number of possible sequences, and there seems to be little sense in looking for an asymptotic behaviour. However, there is quite often a "simple" sequence defined by these first terms. This approach was initiated by F. Bergeron and S. Plouffe [2], who looked for Padé approximants of the generating series. When the number of non-zero coefficients of the Padé approximant is "significantly" smaller than the number of given terms of the sequence, it is natural to conjecture that the generating series is rational and that a closed-form was found. This method can be extended by applying it to the logarithmic derivative or to the functional inverse of the given power series, which yields nice generating functions.

With P. Zimmermann, we applied this idea of looking for a "simple" generating function given its first coefficients to the quest of "holonomic" sequences, i.e. sequences satisfying a linear recurrence with polynomial coefficients. Rather than looking for a Padé approximant, this recurrence is sought by an undeterminate coefficients method. When the number of non-zero coefficients of the recurrence is "sufficiently" smaller than the number of given terms, the recurrence is conjectured as being satisfied by the whole sequence. This is implemented in the Gfun package [12].

Both these methods are very efficient in practice. Among the approximately 6000 sequences of the next edition of Sloane's book [14], roughly 25% of the sequences are thus conjectured rational, and an extra 5% are conjectured holonomic non-rational [9].

Combinatorial method. A large number of sequences f_n enumerate the number of objects of size n in some *decomposable* combinatorial data-structure. This means that the structure can be expressed in terms of a small combinatorial toolbox comprising cartesian product, disjoint union, list, set, cycle and basic atoms. Thus the structure "functional graph" (the graph of an application of a set of n elements into itself) is

expressed as a set of connected components, these components being cycles of trees, these trees themselves being recursively defined as the cartesian product of a node (the root of the tree) by a set of trees.

The $\Lambda\Upsilon\Omega$ system, developed jointly with P. Zimmermann and Ph. Flajolet [3, 4] implements a translation of these combinatorial specifications into equations relating the corresponding generating functions. In the example of functional graphs, the first part of the system will produce the following equations:

$$\mathrm{FuncGraph}(z) = \exp(\mathrm{comp}(z)), \quad \mathrm{comp}(z) = \log[1/(1-\mathrm{tree}(z))], \quad \mathrm{tree}(z) = z\,\exp(\mathrm{tree}(z)).$$

A second part of the system then attempts to find an explicit form of the generating function from this system. For, in its current state, the asymptotic part of the $\Lambda\Upsilon\Omega$ system can only handle explicit generating functions. In this example, thanks to Maple's W function, the following "explicit" form is obtained:

$$\frac{1}{1+W(-z)}.$$

Conclusion. Two very different methods have been described to obtain the generating function of a sequence. The first one finds *holonomic* generating functions, i.e. solutions of linear differential equations with polynomial coefficients. The second one is more combinatorial and finds generating functions that obey functional equations expressed in terms of some "elementary" functions. In some cases, these equations can be solved.

Known algorithms to get "explicit" forms from these equations can be summarised as follows.

- Liouvillian solutions of linear differential equations can be obtained by Kovacic's algorithm for the case of order 2. This algorithm is (at least partially) implemented in most computer algebra systems. An algorithm due to M. Singer treats the general case, but is not practical. The third order has been made practical by F. Ulmer, but there is no generally available implementation;
- Hypergeometric solutions of linear differential equations can be found by an algorithm due principally to M. Petkovšek, without any limitation on the order of the equation [8];
- Elementary functional equations can only be solved in some special cases.

2. From generating functions to asymptotics

When the generating series defines an analytic function, Cauchy's formula yields the nth Taylor coefficient as

$$[z^n]f(z) = \frac{1}{2i\pi}\oint \frac{f(z)}{z^{n+1}}dz.$$

The path of integration is a closed contour containing the origin and no other singularity.

We are looking for an asymptotic estimate as n tends to infinity. First of all, Hadamard's rule implies that the coefficients grow roughly as $1/R^n$, where R is the radius of convergence. This relates the exponential growth of the Taylor coefficients of a generating function to the location of its singularities. Besides, simple functions whose coefficients are known, such as $1/(1-z)^\alpha$, give the intuition that sub-exponential growth of the coefficients is related to the local growth of the generating function in the neighbourhood of its singularity of smallest modulus. This can be made precise.

2.1. Singularity analysis. In 1878, G. Darboux treated the case of algebraic singularities. This result was extended by R. Jungen in 1934 to handle singularities in $(1-z)^\alpha \log^k(1-z)$, where k is a non-negative integer. Finally, Ph. Flajolet and A. Odlyzko [5] described the more general case where the exponents of $(1-z)$ and of the logarithm are complex numbers. These methods yield a full asymptotic expansion of the Taylor coefficients.

This leads to the following algorithm to find the asymptotic expansion of coefficients of a generating function.

(1) Locate the singularities of smallest modulus;
(2) Compute the expansion of the function in the neighbourhood of these singularities;
(3) Translate this expansion into the expansion of the coefficients.

The last step above is easy. We now insist on how the first two steps can be automated. This depends on the type of equation defining the generating function.

When the generating function is given as a solution to a linear differential equation, its singularities are found among the poles of the coefficients of the equation and the roots of its leading coefficient. Since the coefficients are polynomials, singularities in this case are therefore algebraic numbers. When the generating function is given explicitly in terms of elementary functions, it is easy to find a set of points containing the singularities by a recursive algorithm.

Then one has to compare the moduli of the singularities. Algebraic numbers can be compared by purely algebraic methods using resultants and Sturm sequences. It is also possible to make use of guaranteed numerical estimates, see [6]. In the more general case of elementary constants one is confined to heuristics, the problem being related to difficult questions of transcendency.

Once the dominant singularities have been located, one looks for the local behaviour of the generating function in the neighbourhood of these singularities. When the function is given explicitly as an exp-log function (functions built up from $\mathbb{Q}$ and x by field operation, exp and $x \mapsto \log|x|$), a recent algorithm due to J. Shackell [13] makes it possible to compute the local expansion. When the generating function is holonomic, the possible behaviours have been given by E. Fabry in 1885, and have the form

$$\exp[P(1/(1-(z/\rho)^{1/d}))](1-z/\rho)^{\alpha}\sum_{k=0}^{K}\phi_k(z)\log^k(1-z/\rho),$$

where ϕ_k are formal power series in $1-z/\rho$. Such local solutions can be determined automatically [15]. Once a basis of local solutions has been found, one has to find the right linear combination in terms of the first elements of the sequence. While these elements are given by the Taylor expansion of the function at the origin, we have a basis of local solutions at the singularity. Besides, the formal power series ϕ_k are generally divergent. One must then resort to the theory of resummation [1].

2.2. Saddle-point method. When the function is entire or has a singularity of a more "violent" type than a mere algebraico-logarithmic type, it is often possible to use a saddle-point method. Setting $h(z) = \log(f(z)) - (n+1)\log z$, the contour of Cauchy's integral is deformed to pass through a point (*the saddle-point*) where $h'(z) = 0$. With a few extra hypotheses, Cauchy's integral is then concentrated in the neighbourhood of the saddle-point and the integral can be approximated by a Gaussian. If we denote the saddle-point by R, the nth coefficient is then estimated as

$$[z^n]f(z) \approx \frac{f(R)}{R^{n+1}\sqrt{2\pi h''(R)}}.$$

To automate this method and the approximations it requires, one uses a theorem due to W. K. Hayman [7], which makes it possible to decide sufficient conditions under which the method applies. A last technical problem is that the saddle-point is often only available as an asymptotic expansion deduced from the equation $h'(R) = 0$. An algorithm to compute this expansion under very general conditions has been developed in [11].

Bibliography

[1] Balser (W.), Braaksma (B. L. J.), Ramis (J.-P.), and Sibuya (Y.). – Multisummability of formal power series solutions of linear ordinary differential equations. *Asymptotic Analysis*, vol. 5, 1991, pp. 27–45.

[2] Bergeron (F.) and Plouffe (S.). – Computing the generating function of a series given its first terms. *Journal of experimental mathematics*, 1993.

[3] Flajolet (P.), Salvy (B.), and Zimmermann (P.). – *Lambda-Upsilon-Omega: The 1989 CookBook*. – Research Report n° 1073, Institut National de Recherche en Informatique et en Automatique, August 1989. 116 pages.

[4] Flajolet (P.), Salvy (B.), and Zimmermann (P.). – Automatic average-case analysis of algorithms. *Theoretical Computer Science, Series A*, vol. 79, n° 1, February 1991, pp. 37–109.

[5] Flajolet (Philippe) and Odlyzko (Andrew M.). – Singularity analysis of generating functions. *SIAM Journal on Discrete Mathematics*, vol. 3, n° 2, 1990, pp. 216–240.

[6] Gourdon (Xavier) and Salvy (Bruno). – Asymptotics of linear recurrences with rational coefficients. In Barlotti (A.), Delest (M.), and Pinzani (R.) (editors), *Formal Power Series and Algebraic Combinatorics*, pp. 253–266. – 1993. Proceedings of FPACS'5, Florence (Italy).

[7] Hayman (W. K.). – A generalization of Stirling's formula. *Journal für die reine und angewandte Mathematik*, vol. 196, 1956, pp. 67–95.

[8] Petkovšek (Marko) and Salvy (Bruno). – Finding all hypergeometric solutions of linear differential equations. In Bronstein (Manuel) (editor), *ISSAC'93*. pp. 27–33. – ACM Press, July 1993.

[9] Plouffe (S.). – *Approximations de séries génératrices et quelques conjectures.* – Master's thesis, Université du Québec à Montréal, September 1992. Also available as Research Report 92-61, Laboratoire Bordelais de Recherche en Informatique, Bordeaux, France.

[10] Salvy (Bruno). – *Asymptotique automatique et fonctions génératrices.* – PhD thesis, École Polytechnique, 1991.

[11] Salvy (Bruno) and Shackell (John). – Asymptotic expansions of functional inverses. In Wang (Paul S.) (editor), *Symbolic and Algebraic Computation*. pp. 130–137. – ACM Press, 1992. Proceedings of ISSAC'92, Berkeley.

[12] Salvy (Bruno) and Zimmermann (Paul). – *Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable.* – Technical Report n° 143, Institut National de Recherche en Informatique et en Automatique, 1992. To appear in *ACM Transactions on Mathematical Software*.

[13] Shackell (John). – Growth estimates for exp-log functions. *Journal of Symbolic Computation*, vol. 10, December 1990, pp. 611–632.

[14] Sloane (N. J. A.). – *A Handbook of Integer Sequences.* – Academic Press, 1973.

[15] Tournier (Évelyne). – *Solutions formelles d'équations différentielles.* – Doctorat d'État, Université scientifique, technologique et médicale de Grenoble, 1987.

Symbolic Computation with P-finite Sequences

Marko Petkovšek
University of Ljubljana, Slovenia

September 16, 1992

[summary by Bruno Salvy]

The talk consists in two parts. The first part is devoted to computer algebra algorithms for the manipulation of P-finite (holonomic in one variable) sequences and the second part, based on M. Petkovšek's thesis, to the resolution of linear recurrences with polynomial coefficients.

1. Manipulations of P-finite sequences

Given two sequences a_n and b_n defined by their linear recurrences and initial values, it is possible to build algorithmically the recurrences and initial values satisfied by αa_n, $a_n + b_n$, $a_n \cdot b_n$, $\sum_{k=0}^{n} a_k b_{n-k}$. From this, identities can be checked quite easily: to check that $a_n = b_n$ for all n, build up the equation satisfied by $a_n - b_n$, and check that the initial conditions are all zero. Note that the algorithms used for this purpose in the case of holonomic sequences (see the summary of P. Flajolet's talk on holonomic functions in last year seminar) can be replaced by faster and simpler ones in the case of C-finite sequences (solutions of recurrences with constant coefficients). These simpler algorithms have been implemented by W. Koepf [1][1]. An example of a C-finite identity which can be checked that way is Cassini's identity for Fibonacci numbers:

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n, \quad n \geq 1.$$

2. Resolution of linear difference equations

2.1. Classes of solutions. By "resolution" of an equation, one means finding an expression of a solution in a well-defined class of expressions. In general, not all solutions of an equation can be expressed in a class (e.g., not all solutions of polynomials in $\mathbb{Q}[x]$ are expressible in terms of radicals), and the problem is to find those solutions that admit such an expression, or to prove that none exists.

In the case of linear recurrence equations, Figure 1 shows the relationships between important classes. Here is a definition of the less well-known of them.

- Exponential polynomials are terms of the form
$$\sum_k e^{n\theta_k} P_k(n),$$
with P_k polynomials and the sum being finite. These are well-known to be the solutions of all C-finite recurrences.
- Quasirational terms are defined similarly, with rational functions instead of polynomials.
- Hypergeometric terms are functions $f(n)$ such that $f(n+1)/f(n)$ is rational in n. The general form of such a term is thus
$$C\frac{(\alpha_1 + n)! \cdots (\alpha_p + n)!}{(\beta_1 + n)! \cdots (\beta_q + n)!} Z^n,$$
with C in the ground field, and Z, α_i and β_j in its algebraic closure.

[1]The case with polynomial coefficients has been implemented in Maple by P. Zimmermann and B. Salvy in the gfun package, and of course by D. Zeilberger in a somewhat exotic Maple.

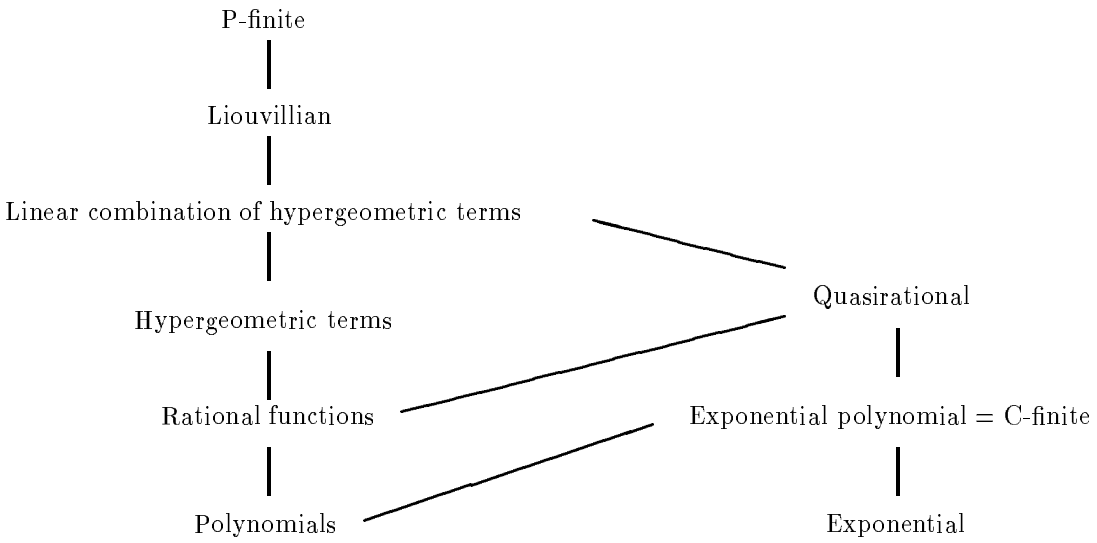


FIGURE 1. Classes of sequences

– Liouvillian terms in this context are terms built up by a finite number of products, sums, algebraic extensions and field operations.

From the algorithmic point of view, polynomial solutions can be found by indeterminate coefficients (the second coefficient yields the degree), rational and quasirational solutions can be found by S. Abramov's algorithm (see the summary of his talk in this seminar, and references there), solutions that are hypergeometric terms or linear combinations of them can be found thanks to M. Petkovšek's algorithm that we now describe.

2.2. Hypergeometric solutions. Let u_n be an hypergeometric solution of

$$p_d(n)u_{n+d} + p_{d-1}(n)u_{n+d-1} + \cdots + p_1(n)u_{n+1} + p_0(n)u_n = 0, \tag{1}$$

where the $p_i(n)$ are polynomials in n. Note that non-homogeneous equations can also be considered by increasing the order (a subtler solution will be presented later). Since u_n is hypergeometric, there exists a rational function $R(n)$ such that $u_{n+1} = R(n)u_n$. Substituting this into (1) and dividing out by u_n, we get a non-linear equation in R. The idea then is to consider poles of the $R(n+i)$, which have to be cancelled. A difficulty arises from the fact that a numerator of some other $R(n+j)$ might interfere in this cancellation. To make things clearer, Gosper introduced a slightly weaker form of the following decomposition lemma due to M. Petkovšek in this form.

LEMMA 1. *Let $\mathbb{F}$ be a field of characteristic 0 and $R \in \mathbb{F}(n)\backslash\{0\}$. Then there exists a unique decomposition*

$$R(n) = Z\frac{A(n)}{B(n)}\frac{C(n+1)}{C(n)},$$

where $Z \in \mathbb{F}$, A, B and C are monic polynomials with coefficients in $\mathbb{F}$ and

– $\gcd(A(n), B(n+k)) = 1$, *for all non-negative integer k,*
– $\gcd(A(n), C(n)) = \gcd(B(n), C(n+1)) = 1$.

Using this lemma and plugging this decomposition for u_{n+1}/u_n into (1), we get

$$\begin{aligned} &p_d(n)Z^d A(n+d)\cdots A(n)C(n+d) + p_{d-1}(n)Z^{d-1}A(n+d-1)\cdots A(n)B(n+d)C(n+d-1) \\ &\quad + \cdots + p_1(n)ZA(n)B(n+d)\cdots B(n+1)C(n+1) + p_0(n)B(n+d)\cdots B(n)C(n) = 0. \end{aligned} \tag{2}$$

Simple divisibility considerations then lead to

$$A(n) \mid p_0(n), \quad B(n+d) \mid p_d(n).$$

From this we deduce M. Petkovšek's algorithm HYPER:

(1) Compute the list of factors of $p_0(n)$ and $p_d(n-d)$ (over their splitting fields),
(2) for each pair of factors, compute equation (2),
(3) check the existence of a polynomial solution.

Note that the factorization in step 1 makes this algorithm expensive, and the loop in step 2 makes it exponential in the degrees of the leading and trailing coefficients of the recurrence.

2.3. Extensions.

A larger class. This algorithm can also be used to find non-hypergeometric solutions: once a solution $f_1(n)$ has been found, one can reduce the order of the recurrence, and call the algorithm recursively. If a solution $f_2(n)$ is then found, it corresponds to a solution $f_1(n)\sum f_2(n)$ of the initial equation. In general, this will not be hypergeometric. To check if it is, one can use either Gosper's or Abramov's algorithm to reduce the sum. Of course, the process can be repeated inductively.

Linear combinations. It is important to note that if $L(u_n)$ is a linear recurrence and h_n is an hypergeometric term (not necessarily a solution of L), then $L(h_n)/h_n$ is a rational function in n. Thus if $h_1, \ldots, h_n$ are hypergeometric terms linearly independent over the field of rational functions, and if a linear combination of them is cancelled by L, then each h_i is a solution of L. Since these can be found by HYPER, we get that this algorithm cannot "miss" a linear combination of hypergeometric terms.

Non homogeneous equations. We now consider an equation of the form

$$Ly = f.$$

If f is a rational function, then an obvious solution is to make the equation homogeneous at the expense of increasing its order by one, and then apply the same algorithm. However, it follows from the considerations in the previous paragraph that there exists a particular polynomial solution in this case, and thus we just have to look for a polynomial.

If f is an hypergeometric term, then from the previous paragraph again, one has to look for a rational multiple of f. One then builds the equation this rational function has to satisfy, and appeal to Abramov's algorithm in order to get it.

When f is not an hypergeometric term and if a basis of solutions of $Ly = 0$ has been found either by HYPER or by its extension to multiple sums, then the following idea of S. Abramov's provides a nice alternative to the variation of constants method. Taking the solutions of the homogeneous equation in turn, one reduces the order of the equation and performs the same modification to the remaining solutions and to the right-hand side. At the end, we are left with an equation of order 0, hence the solution.

Definite hypergeometric summation. Consider

$$S_n = \sum_{k=-\infty}^{+\infty} F(n,k),$$

where $F(n+1,k)/F(n,k)$ and $F(n,k+1)/F(n,k)$ both are rational functions in n and k. Then Zeilberger has given an algorithm [6] that computes a linear recurrence for S_n. From this equation, HYPER will find if there is an hypergeometric sum.

Factorization of recurrence operators. The algorithm HYPER can be viewed as finding the right factors of order 1 or a recurrence operator. M. Petkovšek found another algorithm for the more general case of a right factor of any order. This algorithm is similar to F. Schwarz's algorithm in the differential case [5].

k-hypergeometric sequences. This is another natural extension of HYPER to sequences such that a_{n+k}/a_n is rational. Given k one can find all such sequences solutions of a linear recurrence equation. It is as yet unknown if there is a computable upper bound on the possible values of k for a given recurrence.

Bibliography

[1] Koepf (Wolfram). – Power series in computer algebra. *Journal of Symbolic Computation*, vol. 13, 1992, pp. 581–603.

[2] Petkovšek (Marko). – *Finding Closed-Form Solutions of Difference Equations by Symbolic Methods.* – PhD thesis, CMU, September 1990. Available as Technical Report CMU-CS-91-103.

[3] Petkovšek (Marko). – Factorization of linear difference operators. – Preprint, 1992.

[4] Petkovšek (Marko). – Hypergeometric solutions of linear recurrences with polynomial coefficients. *Journal of Symbolic Computation*, vol. 14, 1992, pp. 243–264.

[5] Schwarz (F.). – A factorization algorithm for linear ordinary differential equations. In *Proceedings of ISSAC'89*. pp. 17–25. – ACM Press, 1989.

[6] Zeilberger (Doron). – The method of creative telescoping. *Journal of Symbolic Computation*, vol. 11, 1991, pp. 195–204.

Rational Solutions of Linear Difference and Differential Equations

Sergeï Abramov
Computer Center of the Russian Academy of Sciences

September 16, 1992

[summary by Bruno Salvy]

Abstract

The talk presents an algorithm due to S. Abramov that computes rational solutions of an equation of the type

$$a_d(n)\,u_{n+d} + a_{d-1}(n)\,u_{n+d-1} + \cdots + a_1(n)\,u_{n+1} + a_0(n)\,u_n = b(n), \tag{1}$$

where the coefficients are polynomials in n. This algorithm computes the solutions without performing any factorization, but only gcd computations. Thus it is rather independent of the ground field and in particular, it performs well when the ground field is some algebraic extension of $\mathbb{Q}$. An analogous algorithm also due to S. Abramov solves the differential case.

1. Description of the algorithm

Once some $P(n)/Q(n)$ has been substituted for u_n into Equation (1), it is natural to attempt to deduce some information from the study of the poles of the rational functions involved. However, this is made difficult by the possibility of roots of Q differing by an integer. The idea of S. Abramov's algorithm is to first compute an upper bound h on the integers differences of roots of possible solutions, and then compute the linear relation satisfied by u_n, u_{n+h}, u_{n+2h}, ... :

$$f_q(n)\,u_{n+qh} + f_{q-1}(n)\,u_{n+(q-1)h} + \cdots + f_1(n)\,u_{n+h} + f_0(n)\,u_n = g(n), \tag{2}$$

In this relation the poles cannot interfere any longer and thus the polynomials f_j have to cancel the denominators of the rational functions u_{n+qh}. In other words,

$$Q(n) \mid \gcd(f_0(n), f_1(n-h), \ldots, f_q(n-qh)).$$

Changing the unknown function by eliminating this gcd, one gets a linear recurrence equation that must have a polynomial solution. Such a solution can be found by undeterminate coefficients.

The main difficulty is to compute an upper bound for h. Substituting again $P(n)/Q(n)$ for u_n in (1), one gets that the maximal integer difference between two roots of $Q(n)$ has to be less that the maximal integer difference between two roots of a_0 and a_d, minus d.

Once this bound for h has been found, there only remains to construct Equation (2). This is done by rewriting all the u_{n+ih} for $0 \le i \le d$ in terms of u_n, u_{n+1}, ... ,u_{n+d-1}, and then performing a Gaussian elimination. Note that in this stage it is only necessary to compute with the homogeneous part of Equation (1).

2. Extension of the algorithm

Once a solution $U_1(n)$ has been found, it is possible to reduce the order of the equation by a change of variable. If a new solution $U_2(n)$ is then found, it corresponds to the solution $U_1 \sum U_2$ of the initial equation. Again the process can be applied and one gets a chain of iterated sums. Of course the process is bound to stop because only d independent solutions can be found.

It is not obvious whether the algorithm outlined above will find *all* the solutions of (1) that are iterated sums, regardless of the order in which the solutions are found and the equation reduced. This was proved to be true in [2].

Another type of extension is by looking for sequences V_n such that $\Delta^k V_n$ is a rational solution of (1)[1]. This is made easy by the fact that for such a k to exist, Equation (1) must have a polynomial solution of degree k. The proof of this is as follows: suppose $\Delta^k V_n$ is a rational solution of (1), while $\Delta^{k-1} V_n$ is not rational. Starting from (1) we can compute a linear difference equation satisfied by $\Delta^{k-1} V_n$. Let this equation be

$$h_p(n)\,\Delta^p u_n + h_{p-1}(n)\,\Delta^{p-1} u_n + \cdots + h_1(n)\,\Delta u_n + h_0(n)\,u_n = b(n).$$

Then if h_0 is not zero, one can rewrite $u_n = \Delta^{k-1} V_n$ as a rational function of $(\Delta^k V_n, \Delta^{k+1} V_n, \ldots)$, and since all these functions are rational, this would imply that $\Delta^{k-1} V_n$ is rational. Thus $h_0 = 0$, but then it means that $\Delta^{k-1} V_n = 1$ is a solution, and this implies that V_n is a polynomial of degree k. This reasoning also provides an algorithm.

Bibliography

[1] Abramov (S. A.). – Rational solutions of linear differential and difference equations with polynomial coefficients. *USSR Computational Mathematics and Mathematical Physics*, vol. 29, n° 11, 1989, pp. 1611–1620. – Translation of the *Zhurnal Vychislitel'noi Matematiki i Matematichesckoi Fiziki*.

[2] Abramov (S. A.). – A problem in computer algebra connected with solutions of linear differential and difference equations. *Kibernetika*, vol. 2, 1991, pp. 30–37. – (Russian).

[1] Here Δ denotes the difference operator: $\Delta u_n = u_{n+1} - u_n$.

Limit computation in computer algebra

Dominik Gruntz

ETH Zürich

March 29, 1993

[summary by Bruno Salvy]

The automatic computation of limits can be reduced to two main sub-problems. The first one is *asymptotic comparison* where one must decide automatically which one of two functions in a specified class dominates the other one asymptotically. The second one is *asymptotic cancellation* and is usually exemplified by

$$e^x[\exp(1/x + e^{-x}) - \exp(1/x)], \quad x \to \infty.$$

In this example, if the sum is expanded in powers of $1/x$, the expansion always yields $O(x^{-k})$, and this is not enough to conclude.

In 1990, J. Shackell [2] found an algorithm that solved both these problems for the case of *exp-log* functions, i.e. functions built by recursive application of exponential, logarithm, algebraic extension and field operations to one variable and the rational numbers. D. Gruntz and G. Gonnet propose a slightly different algorithm for exp-log functions. Extensions to larger classes of functions are also discussed.

1. Shackell's algorithm

An introduction to Shackell's algorithm can be found in the summary of last year's seminar. To simplify, given an exp-log expression, this algorithm rewrites it into its *nested form*, an almost normal form on which the asymptotic behaviour reads off easily. The difficult operation when doing this is addition because of possible cancellations. When faced with a sum, the algorithm first computes a list of the growth orders in the expressions, then orders it, and by substituting the largest ones by zero, tries to determine which one provides the right asymptotic scale, then it rewrites the expression in terms of this one and a recursive application of this gives the nested form. By this method, J. Shackell effectively reduced asymptotic computation on exp-log functions to the equivalence problem for exp-log constants.

2. The Gruntz-Gonnet algorithm

The Gruntz-Gonnet algorithm proceeds as follows. It first computes a list of orders of growth of the expression, then it finds the most rapidly varying term, expands in terms of it, and applies itself recursively on the leading coefficient if necessary. The three main steps may be summarized as follows:

The most rapidly varying term. This is not quite the most rapidly varying term, but the recursive definition is

$$\begin{aligned}
\operatorname{mrv}(f+g) &= \max(\operatorname{mrv}(f), \operatorname{mrv}(g)),\\
\operatorname{mrv}(f\cdot g) &= \max(\operatorname{mrv}(f), \operatorname{mrv}(g)),\\
\operatorname{mrv}(f^c) &= \operatorname{mrv}(f),\\
\operatorname{mrv}(\log f) &= \operatorname{mrv}(f),\\
\operatorname{mrv}(e^f) &= \operatorname{mrv}(f) \quad \text{if } f \text{ does not tend to } \infty,\\
&= \max(e^f, \operatorname{mrv}(f)) \quad \text{otherwise},\\
\operatorname{mrv}(x) &= x.
\end{aligned}$$

To compute this, the comparison of f and g is done by computing the limit of $\log|f|/\log|g|$, except when $f = x$ or $g = x$. In this case, x is first replaced by $\exp(x)$ throughout both expressions.

Rewriting. All the elements of the set returned by mrv have the same order of growth. In this step all the elements are rewritten in terms of one of them, possibly multiplied by functions with a smaller order of growth.

Expansion. Once the "most rapidly varying term" ω has been found, a Puiseux expansion of the expression in the variable ω is computed. The other terms are considered as harmless parameters. This is then repeated recursively on the leading coefficient if the exponent of ω is 0 and thus does not permit to conclude.

It can be shown that the algorithm based on these steps terminates, and reduces the problem of computing limits to the problem of deciding whether an exp-log function is zero or not.

3. Extensions

Some extensions to accommodate more that exp-log functions are possible, but are limited by the inability to decide or compute heuristically whether an expression of the class is zero or not.

4. Comment

Let us give a brief comparison with J. Shackell's algorithm. Shackell's algorithm drawback is that the rewriting into nested forms can lead to very large expressions, while the Gonnet-Gruntz algorithm can content itself with rougher rewritings. On the other hand, in Shackell's algorithm the difficult step of finding the "right" scale is done only when a sum is encountered, and the expansion is performed directly in the right scale instead of going from the finest one to the right one recursively, which is what the Gruntz-Gonnet algorithm does. Neither complexity analysis nor serious testing of these algorithms have been done, but it is certainly not obvious that the new algorithm is more efficient than the older one. In any case, it seems that a faster one could be devised by merging some ideas of both of them.

Bibliography

[1] Gonnet (Gaston H.) and Gruntz (Dominik). – *Limit Computation in Computer Algebra.* – Technical Report n° 187, ETH, Zürich, November 1992.

[2] Shackell (John). – Growth estimates for exp-log functions. *Journal of Symbolic Computation*, vol. 10, December 1990, pp. 611–632.

Introduction to symbolic integration

Bruno Salvy
INRIA Rocquencourt

March 22, 1993

[summary by Daniel Augot]

1. General Introduction

Scientific community is becoming aware of the power and utility of symbolic computations softwares. One of the most surprising achievements of these programs is the ability to perform formal integration, that is:

Given a function $f(z)$ (possibly with parameters), find a function $F(z)$ such that:

$$F'_z(z) = f(z). \tag{1}$$

Most mathematical students have learned how to find such primitives, generally with heuristics. The important point here is that symbolic softwares (like Maple) use *algorithms* which can:

(1) prove or disprove that the primitive of $f(z)$ can be expressed with elementary functions;
(2) find a solution to problem (1).

It is these techniques that we want to introduce here.

Our main interest will be the integration of rational functions and of purely transcendental functions (this will be made more precise later). We will focus on the integration of rational functions first, as the main algorithm can be derived (in structure) from this basic case. We consider that we have some basic tools "at hand", which are common to symbolic softwares. This toolkit includes gcd operations, extended Euclidean algorithm, and some linear algebra techniques.

2. Rational Functions

We want to solve the following problem: given $F \in \mathbb{Q}(z)$, we want to find $\int F$. As a preliminary step, we can write

$$F = P + \frac{Q}{R}$$

where P, Q, R are polynomials, Q and R are coprime and $\deg Q < \deg R$. The polynomial P can be easily integrated, so the remaining task is to compute a primitive of Q/R.

2.1. Structural approach. From the theoretical point of view, the following theorem is well known.

THEOREM 1. *Let $R = \prod_{i=1\ldots n}(z-a_i)^{n_i}$ be the factorisation of R, the fraction Q/R can be written*

$$\frac{Q}{R} = \sum_{i=1\ldots n} \frac{B_i}{(z-a_i)^{n_i}}, \qquad B_i \in \mathbb{Q}[z], \qquad \deg B_i < n_i.$$

We can rewrite this sum

$$\frac{Q}{R} = \sum_{i=1\ldots n} \sum_{j=1\ldots n_i} \frac{b_{i,j}}{(z-a_i)^j}, \qquad b_{i,j} \in \mathbb{Q}.$$

Then the primitive of Q/R is

$$\int \frac{Q}{R} = \sum_{i=1\dots n} b_{i,j} \log(z-a_i) - \sum_{i=1\dots n} \sum_{j=2\dots n_i} \frac{b_{i,j}}{(j-1)(z-a_i)^{j-1}}.$$

This gives some insight about the result: the simple factors of the denominator give logarithms in the result, while multiple factors give rational functions. However, this formula is not practicable, for many reasons:

> The factorization of R has to be known, and it is not easy to compute. We shall see that it is not needed in practice.
> Furthermore, this factorisation gives rise to algebraic numbers, whose use is expensive. One rule in computer algebra is "stay in $\mathbb{Q}$ as most as possible".

Consider the following rewriting of Q:

$$F = P + \frac{A}{D} + \frac{B}{E} \tag{2}$$

where A,B,D,E,P are polynomials in $\mathbb{Q}[z]$, D is square-free, and E has only multiple factors. We want to deal separately with A/D, which leads to logarithmic terms, and with B/E which leads to rational functions.

We recall that the square-free decomposition of a polynomial P is the decomposition

$$P = P_1 P_2^2 \cdots P_m^m$$

where the polynomials $P_1, \dots, P_m$ are pairwise coprime, and each P_i is square-free. We shall call m the *highest multiplicity* of P. This decomposition is not hard to compute, using differentiation of polynomials and gcd operations (Consider it as given in the basic toolkit).

In fact the algorithm computes step by step:

$$F = Q' + \left(\frac{\tilde{A}}{\tilde{D}}\right)' + \frac{\tilde{B}}{\tilde{E}},$$

such that the highest multiplicity of $\tilde{E}$ has been decreased, so that we have to solve the same problem with lower highest multiplicity, until we are left with a fraction whose denominator is square-free.

This process of decreasing the highest multiplicity of the denominator is called the *Hermite reduction*, which gives the rational part, and the logarithmic part (for a square-free denominator) is found by the method of the *Rothstein-Trager* resultant.

2.2. The Hermite reduction. The algorithm dates back to Hermite. We sketch a modern version due to Mack. We present the iterative step of the method.

Input P/Q, $\deg P < \deg Q$, $\gcd(P,Q) = 1$, the highest multiplicity of Q being $m > 1$.

Output $R, B, E \in \mathbb{Q}[X]$ such that $P/Q = (R)' + B/E$, the highest multiplicity m' of E being lower than m.

- Obtain a square-free decomposition of Q, and define G and $G^\star$ as shown:

$$Q = Q_1 Q_2^2 \cdots Q_m^m = Q_1 \underbrace{(Q_2 Q_3 \cdots Q_m)}_{G^\star} \underbrace{Q_2 Q_3^2 \cdots Q_m^{m-1}}_{G}$$

- Compute $QG'/G^2 = Q_1 G^\star G'/G$, which can be seen to be prime to $G^\star$.
- Using the extended Euclidean algorithm, compute the Bezout coefficients A, B of P:

$$P = AQ_1 \frac{G^\star G'}{G} + BG^\star$$

This leads to

$$\frac{P}{Q} = -\left(\frac{A}{G}\right)' + \frac{A'Q_1 + B}{Q_1 G}.$$

– Return $R = -A/G$, $B = A'Q_1 + B$, $E = Q_1 G$. The highest multiplicity of E is now at most $m-1$.

EXAMPLE. We consider the following function

$$f = \frac{z^7 - 24z^4 - 4z^2 + 8z - 8}{z^8 + 6z^6 + 12z^4 + 8z^2} = \frac{P}{Q}$$

Using this algorithm:

$$\begin{aligned} G &= \gcd(Q, Q') = z^5 + 4z^3 + 4z \\ Q_1 G^\star &= Q/G = z^3 + 2z \\ \gcd(G, G^\star) &= z^2 + 2 \\ Q_1 &= (Q_1 G^\star)/(G/\gcd(G, G')) = 1 \\ Q_1 G^\star G'/G &= 5z^2 + 2. \end{aligned}$$

By Bezout, we have $P = -(8z^2+4)(5z^2+2) + (z^4 - 2z^2 + 16z + 4)(z^3 + 2z)$. Thus

$$f = \left(\frac{8z^2+4}{z^5+4z^3+4z}\right)' + \frac{z^4 - 2z^2 + 4}{z^5 + 4z^3 + 4z}.$$

Again, for the second term, the algorithm gives:

$$\begin{aligned} G &= z^2 + 2 \\ Q_1 G^\star &= Q/G = z^3 + 2z \\ \gcd(G, G^\star) &= 1 \\ Q_1 &= z \\ Q_1 G^\star G'/G &= 2z^2. \end{aligned}$$

We get the Bezout coefficients $z^4 - 2z^2 + 4 = -3(2z^2) + (z^2+2)(z^2+2)$. Eventually:

$$f = \left(\frac{8z^2+4}{z^5+4z^3+4z} + \frac{3}{z^2+2}\right)' + \frac{1}{z}$$

2.3. The Hurwitz-Ostrogradsky method. It is possible to compute directly the result by the following remark. The aim is to compute

$$\frac{P}{Q} = \left(-\frac{A}{G}\right)' + \frac{C}{Q_1 \cdots Q_m}$$

i.e.

$$P = AQ_1 \frac{G^\star G'}{G} - A' Q_1 G^\star + CG$$

with the conditions: $\deg A < \deg G$, $\deg C < \deg(Q_1 G^\star)$. This is a linear system in the coefficients of A and C, which can be directly solved by a linear solver (again in the basic machinery of the toolkit).

2.4. The logarithmic part. Now it remains to solve the problem for a fraction $f = P/Q$, where Q is square-free. At this point two difficulties must be pointed out. Consider the example

$$f = \frac{5z^4 + 60z^3 + 255z^2 + 450z + 275}{z^5 + 15z^4 + 85z^3 + 225z^2 + 274z + 120}, \tag{3}$$

whose primitive is

$$\frac{25}{24}\log(z+1) + \frac{5}{6}\log(z+2) + \frac{5}{4}\log(z+3) + \frac{5}{6}\log(z+4) + \frac{25}{24}\log(z+5),$$

given in expanded form. If the factors where factored in simple logarithm, it would be the logarithm of a degree 120 polynomial, with coefficients of order 10^{68}. So the problem of the growth of intermediate numbers is present here.

The other difficulty is that algebraic numbers may be required in the solution, as shown by the example:

$$\int \frac{dz}{z^2-2} = \frac{\sqrt{2}}{4}\log\frac{z-\sqrt{2}}{z+\sqrt{2}}.$$

Then the problem is to compute in the extension of $\mathbb{Q}$ of lowest degree.
The method of Rothstein-Trager gives a good solution. Consider

$$f = \frac{P}{Q} = \sum_{i=1\ldots n} \frac{a_i}{z-\alpha_i}.$$

- One can check that $a_i = P(\alpha_i)/Q'(\alpha_i)$, thus the polynomials Q and $P - a_iQ'$ have a common root α_i. So a_i is a root of $R = \mathrm{Res}_z(Q, P - tQ')$ which belongs to $\mathbb{Q}[t]$. (Res_z stands for the *resultant in* z, another basic tool, which gives algebraic conditions on coefficients for two polynomials in z to have a common root.)
- Then α_i is a root of $G_i = \gcd(Q, P - a_iQ')$ which belongs to $\mathbb{Q}(a_i)[z]$. These roots can be collected for each a_i: for each such a_i, the answer is

$$a_i \sum_{\alpha_j | G_i(\alpha_j)=0} \log(z-\alpha_j) = a_i \log(G_i).$$

- The final answer is

$$\int \frac{P}{Q} = \sum_{a|R(a)=0} a\log(\gcd(Q, P - aQ')).$$

It must be pointed out that this is the expression of the primitive in the lowest degree extension of $\mathbb{Q}$.

Example. We consider the function f given by (3).We have $\mathrm{Res}_z(Q, P-tQ') = (5-4t)(6t-5)^2(24t-25)^2$, and

$$\int f = \frac{5}{4}\log(z+3) + \sum_{\alpha\in\{\frac{25}{24},\frac{5}{6}\}} \alpha\log(z^2+6z+20-72\frac{\alpha}{5}).$$

3. Elementary functions

3.1. Definition. The classical definition of elementary functions, after Liouville's work, is:

Definition 1. Let K be a differential field, y is said to be *elementary* over K if $K(y)$ and K have the same field of constants, and if

(1) either y is algebraic over K,
(2) or there exists $f \in K$ such that $f' = fy'$ (i.e. y is some kind of logarithm),
(3) or there exists $f \in K$ such that $y' = yf'$ (i.e. y is an exponential).

Now the following theorem gives an important characterization of functions which admit an elementary primitive:

Theorem 2 (Liouville). *Let K be a differential field, and C be the field of constants of K, $f \in K$ admits an elementary primitive over K if and only if f can be written*

$$f = v' + \sum_{i=1}^{m} c_i \frac{u_i'}{u_i}$$

where $v \in K$, $c_i \in \overline{C}$, $u_i \in K$.

The integration algorithm in the case of algebraic functions relies on a much more difficult theory, which borrows some tools from algebraic geometry. It is not within the scope of this talk to explain these. So we shall restrict ourselves to transcendental functions, which are amazingly simpler to deal with.

3.2. The strategy of Risch's algorithm; transcendental case. The Risch algorithm appears to be a slight generalisation of the method we have described here for the case of rational functions. We give here Bronstein's version of Risch's algorithm, in the transcendental case:

- Find a tower of extensions of $\mathbb{Q}$ given by $\theta_1 = z, \theta_2, \ldots, \theta_k$ such that θ_i is elementary over the previous field $\mathbb{Q}(\theta_1, \ldots, \theta_{i-1})$ for every i, and such that $f \in \mathbb{Q}(\theta_1, \ldots, \theta_k)$. We note $\theta = \theta_k$.
- Write $f = A(\theta)/D(\theta)$, with $A, D \in \mathbb{Q}(\theta_1, \ldots, \theta_{k-1})$.
- Split D into $D = D_s D_n$, where D_s is the product of the square-free factors F of D such that $\gcd(F, F') \neq 1$. We rewrite the function f as follows
$$f = P + \frac{B}{D_s} + \frac{C}{D_n} = f_p + f_s + f_n.$$
Here f_p is called the polynomial part, f_s is the special part, and f_n the normal part.
- A more general case of Hermite's reduction is applied, to eliminate all factors of the denominators whose highest multiplicity is greater than 1. This gives
$$f = f_p + g' + h$$
where the denominator of h has no multiple factors.
- A Rothstein-Trager resultant is computed to find the logarithmic part (or to decide it does not exists).
- The polynomial part f_p is integrated by an appropriate method, whether y is a logarithm or an exponential.

It is understood that it is a recursive method, since an effective method for the case $k = 1$ (i.e. a simple extension) gives a method for the general case, where computations are performed is some tower of extension, where arithmetic is effective, and primitives recursively computed.

3.3. More details. Now we give details about the main steps of Risch's algorithm. For constructing the extension tower, and finding the primitive of the special part, see the references.

3.3.1. The Hermite reduction We are concerned with the normal part A/D_n, which we would like to rewrite $A/D_n = g' + P + B/Q_n$, where Q_n has no multiple factors. As before we describe a single step of the method, for reducing the highest multiplicity at least by one.

Let V^{k+1} be the highest exponent in the square-free decomposition of D_n, that is $D_n = UV^{k+1}$, where V is square-free, $\gcd(U, V) = 1$ and the highest multiplicity of U is less than k.

We seek two polynomials $G, H \in K[\theta]$, such that $\deg G < \deg V$ and
$$\frac{A}{UV^{k+1}} = \left(\frac{G}{V^k}\right)' + \frac{H}{UV^k}.$$
(Remember that our goal is to lower the highest multiplicity of the denominator.) A small computation gives the relation $A = UVG' - kUV'G + VH$, and modulo V, we have
$$G = -\frac{A}{kUV'} \mod V.$$
Again we pick in our basic toolkit the extended Euclidean algorithm to compute $A/kUV' \bmod V$. H is easily computed from the data of A, U, V, G, k.

Example. Consider
$$f = \frac{z - \tan(z)}{\tan^2(z)} \in \mathbb{Q}(z)(\theta),\ \theta' = 1 + \theta^2.$$
The following equation is to be solved for $G, H \in \mathbb{Q}(z)[\theta], \deg G < 1$:
$$\frac{z - \theta}{\theta^2} = \left(\frac{G}{\theta}\right)' + \frac{H}{\theta}.$$

This leads to $G = -z \mod \theta$, and $H = -\theta z$, thus $f = (-z/\theta)' - z$ and $\int f = -z/(\tan z) - z^2/2$.

3.3.2. The Rothstein-Trager resultant We consider $f = f_p + f_s + G/D$, where D is square-free. Again we consider

$$R(z) = \mathrm{Res}_\theta(G - zD', D).$$

The function f has an elementary primitive if and only if $R(z) = \beta P(z)$, where $\beta \in K$ and $P \in K[z]$ is a monic polynomial with constant coefficients. It may happen that the coefficients of $R(z)$ have a non-zero derivative, in which case f has no elementary primitive.

The logarithmic part of the primitive is

$$\int \frac{G}{D} = \sum_{\alpha | R(\alpha)=0} \alpha \log(\gcd(G - \alpha D', D)).$$

3.3.3. Polynomials parts

First we describe the method for a polynomial in $\log(u(z))$. Consider

$$f_p = a_m(z)\log^m u(z) + a_{m-1}(z)\log^{m-1} u(z) + \cdots + a_1(z)\log u(z) + a_0(z).$$

The Liouville principle implies that, if f_p admit a primitive, f_p can be written

$$f_p = \sum_{i=0}^{m} a_i(z)\log^i(z) = \left(\sum_{i=0}^{n} b_i \log^i u(z)\right)' + \sum_{i=1}^{k} \frac{c_i v_i'}{v_i}$$

Identification gives

$$\begin{aligned} 0 &= B_{m+1}', \\ A_i &= B_i' + (i+1)B_{i+1}\frac{u'}{u}, \quad 1 \le i \le m. \end{aligned}$$

Thus each B_i' can be iteratively computed, and again each B_i' is integrated by a recursive application of the algorithm, and is found up to a constant. Furthermore, by identification, the constant of B_{i+1} is found.

Example.

$$F = \left(\frac{3}{2z} + \frac{1}{\log(z+\frac{1}{2})} - 2\frac{2z}{(2z+1)\log(z+\frac{1}{2})}\right)\log^2(z) + \frac{2\log z}{\log(z+\frac{1}{2})} + \frac{2}{(2z+1)\log(z+\frac{1}{2})}$$

We let $\tau = \log(z+1/2)$, and $\theta = \log z$, such that $F = A_2\theta^2 + A_1\theta + A_0$, $A_i \in \mathbb{Q}(z,\tau)$. A primitive has the form $B_2\theta^3 + B_2\theta^2 + B_1\theta + B_0 + \sum c_i v' i/v_i$ and:

(1) $B_3' = 0$ thus $B_3 = b_3 \in \overline{\mathbb{Q}}$.
(2) $A_2 = B_2' + 3B_3\theta'$. Recursively we get $\int A_2 = 3\theta/2 + z/\tau$, this implies $b_3 = 1/2$ and $B_2 = z/\tau + b_2$.
(3) $A_1 - 2/\tau = B_1' + 2b_2\theta'$. Again we get $\int A_1 - 2/\tau = 0$ and $b_2 = 0$, $B_1 = b_1$.
(4) $A_0 = B_0' + b_1\theta' + \sum c_i v_i'/v_i$. $\int A_0 = \log\log(z+1/2)$, thus $b_1 = 0$, B_0 is a constant, and $c_1 = 1$, $v_1 = \tau$.

In the end, $\int F = \log(z)^3/2 + z\log^2(z)/\log(z+1/2) + \log\log(z+1/2)$.

We explain the algorithm for a polynomials in exponential terms: let f_p be

$$f_p = a_m(z)\exp(mu(z)) + a_{m-1}(z)\exp((m-1)u(z)) + \cdots + a_{-p}(Z)\exp[-pu(z)].$$

The Liouville principle implies that the primitive is of the form $\sum_{i=-p}^{m} b_i(z)\exp(iu(z))$, with

$$b_i' + iu'b_i = a_i$$

which is called the Risch differential equation. This equation can be solved without difficulty since only rational solutions are required.

EXAMPLE. $\int e^{-z^2}$. The Risch differential equation is

$$b'(z) - 2zb(z) = 1$$

for which a rational solution is to be found. Because there is no pole in the coefficients of the equation and the leading coefficient is constant, $b(z)$ has no pole, and so must be a polynomial. But degree constraints show this equation has no polynomial solution. Conclusion: $\int e^{-z^2}$ is not elementary.

Bibliography

[1] Bronstein (Manuel). – Symbolic integration, 1993. Book in preparation.
[2] Davenport (J. H.), Siret (Y.), and Tournier (E.). – *Calcul formel.* – Masson, Paris, 1986.
[3] Geddes (Keith O.), Czapor (Stephen R.), and Labahn (George). – *Algorithms for computer algebra.* – Kluwer, 1992.

Summation of series solutions of linear differential equations

Michèle Loday-Richaud
Université d'Orsay

April 5, 1993

[summary by Bruno Salvy]

Introduction

It is very rare that a linear differential equation with analytic coefficients admits a closed-form solution. However, a lot of local informations can be obtained directly from the equation. For instance, it is well known that at an ordinary point the Taylor series of a solution can be computed by undeterminate coefficients. It is also possible to compute formal local expansions of the solutions of a linear differential equation, or equivalently a first order linear system, in the neighbourhood of a singularity.

Singularities are found to be either poles of the coefficients or roots of the coefficient of highest order. Suppose the singularity of the equation is at the origin, or you move it there by a change of variable. Then a fundamental object to compute is the *Newton polygon*. It is obtained by taking the upper-left convex hull of the set of points $(i, j-i)$ such that $x^j \partial^i$ appears with a non-zero coefficient in the Taylor series of the differential equation. On the Newton polygon one can read whether the singular point is *regular* or *irregular*. In the former case the polygon has only one edge which is horizontal, while it has several ones in the latter case. This distinction corresponds to very different formal solutions.

When the point is ordinary the power series obtained by substitution form a basis of *convergent* series solutions. When the point is a regular singular point, one can obtain a basis of formal solutions of the form

$$\sum f_{i,j}\, x^{\lambda_i} \log^j x,$$

where the $f_{i,j}$ are convergent power series and the λ_i are algebraic numbers. When the singularity is irregular, the formal solutions look like

$$\sum \hat{f}_{i,j,k} x^{\lambda_i} \log^j x\, e^{q_k(1/x)},$$

where the $\hat{f}_{i,j,k}$ are formal power series that are usually divergent, and the q_k are polynomials in some rational power of x.

The question naturally arises of "computing" actual solutions from these series. In the ordinary and regular singular cases, there is no theoretical difficulty since the series converge in the neighbourhood of the origin. In the divergent case the Main Asymptotic Existence Theorem asserts that each formal expansion is the asymptotic expansion of an actual solution in some angular sector of sufficiently small amplitude. Unfortunately, in a small sector there are also *flat* analytic functions whose power series expansion at the origin is 0. The problem of summability is to find a good way to associate a distinguished function to a formal solution while preserving good properties. In the process, one finds explicit formulæ that permit numerical computations of the solutions.

1. The Laplace-Borel method

Given a divergent formal power series $\hat{f} = \sum a_n x^{n+1}$, the Laplace-Borel method in a direction d consists in first applying a *Borel transform* to $\hat{f}$, transforming it into $\phi(\xi) = \sum \frac{a_n}{\Gamma(n+1)} \xi^n$, continuing ϕ analytically

along d, and then applying a *Laplace transform* to ϕ, yielding

$$f(x) = \int_d \phi(\xi) e^{-\xi/x}\, d\xi.$$

When this method works, the resulting function f is an actual solution of the linear differential equation of which $\hat{f}$ was a formal solution. From this expression it is possible to compute numerical values (see [11]). When a series is Laplace-Borel summable for almost all directions d, it is said to be Laplace-Borel summable.

For this method to work, it is necessary that ϕ be a convergent series and that its analytic continuation on a sector containing the direction d have an exponential growth of order at most 1 at infinity. A sufficient condition for this to work is that the series is a solution of a differential equation whose Newton polygon has only one oblique edge, with slope 1.

Unfortunately this method does not apply to all the formal solutions of linear differential equations and has to be generalized to k-summability and multisummability.

2. k-summability

A formal power series $\sum a_n x^n$ is defined to be *k-Gevrey* when $\sum a_n x^n/\Gamma(1+n/k)$ is convergent. A holomorphic function f on an open set V with vertex 0 is said to be *asymptotically k-Gevrey* on V if there exist a formal power series $\hat{f} = \sum a_n x^n$, and two real numbers A and K such that for any positive integer N the following inequality holds uniformly in V

$$|f(x) - \sum_{n<N} a_n x^n| \leq K\Gamma(1+\frac{N}{k}) A^n |x|^n.$$

In this case $\hat{f}$ is necessarily k-Gevrey.

A formal power series $\hat{f}(x)$ is said to be *k-summable* in direction d when $\hat{g}(t) = \hat{f}(t^{1/k})$ is Borel-Laplace summable in direction d. The method to resum these series is to substitute $t^{1/k}$ by x, then apply the Laplace-Borel method (extended so as to accomodate ramified series), and then replace back $t^{1/k}$ by x. While doing this it is necessary to be careful about directions of integration and amplitude of domains. This methods applies when the series is solution of a linear differential equation whose Newton polygon has only one oblique edge, with slope k.

3. Multisummability

Not all formal series solutions of linear differential equations are k-summable for some k. For instance if $k_1 \neq k_2$, and f_1 and f_2 are respectively non-convergent k_1 and k_2-summable series in direction d, then f_1+f_2 is not k-summable in direction d for any value of k. The main theorem [2, 9] is that all the elements of the differential algebra generated by f_1 and f_2 can be written as a sum of a k_1 and a k_2-summable series. This extends to algebras generated by more than two series. Such series are called *multisummable* of levels $(k_1, k_2, \ldots)$ in direction d. Although the representation of a divergent series as an element of this differential algebra is not unique, it can be shown that by resumming each of the series by its k-Borel-Laplace method in direction d and summing the results yields a result which depends only on the initial series and on d. Besides, the values $k_1, k_2, \ldots$ can all be deduced from the slopes of the Newton polygon of an equation having the series as solution.

The next problem is that this decomposition is not given by the above theorems. To actually compute the sum, two methods are known.

3.1. Ecalle's acceleration method. Suppose that $\hat{f} = \hat{f}_1 + \hat{f}_2$, with f_1 k_1-summable and f_2 k_2-summable in direction d. It is impossible to apply successively k_1 and k_2 summability in direction d, because the asymptotic growth of the k_1-Borel transform of $\hat{f}$ is too fast. Instead of this, the idea [5, 6, 7] is to compute

an operator which performs simultaneously the k_1-Laplace transform and the k_2-Borel transform ($k_1 < k_2$). This operator is called *Ecalle accelerator*. Its value is

$$\mathbf{A}_{(k_1,k_2)}(\phi)(\xi_2) = \int_d \frac{1}{\xi_2^{k_2}} \phi(u)\, \mathcal{C}_{k_2/k_1}\big[(\frac{u}{\xi_2})^{k_1}\big]\, du, \quad \text{where} \quad \mathcal{C}_a(\xi) = \frac{1}{2i\pi} \int_{\mathcal{H}} e^{v-\xi v^{1/a}}\, dv,$$

and $\mathcal{H}$ is a Hankel contour. Apart from the case $a = 2$ these are new special functions.

This method applies to any finite number of summands.

3.2. Balser's method. This method [3] first computes the κ_1 and κ_2-Borel transforms, and then all the corresponding κ-Laplace transforms in reverse order. The values of the κ's are related to the previous values of k by

$$\frac{1}{\kappa_p} = \frac{1}{k_p}, \qquad \frac{1}{\kappa_j} = \frac{1}{k_j} - \frac{1}{k_{j+1}} \quad (j < p).$$

Here also, the sum depends only on the initial formal power series, and it happens to be the same as given by Ecalle's method.

Final comments

Most of the proofs of these theorems involve highly sophisticated tools in algebra and analysis. The reader who wants to see more of it should consult the references.

Bibliography

[1] Balser (W.), Braaksma (B. L. J.), Ramis (J.-P.), and Sibuya (Y.). – Multisummability of formal power series solutions of linear ordinary differential equations. *Asymptotic Analysis*, vol. 5, 1991, pp. 27–45.

[2] Balser (Werner). – A different characterization of multi-summable power series. *Analysis*, vol. 12, 1992, pp. 57–65.

[3] Balser (Werner). – Summation of formal power series through iterated Laplace integrals. *Math. Scand.*, vol. 70, 1992, pp. 161–171.

[4] Balser (Werner). – Addendum to my paper on multisummable power-series. – Preprint, January 1993. Universität Ulm.

[5] Ecalle (J.). – *Introduction aux fonctions analysables et preuve constructive de la conjecture de Dulac.* – Hermann, 1992, *Actualités Mathématiques.*

[6] Loday-Richaud (Michèle). – Introduction à la multisommabilité. *Gazette des Mathématiciens*, vol. 44, April 1990, pp. 41–63.

[7] Loday-Richaud (Michèle). – Sommation des séries provenant de systèmes différentiels linéaires. – Journées X-UPS, 1991. Submitted to *Expositiones Mathematicae.*

[8] Malgrange (B.). – Introduction aux travaux de J. Ecalle. *L'Enseignement Mathématique*, 1984.

[9] Malgrange (B.) and Ramis (J.-P.). – Fonctions multisommables. *Annales de l'Institut Fourier*, vol. 42, n° 1-2, 1992, pp. 353–368.

[10] Ramis (J.-P.). – Equations différentielles : phénomène de Stokes et resommation. *Comptes-Rendus de l'Académie des Sciences*, vol. 301-I, n° 4, 1985, pp. 99–102.

[11] Thomann (Jean). – Resommation des séries formelles. Solutions d'équations différentielles linéaires du second ordre dans le champ complexe au voisinage de singularités irrégulières. *Numerische Mathematik*, vol. 58, 1990, pp. 503–535.

[12] Wasow (W.). – *Asymptotic Expansions for Ordinary Differential Equations.* – Dover, 1987. A reprint of the John Wiley edition, 1965.

The exclusion algorithm

Jean-Claude Yakoubsohn
Université Paul Sabatier, Toulouse

March 8, 1993

[summary by François Morain]

1. Introduction

Most numerical algorithms that look for the roots of a polynomial P over a field $\mathbf{K}$ first try to find subsets of $\mathbf{K}$ that contain just one root of P. Then, some sort of refining algorithm is used to get a more accurate value of the roots of P (e.g., Newton's algorithm). For this, we refer to [3].

The exclusion algorithm, on the contrary, eliminates large regions of K that do not contain any root of P. After this, the refining algorithms are used in the subsets that were found to have roots of P.

First of all, we describe the exclusion algorithm for computing real roots of polynomials. Then, we briefly describe the changes to be made when trying to localize hypersurfaces.

2. The exclusion algorithm in the 1-dimensional case

Let $P(x) = \sum_{k=0}^{d} a_k x^k$ be a polynomial in $\mathbb{R}[x]$, with $a_d \neq 0$. Let Z denote the (finite) set of real zeroes of $P(x)$. We suppose that we are given a positive real number ρ such that $Z \subset [-\rho, \rho]$. (Such a number can be computed using Cauchy's bound, see [4].) Let $\varepsilon > 0$ be any real number (the precision of the exclusion). The goal of the algorithm is to find a set F_ε such that

$$Z \subset F_\varepsilon \subset Z + [-K\varepsilon, +K\varepsilon]$$

where K is an absolute constant independent of ε.

2.1. The exclusion function. For $x \in \mathbb{R}$, let $M(x, r)$ be the polynomial

$$M(x,t) = |P(x)| - \sum_{k=1}^{d} \frac{|P^{(k)}(x)|}{k!} t^k.$$

It is easy to see that $M(x,t)$ is decreasing and concave, has a positive value in $t = 0$, and tends to $-\infty$ when t tends to $+\infty$, and therefore $M(x,t)$ has a unique positive root noted $m(x)$. We call $m(x)$ the *exclusion function* associated to $P(x)$. Let $d(x, Z)$ denote the distance from x to Z.

Proposition 1. *The function m has the following properties:*

(1) $m(x) = 0$ *if and only if* $P(x) = 0$;
(2) *if* $P(x) \neq 0$, *then* $]x - m(x), x + m(x)[\cap Z = \emptyset$;
(3) *for all* x, y *in* $\mathbb{R}$, $|m(x) - m(y)| \leq |x - y|$;
(4) *if* $Z \neq \emptyset$, *then there is a constant* $\alpha > 0$ *such that for all* x, $\alpha d(x, Z) \leq m(x) \leq d(x, Z)$.

2.2. A very simple exclusion algorithm. We start from $Z \subset [-\rho, \rho]$. The algorithm runs as follows:

```
function Exclusion(P, x, r, eps)

  if r < eps then return(]x-r, x+r[)
  else
    compute M(x, t)
    if M(x, r) < 0 then
      return(Exclusion(P,x-r/2,r/2,eps) union Exclusion(P,x+r/2,r/2,eps));

end.
```

We start with $\texttt{Exclusion}(P, 0, \rho, \varepsilon)$ and at each iteration, we determine whether $Z \subset]x-r, x+r[$ by testing whether $M(x, r) < 0$ or not. This trick is due to X. Gourdon who simplified the method given in [1, 2]. Note that this algorithm always stops as soon as we enter intervals of length less than ε.

A MAPLE implementation of this would simply be:

```
Exclusion := proc(P, X, x, r, eps) local mxt, d, k, t;
   if r < eps then RETURN((x-r)..(x+r)) fi;
   d:=degree(P, X);
   mxt:=0;
   for k to d do mxt:=mxt+abs(subs(X=x,diff(P,X$k)))*t^k/k! od;
   mxt:=abs(subs(X=x,P))-mxt;
   if subs(t=r, mxt) < 0 then
      RETURN(Exclusion(P,X,x-r/2,r/2,eps), Exclusion(P,X,x+r/2,r/2,eps))
   fi;
end:
```

If we try it on $P(X) = X^3 + X + 1$ and $\rho = 3$, we get:

```
> Exclusion(X^3+X+1,X,0.,3.,0.001);
          -.6826171876 .. -.6811523438, -.6811523438 .. -.6796875000
```

whereas

```
> fsolve(X^3+X+1);
                                -.6823278038
```

An iterative exclusion algorithm is given in [2], together with an analysis of the complexity of the algorithm. In particular, it is shown that the iterative version enables one to get

$$Z \subset F_\varepsilon \subset Z + [-K\varepsilon, +K\varepsilon]$$

with $K = 2/\alpha$ with α defined above. The complexity of the algorithm is then shown to be

$$O(d^2 |\log \varepsilon| + d |\log \varepsilon| \log |\log \varepsilon|).$$

3. Localization of hypersurfaces

Let $P(x)$ be a polynomial in $\mathbf{K}[x]$, where $x = (x_1, \ldots, x_n)$ with degree d. This time the set of zeroes of P need no longer be finite. We suppose first that Z has a point at infinity (which means we treat the affine case).

Put

$$M(x, t) = |P(x)| - \sum_{k=1}^{d} b_k t^k$$

with

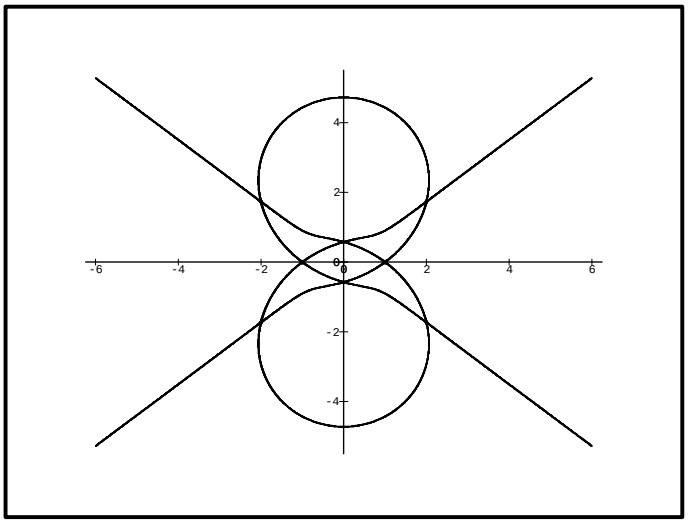
$$b_k = \frac{1}{k!} \sum_{1 \le i_1 \le \cdots \le i_k \le n} \left| \frac{\partial^k P(x)}{\partial x_{i_1} \cdots \partial x_{i_k}} \right|.$$

As in the 1-dimensionnal case, $M(x,t)$ is concave and decreasing, implying it has a unique positive root $m(x)$. We have:

PROPOSITION 2. (1) *$m(x) = 0$ if and only if $P(x) = 0$. Moreover x is a singular point of Z if and only if $m(x)$ is a root of $M(x,t)$ of multiplicity greater than 2;*
(2) *if $P(x) \neq 0$, then $B_o(x, m(x)) \cap Z = \emptyset$;*
(3) *$m(x)$ is continuous and semi-algebraic.*
(4) *let F be a semi-algebraic compact subset of $\mathbf{K}^n$. There is a constant $\alpha > 0$ and an integer $n_1 \neq 0$ such that for all $x \in F$, one has*

$$\alpha d(x,Z)^{n_1} \leq m(x) \leq d(x,Z).$$

Using this, we can write a very naïve program that localizes Z in a compact F. It is just the same algorithm as in the 1-dimensionnal case, where we replace the interval $]x-r, x+r[$ with the open ball $B_o(x,r)$ and we replace dichotomy in two subintervals by dichotomy in four regions of the plane (in the case $\mathbf{K} = \mathbb{R}^2$).



The resulting algorithm has been programmed by Bruno Salvy in MAPLE and gives very good results. For example, the curve of Gergueb, corresponding to

$$\begin{aligned} P(x,y) \quad = \quad & -7 + 9y^8 - 204y^6 + 70y^4 - 7x^8 + 28x^6 - 42x^4 + 28x^2 - 52x^2y^2 \\ & +68x^2y^4 + 20x^2y^6 + 44x^4y^2 + 6x^4y^4 - 12x^6y^2 + 20y^2 \end{aligned}$$

was drawn using MAPLE (see figure).

The reader interested in an iterative version of this algorithm, together with an analysis of its complexity is referred to [1].

Bibliography

[1] Dedieu (Jean-Pierre) and Yakoubsohn (Jean-Claude). – Localization of an algebraic hypersurface by the exclusion algorithm. *Applicable Algebra in Engineering, Communication and Computing*, vol. 2, 1992, pp. 239–256.
[2] Dedieu (Jean-Pierre) and Yakoubsohn (Jean-Claude). – Computing the real roots of a polynomial by the exclusion algorithm. *Numerical Algorithms*, vol. 4, 1993, pp. 1–24.

[3] Gourdon (Xavier). – *Algorithmique du théorème fondamental de l'algèbre.* – Technical Report n° 1852, Institut National de Recherche en Informatique et en Automatique, February 1993.

[4] Marden (M.). – Geometry of polynomials. In *AMS Surveys.* – AMS, second edition, 1966.

Construction d'intégrateurs symplectiques pour des mouvements kepleriens

Pierre-Vincent Koseleff
Aleph et Géode
Centre de Mathématiques
École polytechnique

26 avril 1993

[résumé par Stéphane Gaubert]

1. Introduction

On s'intéresse à l'intégration numérique du système hamiltonien:

$$(q,p) \in \mathbb{R}^{2n}, \quad \dot{p_i} = -\frac{\partial H}{\partial q_i}, \qquad \dot{q_i} = \frac{\partial H}{\partial p_i} \tag{1}$$

avec $H = H(p,q,t)$. Dans le cas où H ne dépend pas du temps, l'énergie (hamiltonien H) est constante au cours du mouvement, et le flot hamiltonien conserve la *forme symplectique*, c'est-à-dire que l'application $S_H(\tau)$ qui envoie la position (q,p) à $t=0$ sur (q',p') à $t=\tau$ satisfait

$$dp \wedge dq = dp' \wedge dq' \ .$$

Si l'on intègre naïvement le système (1), on perd ces propriétés. Considérons par exemple la méthode d'Euler sur un pas de temps τ, soit

$$q' = q + \tau \frac{\partial H}{\partial p}, \qquad p' = p - \tau \frac{\partial H}{\partial q} \tag{2}$$

Pour l'oscillateur harmonique de dimension 1, $H = \frac{1}{2}(p^2+q^2)$, l'énergie est multipliée par $(1+\tau^2)$ à chaque pas de l'intégration (2), i.e.

$$p'^2 + q'^2 = (1+\tau^2)(p^2+q^2)$$

et de même, la forme symplectique $dp \wedge dq$ (en l'occurrence l'aire infinitésimale dans l'espace des phases $\mathbb{R}^2$) est dilatée d'un facteur $1+\tau^2$. Cette non conservation d'invariants physiques par l'intégrateur devient d'autant plus sensible que l'on intègre sur un grand nombre de pas de temps (par exemple en mécanique céleste). Cela motive la recherche de schémas numériques d'intégration préservant soit l'hamiltonien, soit la forme symplectique. Ce sont ces derniers intégrateurs (dits *symplectiques*) que nous étudions ici.

2. Programme

Considérons le cas d'un hamiltonien du type énergie cinétique + énergie potentielle:

$$H = T(p) + V(q) \ . \tag{3}$$

La remarque essentielle est que la méthode d'Euler donne l'expression exacte des flots hamiltoniens S_T et S_V associés à T et à V, soient

$$S_T(\tau): \qquad q' = q + \tau \frac{\partial T}{\partial p}, \quad p' = p \tag{4}$$

$$S_V(\tau): \quad p' = p - \tau \frac{\partial V}{\partial q}, \quad q' = q \ . \tag{5}$$

Il est donc naturel de chercher un intégrateur pour le système d'hamiltonien H sous la forme

$$S^{(n)}(\tau) = S_T(c_1\tau)S_V(d_1\tau)\cdots S_T(c_n\tau)S_V(d_n\tau) \tag{6}$$

où les c_i, d_i sont des constantes choisies de sorte que $S^{(n)}(\tau)$ coïncide avec le flot hamiltonien $S_H(\tau)$ jusqu'à un ordre k convenable, i.e. $S^{(n)}(\tau) = S_H(\tau) + o(\tau^k)$. Le schéma (6) s'implémentera alors aisément via (4) et (5). Il sera par construction symplectique comme composé de flots hamiltoniens. La détermination des c_i, d_i conduit à des problèmes de calcul formel que nous considérons maintenant.

3. Méthodes de Lie

Introduisons les crochets de Poisson

$$\{f, g\} \stackrel{def}{=} f_q g_p - f_p g_q = \sum_{i=1}^{n} \frac{\partial f}{\partial q_i}\frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i}\frac{\partial g}{\partial q_i}$$

qui munissent les fonctions lisses sur l'espace des phases (i.e. $\mathbb{R}^{2n}$) d'une structure d'algèbre de Lie. En posant $z = (q, p) \in \mathbb{R}^{2n}$, les équations d'Hamilton (1) se réécrivent

$$\dot{z_i} = \{z_i, H\} \tag{7}$$

soit en introduisant la dérivation de Lie L_H:

$$L_H f \stackrel{def}{=} \{H, f\}$$

$$\dot{z_i} = -L_H z_i \ .$$

Dans le cas où H ne dépend pas du temps, on en déduit l'expression formelle

$$z(t) = \exp(-tL_H)z(0) \ .$$

Considérons à nouveau un Hamiltonien de type $T(p) + V(q)$. On a $L_H = L_T + L_V$. En posant $A \stackrel{def}{=} L_T$, $B \stackrel{def}{=} L_V$, la détermination d'un intégrateur symplectique de la forme (6) se ramène à satisfaire l'identité suivante entre séries formelles

$$\exp(-\tau(A+B)) = \exp(-c_1\tau A)\exp(-d_1\tau B)\cdots\exp(-c_n\tau A)\exp(-d_n\tau B) + o(\tau^k) \ . \tag{8}$$

Un telle identité rappelle la formule de Campbell-Haussdorf (qui affirme que $\ln(\exp(A)\exp(B))$ est une somme de monômes de Lie en A et B), en particulier les premiers termes de cette formule donnent

$$\exp(-\tau A)\exp(-\tau B) = \exp(-\tau(A+B) + \frac{\tau^2}{2}[A, B] + \cdots) = \exp(-\tau(A+B)) + o(\tau) \tag{9}$$

d'où il résulte immédiatement que $S_T(\tau)S_V(\tau) = \exp(-\tau A)\exp(-\tau B)$ est un intégrateur symplectique à l'ordre 1. Plus généralement, on peut obtenir les équations algébriques vérifiées par les c_i, d_i par l'une des trois méthodes suivantes:

Méthode directe. On développe les exponentielles et l'on identifie les termes de part et d'autre de (8).

Méthode de la fonction invariante. Par application répétée de la formule de Campbell-Haussdorf, on trouve une série formelle de Lie K en les indéterminées T et V (à coefficients dans $\mathbb{Q}[\tau, c_i, d_i]$) telle que

$$S_T(c_1\tau)S_V(d_1\tau)\cdots S_T(c_n\tau)S_V(d_n\tau) = \exp(-\tau L_{K(\tau)}) \quad . \tag{10}$$

Il reste à choisir les c_i, d_i pour que $K(\tau) = H + o(\tau^{k-1})$. On peut voir $K(\tau)$ comme l'Hamiltonien d'un système ayant pour opérateur d'évolution en temps τ l'intégrateur (6). En particulier, l'intégrateur (6) préserve l'hamiltonien $K(\tau)$ (i.e. $K(\tau, q', p') = K(\tau, q, p)$) proche à $o(\tau^{k-1})$ près de l'énergie du système, d'où le nom de fonction invariante.

Méthode de l'hamiltonien perturbé. Soit $S_u(t)$ une transformation symplectique vérifiant

$$\frac{\partial S_u}{\partial t} = -S_u L_u, \qquad S_u(0) = \mathrm{Id}$$

(c'est l'opérateur d'évolution associé à l'hamiltonien u, qui diffère de $\exp(-tL_u)$ lorsque u dépend du temps, S_u est aussi connu classiquement comme la "transformation de Lie" T_w associée à $w = \int u dt$ [2]). Soit S_v une autre transformation du même type. Il vient

$$\frac{\partial S_u S_v}{\partial t} = -S_u S_v L_{S_v^{-1}u+v} \quad ,$$

donc les transformations symplectiques de type S_u sont stables par composition, avec la loi

$$S_u S_v = S_{S_v^{-1}u+v} \quad . \tag{11}$$

A partir de là, on obtient $W = W(\tau)$ tel que

$$S_T(c_1\tau)S_V(d_1\tau)\cdots S_T(c_n\tau)S_V(d_n\tau) = S_W(\tau) \tag{12}$$

et l'on choisit les c_i, d_i pour que $W(\tau)$ soit une perturbation à $o(\tau^{k-1})$ près de H.

On montre que les trois méthodes conduisent au même résultat, i.e. fournissent le même idéal annulé par les c_i, d_i. D'un point de vue pratique, la méthode la plus simple est la troisième, qui s'effectue par application répétée de (11) sans recours à des identités exponentielles. L'implémentation de (11),(12) se fait commodément en décomposant le hamiltonien perturbé W sur la *base de Lyndon* [4, 5, 7, 3] de l'algèbre de Lie libre sur T, V.

On retrouve de la sorte l'intégrateur symplectique à l'ordre 2:

$$S_2(\tau) = S_T(\frac{\tau}{2})S_V(\tau)S_T(\frac{\tau}{2}) \tag{13}$$

bien connu par ailleurs. La méthode permet d'obtenir par exemple tous les intégrateurs symplectiques d'ordre 4, mais à partir de $k = 6$, le nombre d'équations algébriques déterminant les c_i, d_i devient trop grand pour pouvoir conclure. Cette limitation suggère de se restreindre aux intégrateurs ayant une structure particulière motivée par des considérations physiques.

4. Cas spéciaux

Intégrateurs réversibles. Un intégrateur S est dit *réversible* si $S(-t) = S(t)^{-1}$. Nous chercherons de tels intégrateurs sous la forme

$$S_R^{(n)}(\tau) = S_T(c_n\tau)S_V(d_n\tau)\cdots S_T(c_1\tau)S_V(d_1\tau)S_T(c_0\tau)S_T(d_1\tau)\cdots S_T(d_n\tau)S_T(c_n\tau) \tag{14}$$

ou encore plus particulièrement comme produit réversible d'intégrateurs du second ordre de type (13):

$$S_2(c_n t)\cdots S_2(c_1 t)S_2(c_0 t)S_2(c_1 t)\cdots S_2(c_n t) \quad . \tag{15}$$

En raffinant les méthodes de Lie décrites en §3, on obtient un recensement exhaustif des opérateurs symplectiques de ce type d'ordre petit ($k = 6$).

Énergie cinétique quadratique. Supposons maintenant que $T(p)$ soit quadratique (ce qui est en particulier le cas du mouvement keplerien qui motive cette étude). Alors, comme $\{\{T,V\},V\}$ ne dépend que de q, on a une formule exacte pour le flot associé à $V_1(\alpha,\beta) = \alpha V + \tau^2\beta\{\{T,V\},V\}$ (où α,β sont des constantes et τ est fixé), soit

$$S_{\alpha,\beta}(\tau): \quad (q,p) \to (q, p - \tau\frac{\partial V_1(\alpha,\beta)}{\partial q}) \ .$$

On trouve de manière analogue des intégrateurs symplectiques de la forme

$$S_{c_n,z_n}(\tau)S_T(d_n\tau)\cdots S_{c_1,z_1}(\tau)S_T(d_0\tau)S_{c_1,z_1}(\tau)\cdots S_T(d_n\tau)S_{c_n,z_n}(\tau)$$

pour un choix convenable des constantes c_i, z_i, d_i. Ces intégrateurs requièrent moins d'opérations élémentaires que les intégrateurs réversibles généraux précédemment décrits.

Bibliographie

[1] Channel (P. J.) et Scovel (J. C.). – Symplectic integration of Hamiltonian systems. *Nonlinearity*, vol. 3, 1990, pp. 231–259.

[2] Deprit (A.). – Canonical tranformations depending on a small parameter. *Celestial Mechanics*, vol. 1, 1969, pp. 12–30.

[3] Koseleff (P. V.). – *Calcul formel pour les méthodes de Lie en mécanique hamiltonienne.* – Thèse de doctorat, École polytechnique, 1993.

[4] Perrin (D.). – Factorization of free monoids. *In: Combinatorics on words*, éd. par Lothaire (M.). – Addison-Wesley, 1983.

[5] Reutenauer (C.). – *Free Lie Algebras.* – Clarendon Press, Oxford, 1993.

[6] Steinberg (S.). – Lie series, Lie transformations and their applications. *In: Lie Methods in Optics. Lecture Notes in Physics*, vol. 250. – Springer-Verlag, 1985.

[7] Viennot (G.). – *Algèbres de Lie libres et monoïdes libres.* – Springer-Verlag, 1978, *Lecture Notes in Mathematics*, vol. 691.

[8] Yoshida (H.). – Construction of higher order symplectic integrators. *Phisics Letter A*, vol. 150, 1990, pp. 262–268.

Part III

Asymptotic Analysis

Limit distributions and analytic methods

M. Drmota
University of Vienna

September 17, 1992

[summary by Michèle Soria]

Abstract

This paper presents a survey of analytic methods for estimating coefficients of functions in complex variables, and their application to obtain limit distributions in combinatorial structures. Two cases are specially investigated, with new results given: functional equations and product schemas.

1. Analytic Methods

Let $y(x) = \sum y_n x^n$, analytic at the origin, with $y_n \geq 0$; the coefficients can be evaluated by Cauchy's formula. Two types of well known methods are used according to the nature of $y(x)$.

1.1. Saddle point method. For functions with at least exponential growth, for example Hayman's admissible functions [14], the saddle point method applies:

$$y_n \sim \rho_n^{-n} \frac{y(\rho_n)}{\sqrt{2\pi\sigma_n^2}},$$

where the saddle point ρ_n satisfies $\frac{\partial}{\partial u} \log y(\rho_n e^u)\big|_{u=0} = n$, and $\sigma_n^2 = \frac{\partial^2}{\partial u^2} \log y(\rho_n e^u)\Big|_{u=0}$.

1.2. Singularity analysis. For functions with algebraic and logarithmic singularities, i.e. with local behaviour $y(x) = \frac{1}{(1-x)^\alpha} \log^\beta \frac{1}{1-x}$, $\alpha \in \mathbb{R} - \{-1, -2, \ldots\}$ and $\beta \in \mathbb{R}$, singularity analysis on a Hankel contour (Flajolet and Odlyzko [9]) gives

$$y_n \sim \frac{n^{\alpha-1}}{\Gamma(\alpha)} \log^\beta(n).$$

An interesting application of both methods is the asymptotics of coefficients of powers of generating functions: $[x^n]y(x)^k$, when both n and k tend to infinity.

- When $0 < a \leq k/n \leq b < \infty$, the saddle point of $y(x)^k$ stays in a bounded interval $[c, d], c > 0, d < \infty$, and the saddle point method gives an estimation which is uniform for $k/n \in [a, b]$. This result was proved by Daniels [4], and extended by Good [13]. The case $n = o(k)$ is studied by Gardy [12].
- When $k = o(n)$, the saddle point method does not apply, but singularity analysis can be used for some specialised functions $y(x)$. For example, Drmota [6, 8] shows that

$$[x^n](1 - \sqrt{1-x})^k \sim \frac{k}{2n^{3/2}\sqrt{\pi}}\, e^{-k^2/4n}, \quad \text{uniformly for} \quad k = o(\sqrt{n \log n}).$$

$$[x^n]\left(\log \frac{1}{1-x}\right)^k \sim \frac{\log^k n}{n\Gamma(k/\log n)}, \quad \text{uniformly for} \quad k = o((\log n/\log\log n)^2).$$

1.3. Multivariate functions. Let $y_{n_1,\dots,n_m} = [x_1^{n_1}\dots x_m^{n_m}]\, y(x_1,\dots,x_m)$.
The saddle point method applies for admissible functions:

$$y_{n_1,\dots,n_m} \sim \frac{y(\rho_1,\dots,\rho_m)}{\sqrt{(2\pi)^m}\sqrt{\det(\sigma_{jl}^2)}\,\rho_1^{n_1}\dots\rho_m^{n_m}},$$

with $\frac{\partial}{\partial u_j}\log y(\rho_1 e^{u_1},\dots,\rho_m e^{u_m})\Big|_{u=0} = n_j$, and $\sigma_{jl}^2 = \frac{\partial^2}{\partial u_j \partial u_l}\log y(\rho_1 e^{u_1},\dots,\rho_m e^{u_m})\Big|_{u=0}$.
For coefficients of powers of generating functions, the saddle point method also applies for

$$[x_1^{n_1}\dots x_m^{n_m}]\, y(x_1,\dots,x_m)^k$$

when $k/n_j \in [a_j, b_j]\,, a_j > 0$ [4].
When $k = o(n)$, singularity analysis can be used for some specialised functions $y(x_1,\dots,x_m)$. (See e.g. [7] for an illustration of a double Hankel contour.)

2. Generating Functions and Limit Distributions

To a class $\mathcal{A}$ of combinatorial structures is associated the generating function $a(x) = \sum a_n x^n$ (or $a(x) = \sum a_n x^n/n!$ in a labelled context), where a_n is the number of $\mathcal{A}$-structures of size n. The power of generating functions in combinatorics rests on the correspondence between classical combinatorial constructions and functional operators on generating functions. This mechanism is described by Flajolet in [15].

Additional parameters of structures, $\phi_i : \mathcal{A} \to N, i = 1,\dots,m$ can be handled with multivariate generating functions $a(x,z) = \sum a_{nk} x^n z^k$, where $z = (z_1,\dots,z_m)$ with $z^k = z_1^{k_1}\cdots z_m^{k_m}$, and a_{nk} is the number of $\mathcal{A}$-structures α of size n such that $\phi_i(\alpha) = k_i, i = 1,\dots,m$.

Consider the (discrete) random variables $X_n = (X_{n_1},\dots,X_{n_m})$ with probability distribution $\Pr(x_n = k) = a_{nk}/a_n$. The expected value $\mathrm{E}\,X_n = (\mathrm{E}\,X_{n_1},\dots,\mathrm{E}\,X_{n_m})$ is given by $\mathrm{E}\,X_{n_j} = \frac{1}{a_n}[x^n]a_{z_j}(x,1)$ and the covariance matrix $\mathrm{Cov}\,X_n = (\mathrm{E}\,X_{n_j}X_{n_l} - \mathrm{E}\,X_{n_j}\,\mathrm{E}\,X_{n_l})$ can be evaluated by $\mathrm{E}\,X_{n_j}^2 = \frac{1}{a_n}[x^n](a_{z_jz_j}(x,1) + a_{z_j}(x,1))$, and $\mathrm{E}\,X_{n_j}X_{n_l} = \frac{1}{a_n}[x^n](a_{z_jz_l}(x,1))$.
There are three typical cases for the limiting distribution:

- X_n tends to a discrete distribution;
- $X_n/\sqrt{|\mathrm{Cov}(X_n)|}$ tends to a one-sided continuous distribution;
- $(X_n - \mathrm{E}\,X_n)/\sqrt{|\mathrm{Cov}(X_n)|}$ tends to a normal distribution.

In each of these cases it is possible to find the limit distribution by use of the characteristic function $\Phi_{X_n}(t) = \mathrm{E}\,e^{itX_n}$. This approach gives the distribution function of the limit distribution (global limit theorem). A more accurate information can be obtained by explicit or uniform asymptotic formulae for the density a_{nk}/a_n (local limit theorem). The study of limiting distributions in combinatorial schemas, initiated by Bender [1], is being pursued by several authors [2, 3, 10].

3. Functional Equations

It is a well known result that the number of leaves in plane trees satisfies a Gaussian limit distribution. The generating function of plane trees is implicitly defined by $a(x) = \frac{x}{1-a(x)}$, and the bivariate generating function, with z marking the leaves is $a(x,z) = xz + \frac{x\,a(x,z)}{1-a(x,z)}$.

The result of this section shows that more generally, in generating functions defined by functional equations, Gaussian limit distributions are to be expected.

THEOREM 1. [5, 6] *Let $z = (z_1,\dots,z_m), m \geq 1$, and $a(x,z) = \sum a_{nk}x^n z^k$ a generating function of nonnegative numbers a_{nk} satisfying a functional equation $F(a,x,z) = 0$, where F is analytic in the "range of interest" (plus some minor assumptions on a_{nk} and F).*

Let $x_0, a_0 > 0$ be solutions (x_0 minimal) of

$$F(a_0, x_0, 1) = 0$$
$$F_a(a_0, x_0, 1) = 0$$

and suppose that $F_{aa}(a_0, x_0, 1)F_x(a_0, x_0, 1) > 0$.

Then the numbers a_{nk} *satisfy a* central limit theorem *with mean value* $E(X_n) = \mu.n + O(1)$, *where* $\mu = (\mu_1, \ldots, \mu_m)$ *is given by* $\mu_j = F_{z_j}(a_0, x_0, 1)/x_0 F_x(a_0, x_0, 1)$.

Furthermore let $\rho = (\rho_1, \ldots, \rho_m)$, *and* a_ρ, x_ρ, z_ρ *be the solution of*

$$\begin{aligned} F(a_0, x_0, 1) &= 0, \\ F_a(a_0, x_0, 1) &= 0, \\ z_j F_{z_j}(a, x, z) &= \rho_j \, x F_x(a, x, z), \end{aligned}$$

then the covariance matrix is given by $\operatorname{Cov} X_n = \sigma^2_{jl}(\rho).n + O(1)$, *where* $\sigma^2_{jl}(\rho) = G_{jl}(a_\rho, x_\rho, z_\rho)$ *and* G_{jl} *is expressed in terms of first and second derivatives of* F *w.r.t.* a, x, z_j, z_l.

Moreover let $\rho = \frac{k}{n} = \left(\frac{k_1}{n_1}, \ldots, \frac{k_m}{n_m}\right)$, *then the numbers* a_{nk} *satisfy a* local limit theorem:

$$a_{nk} = x_\rho^{-n} z_\rho^{-k} \, \frac{n^{-\frac{m+3}{2}}}{(2\pi)^{\frac{m+1}{2}} \sqrt{\det(\sigma^2_{jl}(\rho))}} \sqrt{\frac{x_\rho F_x(a_\rho, x_\rho, z_\rho)}{F_{aa}(a_\rho, x_\rho, z_\rho)}} \, (1 + O(1/n)) \,,$$

uniformly for k/n *in a compact set containing only positive components.*

Proof. The proof is in three steps. First the implicit function theorem gives a local representation of $a(x, z)$. Second extract the coefficient of x^n in $a(x, z)$ by singularity analysis. And finally use saddle point method to obtain the coefficient of $x^n z^k$ in $a(x, z)$. □

An application of the theorem to independent subsets of simply generated trees is given by Drmota [5]: the number of *independent subsets* (a subset of a tree is independent if two different nodes are not adjacent) has a normal limit distribution with asymptotic mean value $n/3$; and the number of *maximal independent subsets* (an independent subset is maximal if any node not contained in it is adjacent to a node contained in it) has a normal limit distribution with asymptotic mean value $n/2$.

4. Product Schemas

The analysis of functional composition $F(uw(x))$, that translates into generating functions the combinatorial operation of substitution, has been largely investigated [1, 3, 10, 11]. It leads to discrete, or normal, or special distributions, according to analytic properties of F and w. In the case of product schemas

$$y(x, u) = g(x)F(uw(x))$$

studied by Drmota and Soria [8], the limit distribution may be dictated either by $g(x)$, or by $F(uw(x))$, or it should involve both g and F.

The analytic criterion to distinguish between these cases is *singular order*. Let $f_1(x)$ and $f_2(x)$ be analytic at the origin, with non negative coefficients, we say that f_1 is of higher singular order than f_2 if either the radius of convergence of f_1 is smaller than the one of f_2, or f_1 and f_2 have the same radius of convergence and the saddle point of f_1 is asymptotically smaller than the one of f_2.

We always assume that the coefficients of the Taylor expansions of $g(x)$, $w(x)$ and $F(w(x))$ can be evaluated, by saddle point method or singularity analysis.

4.1. g **is dominated.** If $F(w(x))$ is of higher singular order than $g(x)$, and $w(x)$ is of higher or equal singular order than $g(x)$, then $g(x)$ is (usually) dominated in $y(x, u)$.

When g is dominated, the factor $g(x)$ has actually no influence over the limit distribution, i.e. the limit distribution of $y(x, u)$ is the same as the limit distribution of $F(uw(x))$.

4.2. g dominates. If $g(x)$ is of higher singular order than $F(w(x))$ and $F'(w(x))$, then $g(x)$ (usually) dominates in $y(x,u)$.

When g dominates there are only a few kinds of limit distributions, which can be classified in the following way.

- If $\lim_{x\to r-} w(x) = w(r)$ exists and $F(z)$ is regular at $w(r)$, then X_n (related to $y(x,u)$) has a discrete limit distribution.
- If $\lim_{x\to r-} w(x) = \infty$ and $F(z)$ is admissible, then X_n is asymptotically normally distributed.
- If $\lim_{x\to r-} w(x) = w(r)$ exists and $F(z)$ is singular at $z = w(r)$
  - if $F(z)$ is admissible then X_n is asymptotically normally distributed.
  - if $F(z)$ has an algebraico-logarithmic singularity, then X_n is asymptotically Gamma distributed.

Bibliography

[1] Bender (Edward A.). – Central and local limit theorems applied to asymptotic enumeration. *Journal of Combinatorial Theory*, vol. 15, 1973, pp. 91–111.

[2] Bender (Edward A.) and Richmond (L. Bruce). – An asymptotic expansion for the coefficients of some power series II: Lagrange inversion. *Discrete Mathematics*, vol. 50, 1984, pp. 135–141.

[3] Canfield (E. Rodney). – Central and local limit theorems for the coefficients of polynomials of binomial type. *Journal of Combinatorial Theory, Series A*, vol. 23, 1977, pp. 275–290.

[4] Daniels (H. E.). – Saddlepoint approximations in statistics. *Annals of Mathematical Statistics*, vol. 25, 1954, pp. 631–650.

[5] Drmota (Michael). – Asymptotic distributions and a multivariate Darboux method in enumeration problems. *Journal of Combinatorial Theory, Series A*. – To appear.

[6] Drmota (Michael). – A bivariate asymptotic expansion of coefficients of powers of generating functions. *European Journal of Combinatorics*. – To appear.

[7] Drmota (Michael). – The height distribution of leaves in rooted trees. *Discrete Math. Applications*. – To appear.

[8] Drmota (Michael) and Soria (Michèle). – Marking in combinatorial constructions and limit distributions 1: Generating functions and limit distributions. – Manuscript, November 1993.

[9] Flajolet (Philippe) and Odlyzko (Andrew M.). – Singularity analysis of generating functions. *SIAM Journal on Discrete Mathematics*, vol. 3, n° 2, 1990, pp. 216–240.

[10] Flajolet (Philippe) and Soria (Michèle). – General combinatorial schemas: Gaussian limit distributions and exponential tails. *Discrete Mathematics*, vol. 114, 1993, pp. 159–180.

[11] Flajolet (Philippe) and Soria (Michèle). – General combinatorial schemas: special limit distributions. – Manuscript, November 1993.

[12] Gardy (Danièle). – *Some results on the Asymptotic Behaviour of Coefficients of Large Powers of Functions*. – Research Report n° 769, Laboratoire de Recherche en Informatique, Université de Paris XI, August 1992. 23 pages.

[13] Good (I. J.). – Saddle-point methods for the multinomial distribution. *Annals of Mathematical Statistics*, vol. 28, 1957, pp. 861–881.

[14] Hayman (W. K.). – A generalization of Stirling's formula. *Journal für die reine und angewandte Mathematik*, vol. 196, 1956, pp. 67–95.

[15] Vitter (Jeffrey Scott) and Flajolet (Philippe). – Analysis of algorithms and data structures. In van Leeuwen (J.) (editor), *Handbook of Theoretical Computer Science*, Chapter 9, pp. 431–524. – North Holland, 1990.

Analysis of families of polynomials

Xavier Gourdon
INRIA Rocquencourt

March 8, 1993

[summary by Bruno Salvy]

Abstract

When the generating function of a family of polynomials $P_n(x)$ can be handled by singularity analysis, it is possible to obtain quantitative results about the localization of the roots of these polynomials. The computation goes through three main steps: *i)* computation of the singularities when x is fixed as functions of x; *ii)* application of a uniform version of singularity analysis at these singularities; *iii)* matching the singular expansions to get an equation relating the roots x_n and n. One can then obtain an error bound on the asymptotic estimate of the zeros by Rouché's theorem.

The talk describes the use of this method on four examples displaying different cases corresponding to different types of singularities. In all cases, the generating function has an explicit form looking like

$$P(x,z) = \sum_{n\geq 0} P_n(x) z^n = \frac{1}{1 - x a(z)},$$

where a is an analytic function which is 0 at the origin.

1. Two simple poles

This first example, $a(z) = z + z^2$ shows the outline of the method but does not require singularity analysis.

(1) When x is fixed, the singularities are at the two roots of the denominator, namely $z_\pm = -1/2(1 \pm \sqrt{1 + 1/4x})$;

(2) Since the poles are simple (except when $x = -1/4$), one gets the exact value $P_n(x) = \frac{z_+^{-n-1}}{1-x(1+2z_+)} + \frac{z_-^{-n-1}}{1-x(1+2z_-)}$.

(3) For x to be a zero, it is necessary that the terms in the above sum cancel. A simple computation shows that this happens only when $z_+^{n+1} = z_-^{n+1}$. In other words, z_+/z_- has to be a $n+1$st root of unity. After resolution this yields the roots $x = -4\cos^2(k\pi/(n+1))$.

In this example, it would have been possible to be more direct by noticing that the polynomials P_n are related to Tchebychev polynomials of the second kind.

2. A fixed algebraic singularity and a moving pole

In this example $a(z) = 1 - \sqrt{1-z}$.

(1) Obviously $z = 1$ is a singularity, while the cancellation of the denominator yields a polar singularity at $z_1 = 1 - (1 - 1/x)^2$.

(2) Fixing some $\delta > 0$ for uniformity, one gets the local expansion at 1 as

$$P(x,z) = \frac{1}{1-x} - \frac{x}{(1-x)^2}\sqrt{1-z} + \frac{x^2}{(1-x)^3}(1-z) + O[(1-z)^{3/2})],$$

where the $O()$ is uniform in $|1-x| \geq \delta$.
At z_1, the residue is $2\frac{1-x}{x^2}$.
Singularity analysis then yields

$$P_n(x) = 2\left(\frac{x-1}{x^2}\right) z_1^{-n-1} + \frac{x}{(1-x)^2}\frac{n^{-3/2}}{2\sqrt{\pi}}[1+O(1/n)],$$

where the $O()$ is uniform in $|x| \geq \delta$, $|1-x| \geq \delta$.

(3) Cancellation of the leading terms yields

$$z_1^{-n-1} = \frac{n^{-3/2}}{4\sqrt{\pi}}\frac{x^3}{(1-x)^3}[1+O(1/n)],$$

and this can be solved asymptotically. One gets at the first order

$$x = \frac{1}{1-\sqrt{1-e^{i\theta}}}, \quad \theta = \frac{2k\pi}{n+1}, \quad |x| \geq \delta.$$

This shows a limit curve to which the roots tend regularly.

Rouché's theorem makes it possible to show that this first order estimate is accurate up to $O(1/n)$.

3. An infinity of poles

We now consider $a(z) = e^z - 1$. Properly normalized, the polynomials P_n have Stirling numbers of the second kind as coefficients.

(1) Cancelling the denominator gives the simple poles $z_k = \log(1+1/x) + 2ik\pi$.
(2) The residue is $1/(1+x)$.
(3) Cancellation of the dominant contributions implies $z_0 = \overline{z_1}$, and as a consequence, $1+1/x$ must be real negative. Solving the first order cancellation yields

$$x_k = -\frac{1}{1+\exp\left[-\pi\cot\left((k+1/2)\frac{\pi}{n+1}\right)\right]}.$$

Here also, an argument based on Rouché's theorem gives an error bound, and using a recurrence on the P_n one shows that the roots are not only asymptotically real, but actually lie in the interval $]-1,0]$. This last property implies that the sequence of coefficients of P_n is unimodal.

4. A moving pole and a fixed logarithmic singularity

The following generating function originates in a question by P. Curtz [1]:

$$P(x,z) = \frac{\log(1+z)}{z[1-x\log(1+z)]}.$$

The coefficients can be shown to be related to Stirling numbers from which integral representations of the generating function can be deduced and this gives another means to analyze the zeroes. Using the same method as previously, we get

(1) A fixed singularity at $z=-1$ and a pole at $z_1 = e^{1/x} - 1$;

(2) Summing the contribution obtained by singularity analysis at -1 and by residue computation at z_1 one gets that

$$P_n(x) = \frac{e^{1/x}}{x^2} z_1^{-n-2} + \frac{(-1)^n}{x^2} \frac{1}{n \log^2 n} [1 + O(1/\log n)],$$

uniformly for $|x| \geq \delta$;

(3) Cancellation gives

$$x = \frac{1}{\log(1 + e^{i\theta})}, \quad \theta = \frac{2k\pi}{n+2}.$$

Once again the roots accumulate regularly around a limiting curve and an error bound can be obtained by Rouché's theorem.

Conclusion

This method seems to be of wide application. It is possible to extend it in order to get a full asymptotic expansion of the roots. It is also possible to study the case of families of polynomials whose generating function can be treated by a saddle-point method. Another extension leads to a quantitative version of Jentzsch's theorem about the roots of truncatures of Taylor series.

Bibliography

[1] Flajolet (Philippe), Gourdon (Xavier), and Salvy (Bruno). – Sur une famille de polynômes issus de l'analyse numérique. *Gazette des Mathématiciens*, vol. 55, January 1993, pp. 67–78.

Series and infinite products related to binary expansion of integers

Jean-Paul Allouche
CNRS, Université de Bordeaux I

December 7, 1992

[summary by Philippe Dumas]

Abstract

Various problems related to the binary expansion of integers are investigated. The Thue-Morse sequence, which gives the parity of the number of 1's in the binary expansion of an integer, appears in several identities and constants. We illustrate techniques, based on Dirichlet series or elementary methods, used to obtain such formulae.

The starting point is the sum $s_2(n)$ of the bits of the binary representation of n and the Thue-Morse sequence, $\epsilon(n) = (-1)^{s_2(n)}$. The next three relations will be our leading thread;

$$\sum_{n=1}^{+\infty} \frac{s_2(n)}{n(n+1)} = 2 \ln 2, \tag{1}$$

$$\prod_{n=0}^{+\infty} \left(\frac{2n+1}{2n+2}\right)^{\epsilon(n)} = \frac{\sqrt{2}}{2}, \tag{2}$$

$$\sum_{k=0}^{n} \epsilon(3k) > 0. \tag{3}$$

All these examples relate to the domain of automatic sequences whose prototype is the Thue-Morse sequence. Such sequences are at the frontier between the theory of formal languages and the theory of numbers. Their definitions are often simple but the techniques often involve Dirichlet series and asymptotic analysis.

1. Series

Formula 1 is excerpted from the Putnam competition (1981) and was generalized by Shallit [12] into

$$\sum_{n=1}^{+\infty} \frac{s_B(n)}{n(n+1)} = \frac{B}{B-1} \ln B, \tag{4}$$

where $s_B(n)$ is the sum of the digits of n for radix B. We show an example which extends this result. We take the sequence $u(n)$ which counts the number of blocks 11 in the binary expansion of n. For instance, since $14 = \overline{1110}$, then $u(14) = 2$. Introducing an appropriate function $f(x)$, which will be defined later, we consider the two series

$$\sum_{n=0}^{+\infty} u(n)\, f(2n+1), \quad \sum_{n=0}^{+\infty} u(2n+1)\, f(2n+1).$$

The only reasonable idea we can make use of is to split these series according to the parity of the integer n:

$$\sum_{n=0}^{+\infty} u(n)\, f(2n+1) = \sum_{n=0}^{+\infty} u(2n)\, f(4n+1) + \sum_{n=0}^{+\infty} u(2n+1)\, f(4n+2),$$

$$\sum_{n=0}^{+\infty} u(2n+1)\, f(2n+1) = \sum_{n=0}^{+\infty} u(4n+1)\, f(4n+1) + \sum_{n=0}^{+\infty} u(4n+3)\, f(4n+3).$$

But the sequence $u(n)$ satisfies the relations

$$u(n) = u(2n) = u(4n+1),$$

$$u(4n+3) = u(2n+1) + 1.$$

By subtraction, we obtain

$$\sum_{n=0}^{+\infty} u(n)\, f(2n+1) - \sum_{n=0}^{+\infty} u(2n+1)\, f(2n+1) = \sum_{n=0}^{+\infty} f(4n+3)$$

and eventually

$$\sum_{n=0}^{+\infty} u(n)\ [f(n) - f(2n) - f(2n+1)] = \sum_{n=0}^{+\infty} f(4n+3).$$

We apply this formula with

$$f(n) = \frac{1}{n^s} - \frac{1}{(n+1)^s}, \quad f(0) = 0,$$

and we get

$$\left(1 - \frac{1}{2^s}\right) \sum_{n=1}^{+\infty} u(n)\ \left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right] = \sum_{n=0}^{+\infty} \left[\frac{1}{(4n+3)^s} - \frac{1}{(4n+4)^s}\right]. \tag{5}$$

The behaviour of the Riemann and Hurwitz zeta functions near 1 are known [13, §13.21]:

$$\zeta(s) \underset{s\to 1}{=} \frac{1}{s-1} + \gamma + o(1),$$

$$\zeta(s,a) \underset{s\to 1}{=} \frac{1}{s-1} - \frac{\Gamma'}{\Gamma}(a) + o(1),$$

and the local analysis of the terms in Formula 5 in the neighbourhood of 1 gives

$$\sum_{n=1}^{+\infty} \frac{u(n)}{n(n+1)} = \frac{1}{2}\ \left(-\frac{\Gamma'}{\Gamma}(3/4) - \gamma\right).$$

According to Gauss [13, §12.16] [8, p. 94], we have

$$\frac{\Gamma'}{\Gamma}(p/q) = -\gamma - \ln(2q) - \frac{\pi}{2}\ \operatorname{cotg}\frac{\pi p}{q} + 2 \sum_{0<n<q/2} \cos\frac{2\pi p n}{q}\ \ln\sin\frac{\pi n}{q},$$

hence

$$\sum_{n=1}^{+\infty} \frac{u(n)}{n(n+1)} = \frac{3}{2}\ \ln 2 - \frac{\pi}{4}.$$

In the same vein, one can prove the formulae [4]

$$\sum_{n=2}^{+\infty} s_2(n)\, \frac{(2n+1)}{n^2(n+1)^2} = \frac{\pi^2}{9},$$

$$\sum_{n=1}^{+\infty} s_2(n)^2 \, \frac{8n^3+4n^2+n-1}{4n(n^2-1)(4n^2-1)} = \frac{17}{24} + \ln 2,$$

$$\sum_{n=5}^{+\infty} u(n) \, \frac{8n^3-4n^2-n-9}{(n-3)(n+1)(2n-3)(4n^2-1)} = \frac{95}{168} + \frac{5}{4} \ln 2 - \frac{\pi}{8}.$$

The use of the function

$$f(n) = \frac{1}{n^s} - \frac{1}{(n+1)^s}$$

is more than a trick. The crux of the matter is that $f(x)$ is an eigenvector of operator T,

$$Tg(x) = g(x) - \sum_{0 \le j < B} g(B\,x + j).$$

More precisely an eigenvector $g(x)$ such that the series $\sum_n g(n)$ converges and $g(x) \sim x^r$ for x in a neighbourhood of 0 is essentially $f(x)$.

2. Infinite products

Shallit [12] proved Formula 2 by real analysis and Allouche and Cohen [3, 1] gave another proof by means of Dirichlet series. The logarithm of the infinite product is

$$\sum_{n=0}^{+\infty} \epsilon(n) \, \ln\left(1 - \frac{1}{2\,(n+1)}\right) = -\sum_{k=0}^{+\infty} \frac{1}{k\,2^k} \sum_{n=0}^{+\infty} \frac{\epsilon(n)}{(n+1)^k}.$$

Therefore it is natural to introduce the Dirichlet series

$$f(s) = \sum_{n=0}^{+\infty} \frac{\epsilon(n)}{(n+1)^s}.$$

Splitting the sum according to the parity of n yields

$$\left(1 + \frac{1}{2^s}\right) f(s) = \sum_{n=0}^{+\infty} \frac{\epsilon(n)}{2^s\,(n+1)^s} \left(1 - \frac{1}{2(n+1)}\right)^{-s}$$

and by binomial expansion

$$\left(1 + \frac{1}{2^s}\right) f(s) = \sum_{k=0}^{+\infty} \frac{1}{2^{k+s}} \binom{s+k-1}{k} f(s+k).$$

The infinite functional equation

$$f(s) = \sum_{k=1}^{+\infty} \frac{1}{2^{k+s}} \binom{s+k-1}{k} f(s+k),$$

permits us to extend function $f(s)$ throughout the entire complex plane. Moreover

$$f'(0) = \sum_{k=1}^{+\infty} \frac{1}{k\,2^k} f(k)$$

and that is the quantity we are looking for. The function

$$g(s) = \sum_{n=1}^{+\infty} \frac{\epsilon(n)}{n^s}$$

satisfies

$$\left(1-\frac{1}{2^s}\right)\,g(s)=\left(1+\frac{1}{2^s}\right)\,f(s)$$

and can be extended in the same manner as $f(s)$. The only difference lies in the fact that $g(0)=-1$ and this gives

$$f'(0)=-1,$$

hence Formula 2.

Another method to obtain Formula 2 is to apply a greedy algorithm which computes sequentially the exponents $\alpha(n)=\pm 1$ such that

$$\left(\frac{1}{2}\right)^{+1}\left(\frac{3}{4}\right)^{-1}\left(\frac{5}{6}\right)^{+1}\left(\frac{7}{8}\right)^{+1}\cdots\left(\frac{2\,n+1}{2\,n+2}\right)^{\alpha(n)}\cdots=\frac{\sqrt{2}}{2}.$$

The partial products approach the limit alternating from below or above, as do the partial sums of the series

$$\sum_{n=0}^{+\infty}\epsilon(n)\,\ln\frac{2\,n+1}{2\,n+2}.$$

As a result the two sequences α and ϵ are equal.

More generally, for each pattern w there exists a rational function $g(n)$ such that

$$\prod_{n\geq 0}g(n)^{\beta(n)}=\frac{\sqrt{2}}{2},$$

where $\beta(n)$ equals $+1$ or -1 according to the parity of the number of w in the binary expansion of n. For example,

$$\prod_{n\geq 0}\left(\frac{(2\,n+1)^2}{(n+1)(4\,n+1)}\right)^{\beta(n)}=\frac{\sqrt{2}}{2},$$

if $\beta(n)=(-1)^{u(n)}$ is the Rudin-Shapiro sequence associated to pattern $w=11$.

In the same vein, the Flajolet product [6]

$$\prod_{n\geq 0}\left(\frac{2\,n}{2\,n+1}\right)^{\epsilon(n)}$$

is not known. We point out that the rational fraction $2\,n/(2\,n+1)$ is related to pattern $w=01$.

3. Newman-Coquet sequence

This is our last example. The first few terms of the Thue-Morse sequence $\epsilon(n)$ are (with $+\equiv+1$ and $-\equiv-1$)

$$+\;-\;-\;+\;-\;+\;+\;-\;-\;+\;+\;-\;+\;-\;-\;+\;-\;+\;+\;-\;+\;-\;-\;+\;+-$$

and the first few terms of the subsequence $\epsilon(3\,n)$, the Newman-Coquet sequence, are

$$+\;+\;+\;+\;+\;+\;+\;-\;+\;+\;+\;+\;+\;+\;-\;+\;+\;+\;+\;+\;+\;+\;+\;-\;+\;+\,.$$

The abundance of $+$ is startling [10] and it is natural to wonder about the sign of

$$s_N=\sum_{n<N}\epsilon(3\,n).$$

In fact there are asymptotically as many minuses as there are pluses and s_N/N is $o(N)$. Newman and Slater [11] have showed that s_N is of the same order of magnitude as N^α, with $\alpha = \log 3/\log 4$, though not admitting an asymptotic equivalent $C\,N^\alpha$. Next Coquet [5, 7] proved that

$$\sum_{n<x} \epsilon(3\,n) \underset{x\to\infty}{=} x^\alpha\, F\left(\frac{\log x}{\log 4}\right) + O(1),$$

where F is 1-periodic, continuous but nowhere differentiable.

By a greedy algorithm, every sequence of ± 1 can be written as an infinite product

$$\prod_w b_w(n),$$

where $b_w(n)$ is $+1$ or -1 according to the parity of the number of w in the binary expansion of n [9]. For the Coquet sequence, one obtains [2]

$$\epsilon(3\,n) = b_{111}(n) b_{11011}(n) \cdots b_{11(01)^i1}(n) \cdots .$$

The rarity of the blocks $11(01)^i1$ explains the excess of $+$ in the sequence.

Bibliography

[1] Allouche (J.-P.), Cohen (H.), France (M. Mendès), and Shallit (J. O.). – De nouveaux curieux produits infinis. *Acta Arithmetica*, vol. XLIX, 1987, pp. 141–153.

[2] Allouche (J.-P.), Morton (P.), and Shallit (J.). – Pattern spectra, substring enumeration, and automatic sequences. *Theoretical Computer Science*, vol. 94, 1992, pp. 161–174.

[3] Allouche (Jean-Paul) and Cohen (Henri). – Dirichlet series and curious infinite products. *Bulletin of the London Mathematical Society*, vol. 17, 1985, pp. 531–538.

[4] Allouche (Jean-Paul) and Shallit (Jeffrey). – The ring of k-regular sequences. *Theoretical Computer Science*, vol. 98, 1992, pp. 163–197.

[5] Coquet (J.). – A summation formula related to binary digits. *Inventiones Mathematicae*, vol. 73, 1983, pp. 107–115.

[6] Flajolet (P.) and Martin (G. N.). – Probabilistic counting algorithms for data base applications. *Journal of Computer and System Sciences*, vol. 31, n° 2, October 1985, pp. 182–209.

[7] Flajolet (Philippe), Grabner (Peter), Kirschenhofer (Peter), Prodinger (Helmut), and Tichy (Robert). – Mellin transforms and asymptotics: Digital sums. *Theoretical Computer Science*, 1993. – To appear.

[8] Knuth (Donald E.). – *The Art of Computer Programming.* – Addison-Wesley, 1968, vol. 1: Fundamental Algorithms. Second edition, 1973.

[9] Morton (P.) and Mourant (W.). – Paper folding, digit patterns, and groups of arithmetic fractals. *Proceedings of the London Mathematical Society*, vol. 59, 1989, pp. 253–293.

[10] Newman (Donald J.). – On the number of binary digits in a multiple of three. *Proceedings of the American Mathematical Society*, vol. 21, 1969, pp. 719–721.

[11] Newmann (D. J.) and Slater (M.). – Binary digit distribution over naturally defined sequences. *Transactions of the American Mathematical Society*, vol. 213, 1975, pp. 71–78.

[12] Shallit (J. O.). – On infinite products associated with sums of digits. *Journal of Number Theory*, vol. 21, 1985, pp. 128–134.

[13] Whittaker (E. T.) and Watson (G. N.). – *A Course of Modern Analysis.* – Cambridge University Press, 1927, fourth edition. Reprinted 1973.

Asymptotique des suites mahlériennes : quelques exemples typiques

Philippe Dumas
INRIA Rocquencourt

7 Décembre 1992

[résumé par Philippe Dumas]

Résumé

Une suite mahlérienne (u_n) est solution d'une récurrence linéaire qui exprime u_n en fonction de u_{n-1}, u_{n-2}, ..., $u_{n/2}$, $u_{(n-1)/2}$, ..., $u_{n/4}$, etc. Ces suites apparaissent naturellement dans les problèmes de comptage liés à l'écriture binaire des entiers ou dans l'étude d'algorithmes du type "diviser pour régner" et nous nous intéressons ici à leur comportement asymptotique.

Citons deux exemples classiques qui ont suscité de nombreux articles : la suite S_n qui somme les chiffres de l'écriture en base 2 des entiers de 1 à n et la suite b_n du nombre de partitions binaires de l'entier n, à laquelle K. Mahler s'est lui-même intéressé.

Nous proposons une classification qui vise à décrire les différents comportements possibles pour une telle suite. Elle est illustrée de quelques exemples, encore fragmentaires, où l'on voit fonctionner les méthodes classiques de l'analyse asymptotique comme la méthode du col ou de la théorie analytique des nombres comme la formule de Perron.

1. Séries mahlériennes

1.1. Définition et propriétés de clôture. Nous disons qu'une série de Laurent $f(z)$ est B-mahlérienne si elle satisfait une équation de Mahler

$$c_0(z)f(z) + c_1(z)f(z^{\mathrm{B}}) + \cdots + c_N(z)f(z^{\mathrm{B}^N}) = 0$$

à coefficients des fractions rationnelles c_0, ..., c_N avec les $c_k(z)$ non tous nuls. Ici nous allons supposer que le corps de référence, $\mathbb{K}$, est $\mathbb{Q}$ ou $\mathbb{C}$ et pour simplifier les écritures nous allons même imposer $\mathrm{B} = 2$, ce qui recouvre presque tous les exemples naturels.

Cette définition en terme de séries formelles se traduit immédiatement en une définition pour les suites si nous remarquons que les deux opérateurs de multiplication par z et de substitution par z^2

$$f(z) \longmapsto z\,f(z), \quad f(z) \longmapsto f(z^2),$$

se traduisent dans l'espace des suites par l'opérateur de décalage et l'opérateur d'homothétie,

$$(f_n) \longmapsto (f_{n-1}), \quad (f_n) \longmapsto (f_{n/2}).$$

Ainsi une suite (f_n) est 2-mahlérienne si elle satisfait une relation de récurrence

$$\sum_l c_{0,l} f_{n-l} + \sum_l c_{1,l} f_{(n-l)/2} + \cdots + \sum_l c_{N,l} f_{(n-l)/2^N} = 0$$

avec les scalaires $c_{k,l}$ non tous nuls.

L'anneau $\mathbb{K}[z, M]$, où M désigne l'opérateur de substitution par z^2, appelé aussi opérateur de Mahler, cet anneau donc, est euclidien à gauche, ce qui fait que l'on peut parler d'équation minimale d'une série mahlérienne.

D'autre part l'espace des séries 2-mahlériennes possède les propriétés de clôture suivantes :

(1) les fractions rationnelles sont mahlériennes,
(2) si $f(z) \in \mathbb{K}((z))$ satisfait une équation de Mahler

$$c_0(z)f(z) + c_1(z)f(z^2) + \cdots + c_N(z)f(z^{2^N}) = b(z),$$

dont le second membre $b(z)$ est une série mahlérienne, alors $f(z)$ est une série mahlérienne,
(3) si $f(z)$ est mahlérienne, il en est de même de $f(z^2)$,
(4) les séries mahlériennes forment un sous-espace vectoriel du $\mathbb{K}$-espace vectoriel $\mathbb{K}((z))$ (et même du $\mathbb{K}(z)$-espace vectoriel $\mathbb{K}((z))$),
(5) si f et g sont deux séries mahlériennes, il en est de même de leur produit de Cauchy $f \times g$,
(6) si f est une série mahlérienne, sa série dérivée f' est aussi mahlérienne.

Par contre une primitive de série mahlérienne n'est pas nécessairement mahlérienne, comme on le voit en considérant $\ln \dfrac{1}{1-z}$, et le produit de Hadamard de deux séries mahlériennes n'est généralement pas mahlérien.

1.2. Séries 2-régulières. Parmi les séries mahlériennes nous distinguons une classe particulière : celle des séries régulières. Rappelons une définition possible [1, 6]. Nous nous donnons deux matrices carrées A_0, A_1, une matrice ligne λ et une matrice colonne γ, toutes de taille convenable. Si n est un entier naturel, nous écrivons son développement binaire $\varepsilon_l \cdots \varepsilon_1 \varepsilon_0$ et nous calculons le nombre $f_n = \lambda A_{\varepsilon_l} \cdots A_{\varepsilon_1} A_{\varepsilon_0} \gamma$. Alors la série formelle $f(z) = \sum_{n \geq 0} f_n z^n$ est 2-régulière.

La donnée de A_0, A_1, λ et γ est une représentation linéaire de la série régulière $f(z)$ et un peu de réflexion montre que derrière toute série 2-régulière se cache une série rationnelle non commutative sur l'ensemble d'indéterminées $\{x_0, x_1\}$. Cette remarque permet d'obtenir à peu de frais de nombreuses propriétés de ces séries, comme la stabilité par somme ou produit de Hadamard. Il faut noter aussi la stabilité par produit de Cauchy.

La notion de série régulière généralise celle de suite automatique car une série automatique est une série régulière dont les coefficients sont pris dans un ensemble fini.

Le théorème de Christol, Kamae, Mendès France et Rauzy [3, 9], qui relie suites automatiques à valeurs dans $\mathbb{F}_q$ et séries formelles algébriques sur $\mathbb{F}_q(z)$, nous montre, *mutatis mutandis*, qu'une série régulière est mahlérienne.

2. Comportement asymptotique

2.1. Classification. L'équation minimale d'une série mahlérienne a un coefficient $c_0(z)$ qui n'est pas nul et sa résolution se scinde en deux parties : d'abord l'étude d'un système linéaire qui donne la dimension de l'espace des solutions et la partie basse des solutions puis l'application d'une récurrence mahlérienne qui permet de calculer autant de termes que l'on veut de la partie haute. On peut encore dire que cette deuxième phase est la recherche d'un point fixe par itération d'un opérateur contractant dans l'espace des séries formelles et il en résulte que les solutions définissent des fonctions méromorphes dans le disque unité, qui ne peuvent avoir comme pôles que les zéros du coefficient $c_0(z)$ et leurs racines carrées itérées.

Partant de ceci, on montre [6] qu'une série mahlérienne se décompose en un produit de quatre séries mahlériennes

$$f(z) = p_-(z)p(z)p_+(z)g(z).$$

Les trois séries $p_-(z)$, $p(z)$ et $p_+(z)$ sont des produits infinis de la forme

$$\prod_{k \geq 0} \frac{1}{\varphi(z^{2^k})}$$

dans lesquels $\varphi(z)$ est un polynôme dont les racines sont respectivement de module strictement plus petit que 1, de module 1 mais sans être des racines de l'unité d'ordre pair (le mot "ordre" est pris au sens de la

théorie des groupes) ou de module strictement plus grand que 1. Enfin $g(z)$, le dernier terme du produit, est une série régulière.

Comme nous ne savons pas traiter le problème en toute généralité, nous allons nous contenter de considérer des exemples qui ne ressortissent essentiellement que d'un des quatre types précédents.

2.2. Cas interne. Une équation

$$c_0(z)f(z) + \cdots + c_N(z)f(z^{\mathrm{B}^N}) = b(z)$$

dans laquelle $c_0(z)$ a des racines dont au moins une est de module strictement plus petit que 1, apparaît comme une perturbation de l'équation

$$c_0(z)r(z) = b(z)$$

et le comportement des coefficients d'une solution $f(z)$ va être en première approximation du même type que pour la solution rationnelle $r(z)$ de celle-ci.

Ainsi la suite (u_n), définie par les conditions initiales $u_0 = 0$, $u_1 = 1$ et la récurrence

$$u_n = u_{n-1} + u_{n-2} + u_{n/2}$$

est une perturbation de la suite de Fibonacci. La série génératrice associée, $u(z)$, vérifie l'équation

$$(1 - z - z^2)u(z) = z + (1 + z)u(z^2)$$

et ceci nous fournit par itération

$$u(z) = \frac{z}{1 - z - z^2} + \frac{1}{(1 - z - z^2)(1 - z^2 - z^4)}\left[z^2(1 + z) + (1 + z)(1 + z^2)v(z)\right]$$

avec

$$v(z) = \frac{z^4}{1 - z^4 - z^8} + \frac{z^8(1 + z^4)}{(1 - z^4 - z^8)(1 - z^8 - z^{16})} + \frac{z^{16}(1 + z^4)(1 + z^8)}{(1 - z^4 - z^8)(1 - z^8 - z^{16})(1 - z^{16} - z^{32})} + \cdots$$

Par simple soustraction des singularités, nous obtenons

$$u_n \underset{n \to +\infty}{=} C\phi^n + (c_+ + (-1)^n c_-)\phi^{n/2} + O(\phi^{n/4})$$

en notant ϕ le nombre d'or et

$$C = \frac{2\phi + 1}{\sqrt{5}} + \frac{\phi^4}{2} v(1/\phi) \simeq 2.0996360882.$$

2.3. Cas régulier. La classification que nous avons donnée confine essentiellement la difficulté dans l'étude des suites régulières, puisque pour les trois autres cas nous disposons d'une expression explicite en produit infini. D'ailleurs on peut à bon droit s'interroger sur la pertinence d'un développement asymptotique pour certaines suites à l'aspect assez chaotique comme la suite miroir, qui à un entier n associe la valeur de son écriture binaire lue à l'envers (cf. figure 1).

En pratique on est amené à lisser ces suites par application de l'opérateur de sommation. Par exemple la suite $(\nu(n))$ qui donne la somme des bits d'un entier a des variations violentes mais la suite $(S(n))$ qui représente la somme de tous les bits des entiers entre 1 et n a un comportement assez lisse puisque [5]

$$S(n) = \frac{1}{2}\, n \lg n + o(n \lg n),$$

où la notation lg représente le logarithme de base 2.

Remarquons d'abord qu'une suite régulière (u_n) vérifie $u_n = O(n^\alpha)$ pour un certain α [1]. Ceci résulte d'une majoration grossière des coefficients des matrices d'une représentation linéaire. La détermination de la borne inférieure des α possibles est délicate en toute généralité. Une technique consiste à considérer tous les produits de longueur donnée $A_{\varepsilon_1} \cdots A_{\varepsilon_l}$, si A_0, A_1 sont les deux matrices carrées d'une représentation linéaire, et à utiliser le maximum des normes de ces produits en comptant qu'un effet de moyenne va permettre d'affiner les bornes utilisées.

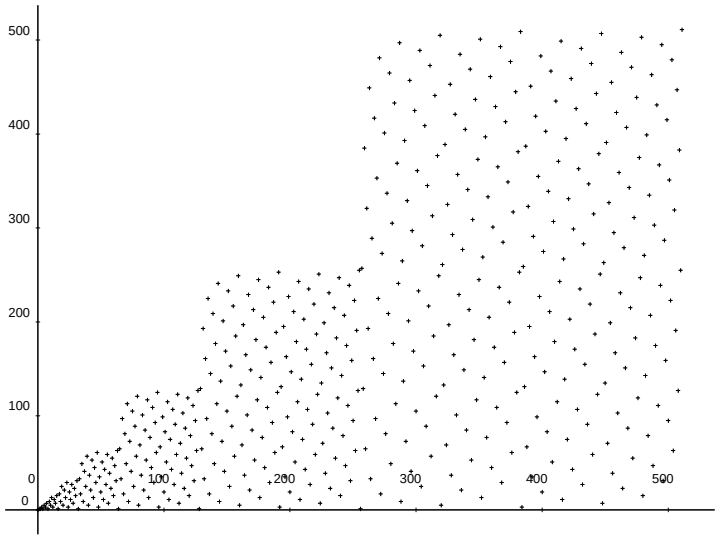


FIGURE 1
La suite miroir présente à la fois un comportement globalement simple et difficile à décrire du point de vue asymptotique.

La majoration précédente permet de considérer la série de Dirichlet

$$u(s) = \sum_{n=1}^{+\infty} \frac{u_n}{n^s}.$$

Une technique utilisée systématiquement dans un contexte voisin par Flajolet *et alii* [8] consiste à invoquer la formule de Perron dans la version

$$\sum_{1 \le k < n} \left(1 - \frac{k}{n}\right) v_k = \frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} v(s) n^{s+1} \frac{ds}{s(s+1)}.$$

Idéalement cette formule s'applique à la série génératrice des différences secondes et les singularités de l'intégrande sont connues, ce qui permet par des calculs de résidus d'obtenir une série asymptotique comme approximation de u_n. Dans les bons cas ce développement est même convergent.

En pratique $v(s)$ est plutôt la série génératrice des différences premières et on a donc un développement asymptotique pour la fonction sommatoire de la suite (u_n).

Considérons par exemple [8, p. 8] le nombre γ_n de 1 dans la représentation en code Gray de l'entier n. La suite des différences arrière $\delta_n = \gamma_n - \gamma_{n-1}$ vérifie $\delta_{2k} = \delta_k$ et $\delta_{2k+1} = (-1)^k$. Sa série de Dirichlet est donc

$$\delta(s) = \frac{2^s\, L(s)}{2^s - 1} \qquad \text{avec} \qquad L(s) = \sum_{k=0}^{+\infty} \frac{(-1)^k}{(2k+1)^s}.$$

D'après la formule de Perron, la fonction sommatoire $G_N = \sum_{n<N} \gamma_n$ est donnée par

$$G_N = \frac{N}{2i\pi} \int_{2-i\infty}^{2+\infty} \frac{2^s\, L(s)}{2^s - 1}\, N^s \frac{ds}{s(s+1)}.$$

L'intégrande est méromorphe avec un pôle double en 0 de résidu

$$\frac{1}{2}\,\frac{\ln n}{\ln 2} + \frac{\ln \Gamma(1/4)/\Gamma(3/4)}{\ln 2} - \frac{3}{4} - \frac{1}{2\ln 2},$$

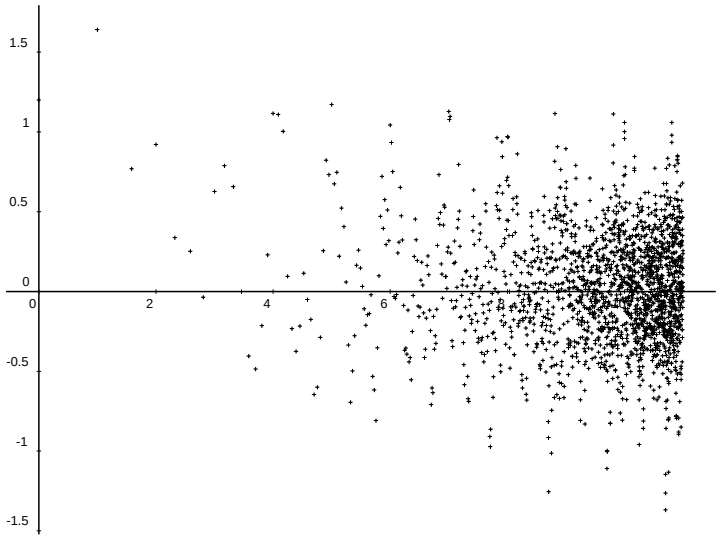


FIGURE 2
Le comportement de la suite des coefficients du produit $\displaystyle\prod_{k\geq 0}\frac{1}{1-6/5\,z^{2^k}+z^{2.2^k}}$ laisse perplexe le petit asymptoticien

un pôle simple en chaque $\chi_k = 2ik\pi/\ln 2$ et un pôle simple en -1. On trouve ainsi

$$G_N = \frac{1}{2}\,N\,\lg N + N\,F(\lg N)$$

où $F(u)$ est une fonction 1-périodique donnée par la série de Fourier

$$F(u) = 2\,\lg\,\Gamma\left(\frac{1}{4}\right) - \frac{3}{2} - \lg\,\pi + \frac{1}{\ln 2}\sum_{k\neq 0}\frac{L(\chi_k)}{\chi_k(\chi_k+1)}\,\exp(2ik\pi u).$$

Évidemment la série de Fourier provient des pôles χ_k et c'est leur disposition régulière qui produit une fonction périodique.

L'apparition d'une fonction périodique est usuelle dans ces questions et nous renvoyons à [8] pour d'autres exemples. Citons aussi [7] qui emploie des méthodes élémentaires.

2.4. Cas complémentaire. La suite des coefficients d'un produit infini comme

$$\prod_{k\geq 0}\frac{1}{1-6/5\,z^{2^k}+z^{2.2^k}},$$

dans lequel le polynôme $\varphi(z)$, ici $1-6/5\,z+z^2$, a comme racines des nombres complexes de module 1 qui ne sont pas des racines de l'unité, a un comportement assez erratique sur lequel nous avons bien peu à dire pour l'instant (cf. figure 2).

Aussi allons nous plutôt évoquer l'étude des coefficients du produit

$$p(z) = \prod_{k\geq 0}\frac{1}{1+z^{2^k}+z^{2.2^k}},$$

où le polynôme utilisé, en l'occurrence $\Phi_3(z)$, est un polynôme cyclotomique dont l'indice est premier avec 2.

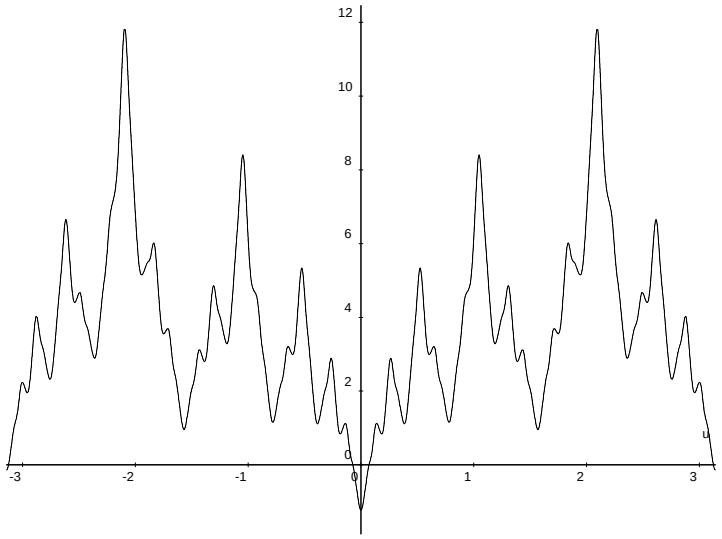


FIGURE 3
Le comportement de $\prod_{k\geq 0} \frac{1}{1+z^{2^k}+z^{2.2^k}}$ sur le contour d'intégration montre une prédominance des racines cubiques primitives de l'unité et de leurs racines carrées itérées. En abscisse on voit l'argument de z et en ordonnée le logarithme du module de la fonction.

Pour extraire le coefficient d'indice n de $p(z)$, nous utilisons la formule de Cauchy

$$[z^n]p(z) = \frac{1}{2i\pi}\int_C \frac{p(z)}{z^{n+1}}\,dz,$$

où C est un lacet entourant l'origine.

Le cercle unité est frontière naturelle mais tous les points du cercle n'ont pas la même importance. Nous avons d'abord les deux racines primitives cubiques j et j^2, qui sont racines de tous les $\Phi_3(z^{2^k})$, puis leurs racines carrées $-j$ et $-j^2$, qui sont racines des $\Phi_3(z^{2^k})$ à partir de $k=1$, etc. Pour mettre en valeur ces comportements nous procédons à une étude locale au voisinage des racines carrées itérées des racines cubiques de l'unité, en utilisant la transformation de Mellin et le calcul des résidus, dans l'esprit de [4] ou [2, chap. 6]. Nous constatons ainsi qu'au voisinage de ω la fonction $p(\omega e^{-t})$ a un comportement en $\exp(\ln^2 t)$ si ω vaut j, j^2 ou une de leurs racines carrées itérées alors qu'elle a seulement un comportement en $\exp(\ln t)$ si ω vaut 1 ou de ses racines carrées itérées.

Nous prenons alors pour C un cercle collé le long du cercle unité et nous le divisons en petits arcs qui font face aux racines carrées itérées de 1, j et j^2. Nous appliquons à chaque intégrale la méthode du col puis nous sommons toutes les approximations obtenues et nous constatons que seules les contributions des arcs associés à j et j^2 importent vraiment.

En appelant ρ l'unique solution strictement positive de l'équation

$$\lg\rho + n\rho - \frac{1}{2} + \lg 3 = 0$$

et en posant

$$v = \frac{\ln\rho}{2\ln 2},$$

nous avons l'équivalence

$$[z^n]\prod_{k\geq 0}\frac{1}{1+z^{2^k}+z^{2.2^k}} \underset{n\to+\infty}{\sim}$$

$$\exp\left[2v^2\ln 2+v(-2+\ln 3)-\frac{1}{2}\ln 2n\pi+C+P(v)\right]\times 2\cos\left(\frac{2n\pi}{3}+\frac{\pi}{12}+P^*(v)\right),$$

où la constante C est

$$C=-\frac{1}{12\ln 2}\left(-3\ln^2 3+3\ln 2\ln 3-\ln^2 2-6\ln 2+12\ln 3+6\gamma^2-\pi^2+12\gamma_1\right)$$

et les fonctions 1-périodiques $P(v)$ et $P^*(v)$ sont définies par leur série de Fourier

$$P(v)=\frac{1}{2\ln 2}\sum_{k\neq 0}\Gamma(s_k)\zeta(1+s_k)\left(3^{-s_k}+1\right)\exp(4ki\pi v),$$

$$P^*(v)=\frac{1}{2\ln 2}\sum_{k}\Gamma(r_k)3^{-1/2-r_k}\left[\zeta(1+r_k,1/3)-\zeta(1+r_k,2/3)\right]\exp((4k+2)i\pi v)$$

avec

$$s_k=2ik\pi/\ln 2,\quad r_k=(2k+1)i\pi/\ln 2.$$

On voit clairement apparaître la périodicité modulo 3, qui est évidente dès que l'on calcule quelques termes de la suite, mais aussi une périodicité en $\lg n$ plus cachée comme dans le cas des suites régulières.

2.5. Cas externe. Il nous reste enfin le cas d'un produit infini associé à un polynôme dont toutes les racines ont un module strictement plus grand que 1. Un exemple typique en est

$$\prod_{k\geq 1}\frac{1}{1-z^{2^k}/\rho}$$

avec $\rho>1$. Ce cas est encore à l'étude et nous nous contenterons d'une remarque. Si nous traçons le graphe de la suite des coefficients (cf. Figure 4, où $\rho=2$) en joignant les points d'abscisse n suivant le nombre de bits égaux à 1 dans l'écriture binaire de n, nous voyons apparaître des phénomènes périodiques et une étude plus approfondie semble montrer que le n-ième terme de la suite vaut asymptotiquement

$$c\prod_{i=1}^{k}\left(a(l_i)+b(l_i)\,F(\lg n)\right)$$

où $F(u)$ est 1-périodique, si l'écriture binaire de n se décompose en k blocs $10\cdots 0$, le i-ème bloc comportant l_i zéros.

2.6. Conclusion. Comme on le voit l'étude du comportement asymptotique des suites mahlériennes est loin d'être achevée.

En particulier une question générale demeure : quelle est la bonne échelle asymptotique pour exprimer ces suites ? Il est clair que les fonctions usuelles n^α, $\ln^\beta n$, etc. sont insuffisantes. L'utilisation des séries trigonométriques permet de décrire des comportements assez chaotiques, mais pose des problèmes de convergence ; il serait peut être pertinent d'introduire certaines suites régulières comme la suite somme des bits ou la suite miroir dans l'échelle utilisée.

Au cas où le lecteur n'aurait pas encore reconnu sa main, nous précisons que les quelques idées pertinentes qui figurent dans ce texte ont été inspirées par le bon docteur Flajolet.

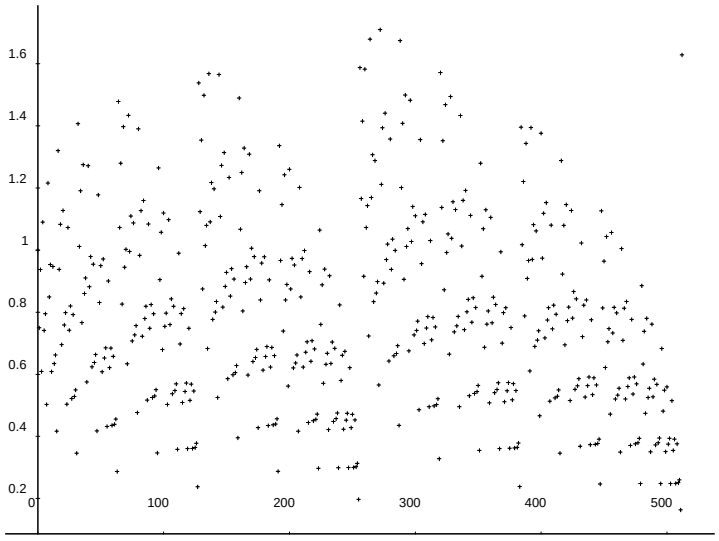


FIGURE 4
Les coefficients de $\prod_{k\geq 1} \frac{1}{1-z^{2^k}/2}$ présentent un comportement périodique quand on classe les entiers suivant la somme des bits de leur écriture binaire.

Bibliographie

[1] Allouche (Jean-Paul) et Shallit (Jeffrey). – The ring of k-regular sequences. *Theoretical Computer Science*, vol. 98, 1992, pp. 163–197.

[2] Andrews (George E.). – *The Theory of Partitions.* – Addison-Wesley, 1976, *Encyclopedia of Mathematics and its Applications*, vol. 2.

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

[4] De Bruijn (N. G.). – On Mahler's partition problem. *Indagationes Mathematicae*, vol. 10, 1948, pp. 210–220. – Reprinted from *Koninklijke Akademie voor Wetenschappen, Series A*.

[5] Delange (Hubert). – Sur la fonction sommatoire de la fonction somme des chiffres. *L'Enseignement Mathématique*, vol. XXI, n° 1, 1975, pp. 31–47.

[6] Dumas (Philippe). – *Récurrences Mahlériennes, suites automatiques, et études asymptotiques.* – Doctorat de Mathématiques, Université de Bordeaux I, 1993.

[7] Dumont (Jean-Marie) et Thomas (Alain). – Systèmes de numération et fonctions fractales relatifs aux substitutions. *Theoretical Computer Science*, vol. 65, 1989, pp. 153–169.

[8] Flajolet (Philippe), Grabner (Peter), Kirschenhofer (Peter), Prodinger (Helmut), et Tichy (Robert). – Mellin transforms and asymptotics: Digital sums. *Theoretical Computer Science*, 1993. – To appear.

[9] Loxton (J. H.). – Automata and transcendance. *In : New Advances in Transcendance Theory*, éd. par Baker (Alan). pp. 215–228. – Cambridge University Press, 1988.

Énumération de permutations et de partitions : nouveaux résultats asymptotiques

A. M. Odlyzko
AT&T Bell Laboratories

3 Septembre 1992

[résumé par Dominique Gouyou-Beauchamps]

1. Introduction

Le but de l'exposé est d'étudier les permutations qui ont un motif interdit. Ce motif sera une permutation fixée τ sur $\{1, 2, \ldots, k\}$. Il faut donc examiner si τ apparaît dans une permutation σ sur $\{1, 2, \ldots, n\}$, c'est-à-dire examiner s'il existe une suite d'indices $1 \leq i_{\tau(1)} < i_{\tau(2)} < \cdots < i_{\tau(k)} \leq n$ tels que $\sigma(i_1) < \sigma(i_2) < \cdots < \sigma(i_k)$.

Exemple. $\tau = (1\ 3\ 2)$ apparaît dans $\sigma = (5\ 2\ 9\ 4\ 14\ 10\ 1\ 3\ 6\ 15\ 8\ 11\ 7\ 13\ 12)$ car, pour la suite d'indices $(i_1 = 1,\ i_2 = 13,\ i_3 = 11)$, la sous-suite $(\sigma(1), \sigma(11), \sigma(13)) = (5\ 8\ 7)$ est de type $(1\ 3\ 2)$ ou, pour la suite d'indices $(i_1 = 4,\ i_2 = 9,\ i_3 = 6)$, la sous-suite $(\sigma(4), \sigma(6), \sigma(9)) = (4\ 10\ 6)$ est aussi de type $(1\ 3\ 2)$ (comme bien d'autres sous-suites).

Les questions d'énumération et d'algorithmique qu'on peut se poser sont les suivantes :

(1) Pour un motif τ donné, soit $F(n, \tau)$ le nombre de permutations de $\mathfrak{S}_n$ qui ne possède pas le motif τ. Comment se comporte $F(n, \tau)$ lorsque $n \to \infty$? Est-ce-que la limite $\lim_{n\to\infty} F(n, \tau)^{1/n}$ est indépendante de τ pour une longueur k de τ fixée ?
(2) Pour un motif τ fixé, quel est le nombre maximum d'occurrences de τ dans une permutation de $\mathfrak{S}_n$ (cf. Lifschitz et Pittel [9]) ?
(3) Comment tester si $\sigma \in \mathfrak{S}_n$ ne contient pas τ ?
(4) Comment obtenir la liste des permutations de $\mathfrak{S}_n$ qui ne contiennent pas τ ?

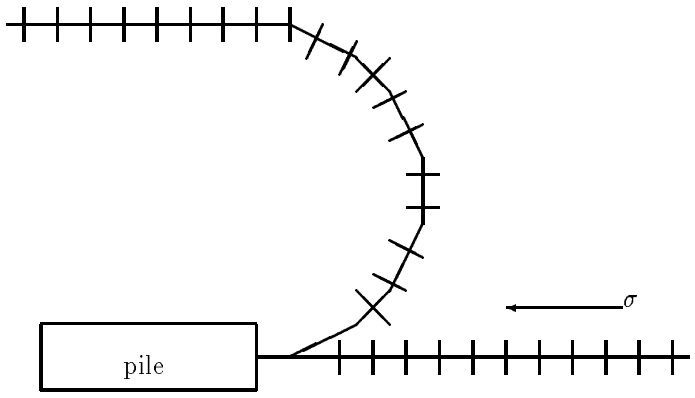


Fig. 1

Parmi les premiers travaux dans ce domaine, on peut citer le problème du tri par voie de garage ("Railroad siding") évoqué par Knuth [8] et Tarjan [19]. Ce problème peut s'énoncer ainsi : comment trier une permutation de $\{1, 2, \ldots, n\}$ avec une pile quand à chaque étape du tri on peut soit mettre la nouvelle lettre entrée sur la pile, soit retirer le sommet de la pile et l'envoyer sur la sortie. On suppose donc que la permutation est entrée lettre par lettre en la lisant de la droite vers la gauche et qu'elle sort triée en ordre croissant. Ceci peut être vu comme un problème de chemin de fer, comme l'illustre la figure 1.

Il est bien connu (Knuth [8]) qu'une permutation σ peut être triée de cette façon si et seulement si elle ne contient pas le motif (1 3 2).

On peut aussi se poser le problème du tri par le réseau illustré par la figure 2 (un réseau parallèle de 4 files FIFO).

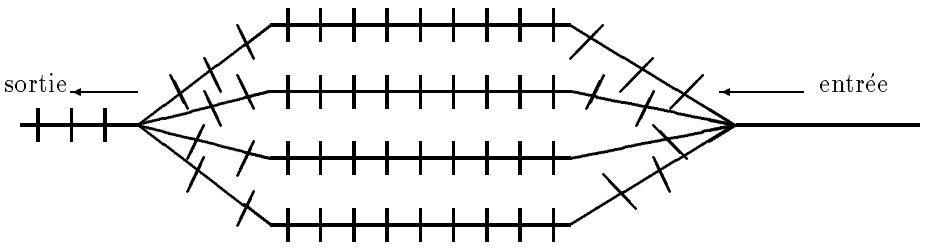


Fig. 2

Il est aussi bien connu qu'une permutation σ peut être triée par un réseau parallèle de m files si et seulement si σ ne contient pas de sous-suite décroissante de longueur supérieure ou égale à $m+1$, c'est-à-dire ne contient pas le motif $(m+1, m, m-1, \ldots, 1)$.

Sur ce sujet, on peut aussi citer les travaux récents de Dulucq, Gire et West [2], Gire [6], Even et Itai [3], Pratt [14], Simion et Schmidt [18], West [21, 22] et Zeilberger [23].

2. Sous-suites non décroissantes

À partir de maintenant, on ne considère que le motif $\tau = (1, 2, \ldots, k, k+1)$, c'est-à-dire que l'on étudie les permutations de $\mathfrak{S}_n$ qui ne contiennent pas de sous-suite croissante de longueur supérieure à k. On note $f(n, k)$ le nombre de telles permutations.

Il est bien connu que l'algorithme de Robinson-Schensted-Knuth permet de mettre en bijection une permutation $\sigma \in \mathfrak{S}_n$ avec une paire de tableaux de Young standard de même forme sur $\{1, 2, \ldots, n\}$. De plus la longueur de la première ligne de ces tableaux est égale à la longueur de la plus longue sous-suite croissante de σ.

On note L_n la longueur de la plus longue sous-suite croissante d'une permutation aléatoire $\sigma \in \mathfrak{S}_n$. Quelle est la distribution de L_n ?

Voici quelques résultats concernant la distribution de L_n :

(1) Il existe une constante $c > 0$ telle que $\frac{L_n}{\sqrt{n}} \to c$ en probabilité lorsque $n \to \infty$ (Hammersley [7]) ;
(2) $E(L_n) \geq 2\sqrt{n}$ (Logan et Slepp [10]) ;
(3) $E(L_n) \sim 2\sqrt{n}$ lorsque $n \to \infty$ (Veršik et Kerov [20]) ;
(4) Soit $\alpha > 1/3$. Alors il existe $\beta = \beta(\alpha) > 0$ tel que $\Pr(|L_n - E(L_n)| \geq n^\alpha) \leq e^{-n^\beta}$ (Frieze [4]).

Concernant $f(n, k)$, on peut citer le résultat de Regev [15, 16, 1] : pour k fixé, lorsque $n \to \infty$,

$$f(n, k) \sim \prod_{j-1}^{k-1} j! \frac{k^{\frac{1}{2}k^2} k^{2n}}{(2\pi)^{\frac{k-1}{2}} 2^{\frac{k^2-1}{2}} n^{\frac{k^2-1}{2}}}.$$

Ce résultat est obtenu en utilisant la formule de équerres pour les tableaux de Young standard et l'intégrale de Selberg [17].

3. L'intégrale de Selberg

Si on note $\Delta = \Delta(X_1, X_2, \ldots, X_n) = \prod_{1 \le h < j \le n}(X_h - X_j)$, l'intégrale de Selberg est donnée par :

$$\int_0^1 \cdots \int_0^1 |\Delta|^{2\gamma} \prod_{j=1}^{n-1} \{X_j^{\alpha-1}(1-X_j)^{\beta-1}\}\, dX_1 \cdots dX_n = \prod_{j=0}^{n-1} \frac{\Gamma(1+\gamma+j\gamma)\Gamma(\alpha+j\gamma)\Gamma(\beta+j\gamma)}{\Gamma(1+\gamma)\Gamma(\alpha+\beta+(n+j-1)\gamma)}.$$

On peut donner cette intégrale sous une autre forme :

$$\int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} |\Delta|^{2\gamma} \exp(-a\sum_{j=1}^{n} X_j^2)\, dX_1 \cdots dX_n = (2\pi)^{\frac{n}{2}} (2a)^{\frac{n}{2}(\gamma(n-1)+1)} \prod_{j=1}^{n} \frac{\Gamma(1+j\gamma)}{\Gamma(1+\gamma)}.$$

La solution de l'intégrale multiple précédente avait été conjecturée par Mehta [12] et est aussi connue sous le nom de conjecture de Mehta. Macdonald [11] a étendu cette conjecture aux groupes finis de réflexions et à d'autres groupes, la conjecture de Mehta correspondant au cas du groupe symétrique. Selberg et Bombieri ont montré dans une lettre non publiée que la preuve de la conjecture de Mehta pouvait être obtenue par des méthodes asymptotiques utilisant une intégrale de Selberg [17] plus simple, d'où le nom d'intégrale de Selberg utilisé dans ce texte.

4. Une autre méthode

Gessel [5] a prouvé que la série :

$$U_k(z) = \sum_{n=0}^{\infty} f(n,k) \frac{z^{2n}}{(n!)^2}$$

était égale à :

$$U_k(z) = \det(I_{h-j}(2z))_{1 \le h,j \le k} \quad \text{où} \quad I_\nu(t) = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{t\cos\theta + i\nu\theta}\, d\theta.$$

On obtient alors :

$$I_h(u) \approx \frac{e^u}{\sqrt{2\pi u}} \sum_{j=0}^{\infty} \frac{(-1)^j\, c(h,j)}{(2u)^j} \quad \text{lorsque} \quad u \to \infty \quad \text{avec} \quad c(h,0) = 1,$$

et donc :

$$U_k(z) \sim \frac{c(k)}{(2z)^{\lambda(k)}} \frac{e^{2kz}}{(4\pi z)^{\frac{k}{2}}}.$$

Le principe de la méthode est que sous des conditions discutées dans [13, Section 10], le comportement asymptotique à l'infini d'une fonction génératrice se traduit en une forme asymptotique des coefficients.

Principe 1. Sous certaines conditions de régularité, si $f(z) = \sum_0^\infty a_n z^n$ est une fonction entière et s'il existe C telle que

$$\left| f(z) - \frac{e^{\alpha z}}{z^k} \right| \le C \frac{e^{\alpha|z|}}{|z|^{k+1}},$$

pour z dans un voisinage convenable de $+\infty$, alors $a_n = \frac{\alpha^{n+k}}{(n+k)!}(1 + O(\frac{1}{\sqrt{n}}))$ lorsque $n \to \infty$.

Or on peut obtenir l'égalité suivante pour $U_k(z)$:

$$\begin{aligned} U_k(z) &= \sum_{n=0}^{\infty} f(n,k)\frac{z^{2n}}{(n!)^2} = \det(I_{h-j}(2z))_{1\le h,j\le k} \\ &= \frac{1}{(2\pi)^k k!}\int_{-\pi}^{\pi}\cdots\int_{-\pi}^{\pi} e^{2z\sum_{j=1}^{k}\cos\theta_j}\prod_{h\neq j}\left|e^{i\theta_h}-e^{i\theta_j}\right| d\theta_1\,\cdots\,d\theta_k. \end{aligned}$$

D'où le problème proposé :

Problème : Donner une évaluation fine de

$$\int_{-\pi}^{\pi}\cdots\int_{-\pi}^{\pi}\sum_{j=1}^{k}(\cos\theta_j)^{2n}\prod_{1\le h<j\le k}\left|e^{i\theta_h}-e^{i\theta_j}\right|^2 d\theta_1\,\cdots\,d\theta_k,$$

pour $k, n \in Z^+$ et $1 \le k < n$.

Bibliographie

[1] Beckner (W.) et Regev (A.). – Asymptotics and algebraicity of some generating functions. *Advances in Mathematics*, vol. 65, 1987, pp. 1–15.

[2] Dulucq (S.), Gire (S.), et West (J.). – Permutations à motifs exclus et cartes planaires non séparables. *In : Formal Power Series and Algebraic Combinatorics*, éd. par Barlotti (A.), Delest (M.), et Pinzani (R.), pp. 165–178. – 1993. Proceedings of FPACS'5, Florence (Italy).

[3] Even (S.) et Itai (A.), Kohavi (Z.) et Paz (A.) (édité par). – *Theory of machines and computation*, Chapitre Queues, stacks and graphs, pp. 71–86. – Academic Press, New-York, 1971.

[4] Frieze (A.). – On the length oh the longest monotone subsequence in a random permutation. *Annals of Applied Probability*, vol. 1, n° 2, 1991, pp. 301–305.

[5] Gessel (Ira M.). – Symmetric functions and P-recursiveness. *Journal of Combinatorial Theory, Series A*, vol. 53, 1990, pp. 257–285.

[6] Gire (S.). – *Arbres, permutations à motifs exclus et cartes planaires : quelques problèmes algorithmiques et combinatoires.* – Thesis, Université de Bordeaux I, 1993.

[7] Hammersley (J. M.). – A few seedlings of research. *In : Proceedings of the Sixth Berkeley Symposium on Mathematical Statistics and Probabilities*, pp. 345–394. – 1972.

[8] Knuth (Donald E.). – *The Art of Computer Programming.* – Addison-Wesley, 1968, vol. 1: Fundamental Algorithms. Second edition, 1973.

[9] Lifschitz (V.) et Pittel (B.). – The number of increasing subsequences of the random permutation. *Journal of Combinatorial Theory, Series A*, vol. 31, 1981, pp. 1–20.

[10] Logan (B. F.) et Slepp (L. A.). – A variational problem for Young tableaux. *Advances in Mathematics*, vol. 26, 1977, pp. 206–222.

[11] Macdonald (I. G.). – Some conjectures for root systems and finite reflexion groups. *SIAM Journal on Mathematical Analysis*, vol. 13, n° 6, 1982, pp. 988–1007.

[12] Mehta (M. L.). – *Random Matrices and the Statistical Theory of Energy Levels.* – Academic Press, New York, 1967.

[13] Odlyzko (A. M.). – Asymptotic enumeration methods. – Preprint, mars 1992. To appear as a chapter in the *Handbook of Combinatorics*, R. Graham, M. Grötschel and L. Lovász, (editors).

[14] Pratt (V. R.). – Computing permutations with double-ended queues, parallel stacks and parallel queues. *In : Proceedings of the Fifth Annual ACM Symposium on Theory of Computing*, pp. 268–277. – mai 1973.

[15] Regev (A.). – Asymptotic values for degrees associated with strips of Young diagrams. *Advances in Mathematics*, vol. 41, n° 2, 1981, pp. 115–136.

[16] Regev (A.). – Young-derived sequences of s_n-characters and their asymptotics. *In : Formal Power Series and Algebraic Combinatorics*, éd. par Barlotti (A.), Delest (M.), et Pinzani (R.), pp. 381–386. – 1993. Proceedings of FPACS'5, Florence (Italy).

[17] Selberg (A.). – Bemerkninger om et multipelt integral. *Nordisk Mat. Tidskr.*, vol. 26, 1944, pp. 71–78.

[18] Simion (R.) et Schmidt (F.). – Restricted permutations. *European Journal of Combinatorics*, vol. 6, 1985, pp. 383–406.

[19] Tarjan (R. E.). – Sorting using networks of queues and stacks. *Journal of the ACM*, vol. 19, n° 2, 1972, pp. 341–346.

[20] Veršik (A. M.) et Kerov (S. V.). – Asymptotics of the planchered measure of the symmetric group and the limiting form of Young tables. *Soviet Mathematical Doklady*, vol. 18, n° 2, 1977, pp. 527–531.

[21] West (J.). – *Permutations with restricted subsequences and stack-sortable permutations.* – Thèse de PhD, MIT, 1990.

[22] West (J.). – Sorting twice through a stack. *Theoretical Computer Science*, vol. 117, 1993, pp. 303–313.

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

Asymptotic estimates of Stirling numbers and related asymptotic problems

Nico M. Temme
CWI, Amsterdam

June 14, 1993

[summary by Helmut Prodinger]

Consider the two families of polynomials x^n and $(x)_n := x(x-1)\cdots(x-n+1)$. They are connected via the formulæ

$$x^n = \sum_{m=0}^{n} S(n,m)(x)_m$$

and

$$(x)_n = \sum_{m=0}^{n} s(n,m)x^m.$$

The coefficients $S(n,m)$ are called Stirling numbers of the second kind, and the coefficients $s(n,m)$ are called Stirling numbers of the first kind. This is the notation of Comtet [2]; other authors use different notations.

These numbers have some combinatorial meanings, e.g. $S(n,m)$ is the numbers of ways to partition the set $\{1,\ldots,n\}$ into exactly m nonempty subsets.

Example.

1234
1|234; 2|134; 3|124; 4|123; 12|34; 13|24; 14|23
1|2|34; 1|3|24; 1|4|23; 2|3|14; 2|4|13; 3|4|12
1|2|3|4,

whence $S(4,1)=1$, $S(4,2)=7$, $S(4,3)=6$, $S(4,4)=1$.

There is the handy recursion $S(n,m) = mS(n-1,m) + S(n-1,m-1)$ to compute them.

The (signless) Stirling numbers of the first kind $|s(n,k)|$ enumerate the number of permutations of the set $\{1,\ldots,n\}$ with exactly m cycles.

Example.

(1)(2)(3)
(12)(3), (13)(2), (23)(1)
(123), (132),

whence $|s(3,1)|=2$, $|s(3,2)|=3$, $|s(3,3)|=1$.

There is also an explicit formula

$$S(n,m) = \frac{1}{m!}\sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}k^n.$$

The asymptotic evaluation of the Stirling numbers has obtained some attention by several authors, but, since there are 2 parameters n and m involved, the range of validity is somehow limited. [1, 3, 4, 5, 6]

The paper [7] (on which the present talk is based) gives an expansion that is uniform in m, as $n \to \infty$.

The approach is based on the saddle point method, starting by expressing the Stirling numbers as Cauchy integrals by means of appropriate generating functions: (m fixed)

$$\sum_n s(n,m)\frac{x^n}{n!} = \frac{\big(\log(1+x)\big)^m}{m!},$$

$$\sum_n S(n,m)\frac{x^n}{n!} = \frac{\big(e^x-1\big)^m}{m!}.$$

Hence

$$S(n,m) = \frac{n!}{m!}\cdot\frac{1}{2\pi i}\oint \frac{\big(e^x-1\big)^m}{x^{n+1}}dx.$$

Rewrite it as

$$S(n,m) = \frac{n!}{m!}\cdot\frac{1}{2\pi i}\oint e^{\phi(x)}\frac{dx}{x},$$

with

$$\phi(x) = -m\log x + m\log(e^x-1).$$

The trick is to introduce a new complex variable t, via

$$\phi(x) = mt + (m-n)\log t + A,$$

where A is not depending on t. It is a linear combination of n and m.

THEOREM 1.

$$S(n,m) \sim e^A m^{n-m}\sqrt{\frac{t_0}{(1+t_0)(x_0-t_0)}}\binom{n}{m}.$$

Here x_0 is the saddle point and t_0 the corresponding t–value. For example, as $m \sim n$, the square root expression may be replaced asymptotically by 1.

The approach for the Stirling numbers of the first kind is similar. The function $\phi(x)$ is now $\phi(x) = n\log(1+t) - m\log t + B$.

THEOREM 2.

$$s(n+1,m+1) \sim (-1)^{n-m}e^B\frac{1}{x_0}\sqrt{\frac{m(n-m)}{n\phi''(x_0)}}\binom{n}{m}$$

Again, if m goes to infinity within a certain ratio of n, the quantities B and x_0 may be replaced by simpler expressions.

Higher order approximations and related topics were also discussed.

Bibliography

[1] Bleick (W. E.) and Wang (P. C. C.). – Asymptotics of the Stirling numbers of the second kind. *Proceedings of the American Mathematical Society*, vol. 42, 1974, pp. 575–580.

[2] Comtet (L.). – *Advanced Combinatorics.* – Reidel, Dordrecht, 1974.

[3] Hsu (L. C.). – Note on an asymptotic expansion of the n-th difference of zero. *Annals of Mathematical Statistics*, vol. 19, 1948, pp. 273–277.

[4] Knessl (C. H.) and Keller (J. B.). – Stirling number asymptotics form recursion equations using the ray method. *Studies in Applied Mathematics*, vol. 84, 1991, pp. 43–56.

[5] Moser (Leo) and Wyman (Max). – Asymptotic development of the Stirling numbers of the first kind. *Journal of the London Mathematical Society*, vol. 33, 1958, pp. 133–146.

[6] Moser (Leo) and Wyman (Max). – Stirling numbers of the second kind. *Duke Mathematical Journal*, vol. 25, 1958, pp. 29–43.

[7] Temme (N. M.). – Asymptotic estimates of Stirling numbers. *Studies in Applied Mathematics*, vol. LXXXIX, n° 3, 1993, pp. 233–244.

Exponentially-improved asymptotic solutions of ordinary differential equations

Adri Olde Daalhuis
CWI, Amsterdam

June 14, 1993

[summary by Bruno Salvy[1]]

Abstract

Re-expansions are found for the optimal remainder terms in the well-known asymptotic series solutions of homogeneous linear differential equations of the second order in the neighbourhood of an irregular singularity of rank one. The re-expansions are in terms of generalized exponential integrals and have greater regions of validity than the original expansions, as well as being considerably more accurate and providing a smooth interpretation of the Stokes phenomenon. They are also of strikingly simple form. Also found are explicit asymptotic expansions for the higher coefficients of the original asymptotic solutions.

The object of study is a linear ordinary differential operator

$$L = \frac{d^2}{dz^2} + f(z)\frac{d}{dz} + g(z),$$

where the coefficients $f(z)$ and $g(z)$ have Laurent expansions in a non-empty neighbourhood of infinity

$$f(z) = \sum_{s\geq 0} \frac{f_s}{z^s}, \quad g(z) = \sum_{s\geq 0} \frac{g_s}{z^s},$$

and infinity is an irregular singular point of rank 1, which means that the asymptotic expansion of two distinct solutions are given by

$$w_1 \sim e^{\lambda_1 z} z^{\mu_1} \sum_{s\geq 0} \frac{a_{s,1}}{z^s}, \quad |\operatorname{Arg}[(\lambda_2-\lambda_1)z]| \leq 3\pi/2 - \delta,$$
$$w_2 \sim e^{\lambda_2 z} z^{\mu_2} \sum_{s\geq 0} \frac{a_{s,2}}{z^s}, \quad |\operatorname{Arg}[(\lambda_1-\lambda_2)z]| \leq 3\pi/2 - \delta,$$

where δ is an arbitrary small real number.

It is known that these expansions are in general divergent, and several methods to get numerical values out of them have been studied. The most widely known is *summation to the least term* where one adds up the contributions from $a_{s,i}/z^s$ until they start increasing. The main result of this paper is an asymptotic expansion of the remainder term which makes it possible to get even more precision than summation to the least term.

The exponents λ_1, λ_2 are roots of the characteristic equation

$$\lambda^2 + f_0\lambda + g_0 = 0,$$

and by changing z into $z/(\lambda_2-\lambda_1)$ one may assume $\lambda_2 - \lambda_1 = 1$.

[1]This very concise summary was written several months after the talk without very precise notes. It should be viewed mainly as a pointer to the reference [1].

Since $e^{2i\pi\mu_1}w_1(ze^{-2i\pi})$ has the same asymptotic expansion as w_1 and is also a solution of the operator, one obtains the following *connection formulæ*:

$$w_1(z) = e^{2i\pi\mu_1}w_1(ze^{-2i\pi}) + C_1 w_2(z),$$
$$w_2(z) = e^{-2i\pi\mu_2}w_2(ze^{2i\pi}) + C_2 w_1(z).$$

We can now state the main result of [1].

THEOREM 1. *Define* $R_n^{(1)}(z)$ *and* $R_n^{(2)}(z)$ *by*

$$w_1 = e^{\lambda_1 z}z^{\mu_1}\sum_{s=0}^{n-1}\frac{a_{s,1}}{z^s} + R_n^{(1)}(s), \quad w_2 = e^{\lambda_2 z}z^{\mu_2}\sum_{s=0}^{n-1}\frac{a_{s,2}}{z^s} + R_n^{(2)}(s),$$

where $n = |z| + \alpha$ *and* α *is bounded. Then*

$$R_n^{(1)}(z) = (-1)^{n-1}ie^{(\mu_2-\mu_1)\pi i}e^{\lambda_2 z}z^{\mu_2}\left\{C_1\sum_{s=0}^{m-1}(-1)^s a_{s,2}\frac{F_{n+\mu_2-\mu_1-s}(z)}{z^s} + R_{m,n}^{(1)}(z)\right\},$$
$$R_n^{(2)}(z) = (-1)^{n}ie^{(\mu_2-\mu_1)\pi i}e^{\lambda_1 z}z^{\mu_1}\left\{C_2\sum_{s=0}^{m-1}(-1)^s a_{s,1}\frac{F_{n+\mu_1-\mu_2-s}(ze^{-\pi i})}{z^s} + R_{m,n}^{(2)}(z)\right\},$$

where m *is an arbitrary fixed non-negative integer, and for large* $|z|$

$$R_{m,n}^{(1)}(z) = O(e^{-|z|-z}z^{-m}), \qquad |\operatorname{Arg} z| \le \pi,$$
$$R_{m,n}^{(1)}(z) = O(z^{-m}), \qquad \pi \le |\operatorname{Arg} z| \le \frac{5}{2}\pi - \delta,$$
$$R_{m,n}^{(2)}(z) = O(e^{-|z|+z}z^{-m}), \qquad 0 \le \operatorname{Arg} z \le 2\pi,$$
$$R_{m,n}^{(2)}(z) = O(z^{-m}), \qquad -\frac{3}{2}\pi + \delta \le \operatorname{Arg} z \le 0 \text{ and } 2\pi \le \operatorname{Arg} z \le \frac{7}{2}\pi - \delta,$$

uniformly with respect to $\operatorname{Arg} z$ *in each case.*

In this theorem F denotes the following generalized exponential integral

$$F_p(z) = \frac{e^{-z}}{2\pi}\int_0^\infty \frac{e^{-zt}t^{p-1}}{1+t}dt.$$

Note that the coefficients that appear in the expansion are precisely the coefficients of the expansions of w_1 and w_2. This is related to the following older theorem of Olver.

THEOREM 2. *Let* m *be an arbitrary fixed non-negative integer. Then as* $s \to \infty$,

$$a_{s,1} = (-1)^s\frac{e^{(\mu_2-\mu_1)\pi i}}{2\pi i}\left\{C_1\sum_{j=0}^{m-1}(-1)^j a_{j,2}\Gamma(s+\mu_2-\mu_1-j) + \Gamma(s+\mu_2-\mu_1-m)O(1)\right\},$$
$$a_{s,2} = -\frac{1}{2\pi i}\left\{C_2\sum_{j=0}^{m-1}a_{j,1}\Gamma(s+\mu_1-\mu_2-j) + \Gamma(s+\mu_1-\mu_2-m)O(1)\right\}.$$

Bibliography

[1] Daalhuis (A. B. Olde) and Olver (F. W. J.). – Exponentially-improved asymptotic solutions of ordinary differential equations II: irregular singularities of rank one. – Preprint, 1993.

Part IV

Analysis of Algorithms and Data Structures

Analytic Analysis of Algorithms

Philippe Flajolet
INRIA Rocquencourt

September 16, 1992

[summary by Pierre Nicodème]

Abstract

Symbolic methods in combinatorial analysis permit to express directly the counting generating functions of wide classes of combinatorial structures. Asymptotic methods based on complex analysis permit to extract directly coefficients of structurally complicated generating functions without a need for explicit coefficient expansions.

Three major groups of problems relative to algebraic equations, differential equations, and iteration are presented. The range of applications includes formal languages, tree enumerations, comparison-based searching and sorting, digital structures, hashing and occupancy problems.

This summary is based on [2].

Introduction

Quicksort. The classical analysis of the Quicksort algorithm results in solving a recurrence based on the recursive structure of the algorithm,

$$\bar{Q}_n = p_n + \sum_{k=0}^{n-1} \pi_{n,k}[\bar{Q}_k + \bar{Q}_{n-1-k}]. \tag{1}$$

There $\bar{Q}_n$ is the expected number of comparisons, $\pi_{n,k}$ is the probability that the partitioning stage splits the file into two subfiles of sizes k and $n-1-k$, and the quantity p_n represents the cost for partitioning.

There is an alternative approach to this problem.

Introduce the *generating function* (GF) of the mean values

$$Q(z) = \sum_{n=0}^{\infty} \bar{Q}_n z^n, \tag{2}$$

and set similarly $p(z) = \sum_{n\geq 0} p_n z^n$. Then, the equation corresponding to recurrence (1) is

$$Q(z) = p(z) + 2\int_0^z Q(t)\,\frac{dt}{1-t}. \tag{3}$$

The solution of this equation is

$$Q(z) = \frac{1}{(1-z)^2}\int_0^z \frac{d}{dt}\{p(t)\}\,(1-t)^2 dt. \tag{4}$$

and with $p(z) = z^2/(1-z)^2$,

$$Q(z) = 2\frac{\log(1-z)^{-1}}{(1-z)^2} - \frac{2z}{(1-z)^2}. \tag{5}$$

If we expand $Q(z)$, we retrieve again the solution of recurrence (1) that involves the harmonic numbers.

The solution expressed by (5) can be used to produce direct asymptotic results from the generating function itself, without any need for explicit expansions. The key observation is that it suffices to examine the generating function *locally* near its *singularity* at $z = 1$ and apply systematic translation mechanisms.

The translation from the local singular behaviour of a function to the asymptotics of its coefficients is a powerful mechanism. General rules valid under simple conditions (analytic continuation) apply, like for instance, the relation

$$[z^n]\ \frac{1}{(1-z)^\alpha}(\log(1-z)^{-1})^k \sim \frac{n^{\alpha-1}}{\Gamma(\alpha)}(\log n)^k.$$

1. Symbolic Methods in Combinatorial Analysis

The very powerful symbolic methods in combinatorial analysis may be summarized as follows:

PRINCIPLE. A number of set-theoretic constructions like union, cartesian product, sequence set, cycle set, power set, substitution have direct translation into generating function equations. Thus, a counting problem which is expressible in the language of these constructions can be translated systematically (and automatically) into generating function equations.

Given a class $\mathcal{F}$ of combinatorial structures, we let $\mathcal{F}_n$ denote the collection of objects of size n, and set $F_n = \mathrm{card}(\mathcal{F}_n)$. The *ordinary generating function* (OGF) and *exponential generating function* (EGF) are defined respectively to be

$$F(z) = \sum_{n\geq 0} F_n z^n \qquad \text{and} \qquad \hat{F}(z) = \sum_{n\geq 0} F_n \frac{z^n}{n!}. \tag{6}$$

A combinatorial construction is *admissible* if it admits a translation into generating functions.

THEOREM 1 (ADMISSIBLE CONSTRUCTIONS FOR OGF'S). *For unlabelled structures, the constructions of union, cartesian product, sequence, cycle, set, multiset, substitution are admissible. The translations into ordinary generating functions are given by the following table*

Construction	*Translation (OGF)*
$\mathcal{F} = \mathcal{G} \cup \mathcal{H}$	$F(z) = G(z) + H(z)$
$\mathcal{F} = \mathcal{G} \times \mathcal{H}$	$F(z) = G(z) \cdot H(z)$
$\mathcal{F} = \mathit{sequence}(\mathcal{G}) = \mathcal{G}^*$	$F(z) = \frac{1}{1-G(z)}$
$\mathcal{F} = \mathit{set}(\mathcal{G})$	$F(z) = \exp(G(z) - \frac{1}{2}G(z^2) + \frac{1}{3}G(z^3) - \cdots)$
$\mathcal{F} = \mathit{multiset}(\mathcal{G})$	$F(z) = \exp(G(z) + \frac{1}{2}G(z^2) + \frac{1}{3}G(z^3) + \cdots)$
$\mathcal{F} = \mathit{cycle}(\mathcal{G})$	$F(z) = \log(1 - G(z))^{-1} + \cdots$
$\mathcal{F} = \mathcal{G}[\mathcal{H}]$	$F(z) = G(H(z))$

THEOREM 2 (ADMISSIBLE CONSTRUCTIONS FOR EGF'S). *For labelled structures, the constructions of union, partitional product, sequence, cycle, set, substitution are admissible. The translations into exponential generating functions are given by the following table*

Construction	*Translation (EGF)*
$\mathcal{F} = \mathcal{G} \cup \mathcal{H}$	$\hat{F}(z) = \hat{G}(z) + \hat{H}(z)$
$\mathcal{F} = \mathcal{G} * \mathcal{H}$	$\hat{F}(z) = \hat{G}(z) \cdot \hat{H}(z)$
$\mathcal{F} = \mathit{sequence}(\mathcal{G}) = \mathcal{G}^*$	$\hat{F}(z) = \frac{1}{1-\hat{G}(z)}$
$\mathcal{F} = \mathit{set}(\mathcal{G})$	$\hat{F}(z) = \exp(\hat{G}(z))$
$\mathcal{F} = \mathit{cycle}(\mathcal{G})$	$\hat{F}(z) = \log(1 - \hat{G}(z))^{-1}$
$\mathcal{F} = \mathcal{G}[\mathcal{H}]$	$\hat{F}(z) = \hat{G}(\hat{H}(z))$

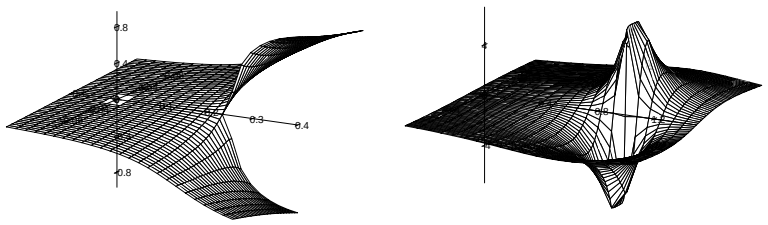


FIGURE 1
A display of the imaginary parts of two generating functions, $f(z) = \frac{1-\sqrt{1-4z}}{2z}$ and $g(z) = \frac{1}{1-z}$. The function $f(z)$ [left] is the ordinary generating function of binary trees with a singularity at $\rho = 1/4$ which is a branch point of the $\sqrt{\ }$ type. The function $g(z)$ [right] is the exponential generating function of permutations with a singularity at $\rho = 1$ of a polar type. The singularities are reflected at the level of coefficients, $[z^n]f(z) \sim \frac{4^n}{\sqrt{\pi n^3}}$ and $[z^n]g(z) = 1$.

2. Complex Analysis and Asymptotics

Complex analytic methods permit to represent coefficients of generating functions and many combinatorial sums as integrals of an analytic function in the complex plane. The choice of a suitable contour of integration often leads to highly non trivial asymptotic results.

Singularity analysis. Most functions occurring in combinatorial enumeration problems are built by operators from standard functions that exist over the whole of the complex plane. They thus tend to exist in larger areas of the complex plane. The method of *singularity analysis* is well suited to extracting coefficients of functions lying in a class that enjoys interesting closure properties.

Saddle point integrals. The saddle point method is useful for the computation of coefficients of whole classes of entire functions, with the following asymptotics:

THEOREM 3 (SADDLE POINT COEFFICIENT ASYMPTOTICS). *For a function $f(z)$ to which the saddle point method applies, one has*

$$[z^n]f(z) \sim \frac{f(\zeta)}{\sqrt{2\pi C}\zeta^{n+1}} \quad \textit{where} \quad C = \frac{d^2}{dz^2}\log\frac{f(z)}{z^{n+1}}\bigg|_{z=\zeta},$$

and $\zeta = \zeta_n$ is the smallest real root of $\frac{d}{dz}\log\frac{f(z)}{z^{n+1}}$.

Although leading to difficult questions, the method may be applied to dimensions higher than 1 dimensional saddle [3] [6].

3. Algebraic Functions and Implicit Functions

Regular languages can be specified either by regular expressions or by finite automata. The corresponding GF's either appear as built from the variable z by means of rational operations ($+$, $\times$, quasi-inverse $Q(y) = (1-y)^{-1}$) or as components of linear systems of equations (over $\mathbb{Z}[x]$). At any rate, they are rational.

An immediate consequence of the partial fraction decomposition of rational functions is the following.

THEOREM 4 (RATIONAL ASYMPTOTICS). *The coefficients of a rational function of $\mathbb{Q}(z)$ are a finite linear combination of 'exponential polynomials' of the form*

$$\lambda\,\omega^n n^k, \tag{7}$$

with λ, ω algebraic numbers and k an integer.

Context free languages lead to polynomial nonlinear equations, provided the grammar is unambiguous or we count words with their multiplicities. Thus, the generating function of a context free language is algebraic and the following theorem holds:

THEOREM 5 (ALGEBRAIC ASYMPTOTICS). *The coefficients of a $\mathbb{Q}(z)$-algebraic function are asymptotic to a sum of 'algebraic elements' of the form*

$$\frac{\lambda}{\Gamma(r/s+1)}\omega^n n^{r/s}, \tag{8}$$

where λ, ω are algebraic numbers, and the exponent r/s is a rational number.

Implicit functions. Functions defined implicitly tend to have singularities like those of algebraic functions, involving fractional exponents. This is reflected by the asymptotics of their coefficients of the form $\omega^n n^{-r/s}$. Such a property also holds for many functions satisfying finite and infinite functional equations involving terms like $f(z^2), f(z^3)$ provided that their radius of convergence is < 1.

4. Holonomic Functions and Differential Equations

Functions satisfying differential equations with polynomial coefficients are sometimes called $\mathcal{D}$-finite and their coefficient sequences which satisfy recurrences with polynomial (in n) coefficients are then called $\mathcal{P}$-recursive. These notions are formalized by the concept of *holonomy* introduced in this range of problems by Zeilberger.

DEFINITION 1. A series $f(z_1, z_2, \ldots, z_r) \in \mathbb{C}[[z_1, z_2, \ldots, z_r]]$ is said to be *holonomic* iff the infinite collection of its partial derivatives

$$\frac{\partial^{j_1}}{\partial z^{j_1}}\frac{\partial^{j_2}}{\partial z^{j_2}}\cdots\frac{\partial^{j_r}}{\partial z^{j_r}} f(z_1, z_2, \ldots, z_r)$$

spans a finite dimensional vector space over the field of rational fractions $\mathbb{C}(z_1, z_2, \ldots, z_r)$.

A sequence $f_{n_1,n_2,\ldots,n_r}$ is holonomic iff its generating function

$$f(z_1, z_2, \ldots, z_r) = \sum_{n_1,n_2,\ldots,n_r} f_{n_1,n_2,\ldots,n_r} z_1^{n_1} z_2^{n_2} \cdots z_r^{n_r}$$

is holonomic.

The major closure theorem here is due to Stanley, Lipschitz, and Zeilberger [4, 5, 7, 8].

THEOREM 6 (HOLONOMIC CLOSURE). *Holonomic functions are closed under sums, Cauchy products, Hadamard products, diagonals, algebraic substitutions, integration, differentiation, direct and inverse Laplace transforms.*

THEOREM 7 (HOLONOMIC ASYMPTOTICS). *A holonomic sequence f_n is asymptotic to a sum of elements of the form*

$$\lambda(n!)^{r/s} e^{Q(n^{1/m})} \omega^n n^{\alpha} (\log n)^k,$$

where r, s, m, k are integers, Q is a polynomial and λ, ω, α are complex numbers.

In our perspective, this theorem relates to the classification of singularities of linear differential equations. The theory of linear differential equations with analytic coefficients distinguishes for solutions of such equations two cases, the regular case and the irregular case. The method of singularity analysis and the method of saddle point integrals are applicable each in one of the two cases.

For instance the expected cost of a partial match query in a quadtree (alternatively a k-d-tree) when a proportion of $\frac{1}{2}$ or $\frac{2}{3}$ of the coordinates is known is of the order of

$$n^{(\sqrt{17}-3)/2} \qquad \text{and} \qquad n^{\theta-1} \quad \text{with} \quad \theta = \left(\frac{109}{27}+\sqrt{\frac{1320}{81}}\right)^{1/3} + \left(\frac{109}{27}-\sqrt{\frac{1320}{81}}\right)^{1/3}.$$

Such algebraic numbers in the exponents are typical of $\mathbb{Q}(z)$ holonomic functions.

5. Functional Equations and Iteration

We confine our discussion to *linear functional equations* of the form

$$f(z) = a(z) + b(z)f(\sigma(z)), \tag{9}$$

where $f(z)$ is the unknown function, and a, b, σ are explicitly known. In the functional equation of (9), everything depends crucially on the dynamics of the iterates of σ. In a few important cases, the iterates are explicit, and one general method available relies on the Mellin transform.

Explicit iterations. The analysis of digital tries furnishes an example of the situation where the iteration of $\sigma(z)$ is explicit. The recurrence of expected path length in tries is of a probabilistic divide-and-conquer type,

$$f_n = n - \delta_{n,1} + 2\sum_{k=0}^{n} \pi_{n,k} f_k \qquad \text{with } \pi_{n,k} = \frac{1}{2^n}\binom{n}{k}.$$

The corresponding EGF satisfies

$$f(z) = z(e^z - 1) + 2e^{z/2} f(\frac{z}{2}).$$

The equation is solved by iteration, after which the solution can be expanded.

The method is also applicable to wide classes of divide-and-conquer recurrences which are almost invariably found to give rise to periodic fluctuations involving fractals.

Implicit iterations. When the iterates $\sigma^{\langle j\rangle}(z)$ admit of no simple explicit form, one often has to resort to an analysis of individual terms in the sum (9), normally by the battery of complex analysis techniques examined so far.

At the moment, a complete classification of the various cases of (9) is still lacking. Some cases appear to involve the theory of analytic iteration and some divergent series. We nonetheless have a number of useful and general tools available in the form of Mellin transforms and iteration theory of analytic functions.

6. Automatic Analysis

The approach of finding general decidable asymptotic properties of combinatorial structures has been prolonged. Flajolet, Salvy and Zimmermann [1] have designed a system called Lambda-Upsilon-Omega ($\Lambda\Upsilon^{\Omega}$) that implements a number of decision procedures on combinatorial structures like the ones discussed here. The kernel specification language consists of the constructions of union, product, sequence, sets, multisets and cycles described in Section 1. The $\Lambda\Upsilon^{\Omega}$ system also makes provisions for specifying traversal algorithms on the structures.

Bibliography

[1] Flajolet (P.), Salvy (B.), and Zimmermann (P.). – Automatic average-case analysis of algorithms. *Theoretical Computer Science, Series A*, vol. 79, n° 1, February 1991, pp. 37–109.

[2] Flajolet (Philippe). – Analytic analysis of algorithms. In Kuich (W.) (editor), *Automata, Languages and Programming, Lecture Notes in Computer Science*, pp. 186–210. – 1992. Proceedings of the 19th International Colloquium, Vienna, July 1992. (Invited lecture).

[3] Gardy (Danièle). – Méthode de col et lois limites en analyse combinatoire. *Theoretical Computer Science*, vol. 92, n° 2, 1992, pp. 261–280.

[4] Lipshitz (L.). – The diagonal of a D-finite power series is D-finite. *Journal of Algebra*, vol. 113, 1988, pp. 373–378.

[5] Lipshitz (L.). – D-finite power series. *Journal of Algebra*, vol. 122, 1989, pp. 353–373.

[6] McKay (Brendan D.). – The asymptotic numbers of regular tournaments, Eulerian digraphs and Eulerian oriented graphs. *Combinatorica*, vol. 10, n° 4, 1990, pp. 367–377.

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

[8] Zeilberger (Doron). – A holonomic systems approach to special functions identities. *Journal of Computational and Applied Mathematics*, vol. 32, 1990, pp. 321–368.

The Height of a Random Tree

Tomasz Łuczak
Adam Mickiewicz University, Poznan, Poland

March 29, 1993

[summary by Wojtek Szpankowski]

1. Introduction

Let T_n be a random labelled rooted tree on the vertex set $[n] = \{1, 2, \ldots, n\}$ with the root $v_0 \in [n]$ (here and below we assume that a root is always the vertex number 1). The limit distribution of the height of $\tilde{H} = \tilde{H}(n)$ of T_n, was found by Rényi and Szekeres [3] who proved the following result.

THEOREM 1. *For every constant $\beta > 0$*

$$\begin{aligned}\lim_{n\to\infty}(\tilde{H} = \lfloor\sqrt{2n}/\beta\rfloor) &= 2\sqrt{\frac{2\pi}{n}}\beta^2\sum_{i=1}^{\infty}\left(2i^4\pi^4\beta - 3i^2\pi^2\right)\exp(-\beta\pi^2 i^2)\\ &= \sqrt{\frac{8}{n\beta}}\sum_{i=1}^{\infty}\left(\frac{2i^4}{\beta} - 3i^2\right)\exp\left(-\frac{i^2}{\beta}\right),\end{aligned}$$

where the convergence is uniform for $\beta \in (c, C)$ for every constants $0 < c < C < \infty$.

Furthermore, they proved that the s-th moment of random variable $h(T_n)/\sqrt{2n}$ tends to $2\Gamma(s/2+1)(s-1)\zeta(s)$. In particular, for the expectation and the variance of $h(T_n)$, one obtains

$$\begin{aligned}\lim_{n\to\infty}\frac{\mathrm{E}\,h(T_n)}{\sqrt{n}} &= \sqrt{2\pi} = 2.50663\ldots\\ \lim_{n\to\infty}\frac{\mathrm{Var}\,h(T_n)}{n} &= \frac{2\pi(\pi-3)}{3} = 0.29655\ldots.\end{aligned}$$

(See also [1] for a generalization of this result to other simply generated families of trees.)

Consider now the following greedy algorithm. For a tree T with the root v_0 let $\mathcal{F}(T)$ be the forest of rooted trees obtained from T by removing the root, where as the root of a tree $T' \in \mathcal{F}(T)$ we choose the vertex adjacent to v_0 in T. The height of a tree can be estimated by using the following simple greedy algorithm, which finds in a tree a path starting from the root. The algorithm starts with a tree $T^{(0)} = T$ on n vertices, removes its root v_0, chooses the largest tree $T^{(1)}$ from $\mathcal{F}(T^{(0)})$ (if there are more than one of them it picks the one with the lexicographically first root), appends its root to a path, and repeats this procedure until for some h tree $T^{(h)}$ consists only of one vertex.

This talk concerns the study of the height $H = H(n)$ found in a random tree by the above greedy algorithm. The limiting distribution of H is found and it is shown that the expected value of $H/\sqrt{n}$ tends to an absolute constant C, where

$$C = \frac{\sqrt{2\pi}}{2\sqrt{2} - \ln(3+2\sqrt{2})} = 2.353139\ldots.$$

Thus, on average, the algorithm finds a path whose length is roughly 93% of the expected height of the tree.

2. Main Results

We need some definitions. Let us define recursively two sequences of random variables $\{\hat{H}_i\}$ and $\{W_i\}$ by setting $\hat{H}_0 = \min_j \{|T_n^{(j)}| \le n/2\}$, $W_0 = |T_n^{(\hat{H}_0)}|$ whereas for $i \ge 1$ let

$$\hat{H}_i = \min_j \{|T_n^{(j)}| \le W_{i-1}/2\}$$

and $W_i = |T_n^{(\hat{H}_i)}|$. Furthermore, set $H_0 = \hat{H}_0$ and $H_i = \hat{H}_i - \hat{H}_{i-1}$ for $1 \le r \le n-1$. Thus, W_i denotes the size of the tree $T_n^{(k)}$ when it first drops under $W_{i-1}/2$ and H_i is the number of steps of the algorithm between two such moments. Note that for every $i \ge 0$ we have $W_i \le 2^{-i-1}n$.

Clearly, the length of the path found by the algorithm can now be written as a sum of H_i's, so

$$\begin{aligned} \Pr(H > k) &= \Pr(\sum_{i\ge 0} H_i > k) \\ &= \Pr(H_0 > k) + \sum_{j\ge 1} \Pr(\sum_{i=0}^{j} H_i > k \wedge \sum_{i=0}^{j-1} H_i \le k) \end{aligned}$$

In order to characterize the behaviour of the probabilities $\Pr(\sum_{i=0}^{j} H_i > k \wedge \sum_{i=0}^{j-1} \le k)$ let us define an integral operator A by setting

$$(Ag)(x) = \int_0^x \int_{1/4}^{1/2} f(z,y) g((x-z)/\sqrt{y}) dy\, dz\ ,$$

where f is a function defined as

$$f(x,y) = \frac{1}{2\pi} \int_{1/2-y}^{y} \frac{x}{t^{3/2} y^{3/2} (1-t-y)^{3/2}} \exp\left(-\frac{x^2}{2(1-y-t)}\right) dt.$$

Furthermore, let

$$g_0(x) = \int_x^\infty \int_{1/4}^{1/2} f(z,y) dy\, dz,$$

and for $j \ge 1$

$$g_j = A g_{j-1} = A^j g_0.$$

The next result shows that functions g_j are closely related to our problem.

LEMMA 1. *For every $x > 0$ we have*

$$\Pr(H_0 > \lfloor x\sqrt{n} \rfloor) = (1 + o(1)) g_0,$$

and for $j \ge 1$

$$\Pr(\sum_{i=0}^{j} H_i > \lfloor x\sqrt{n} \rfloor \wedge \sum_{i=0}^{j-1} H_i \le \lfloor x\sqrt{n} \rfloor) = (1 + o(1)) g_i(x)\,,$$

where, for given constants c, C, the quantity $o(1)$ tends to 0 uniformly for every $x \in (c, C)$.

As a consequence of Lemma 1 one proves the limiting distribution of H.

THEOREM 2. *For every constant $x \ge 0$*

$$\lim_{n\to\infty} \Pr(H > x\sqrt{n}) = h(x),$$

where

$$h(x) = \sum_{j=0}^{\infty} g_j(x) = \sum_{j=0}^{\infty} (A^j g_0)(x).$$

In particular, the function h is the only continuous solution of the integral equation

$$\begin{aligned} h(x) &= g_0(x) + (Ah)(x) \\ &= \int_x^\infty \int_{1/4}^{1/2} f(z,y)dy\,dz + \int_0^x \int_{1/4}^{1/2} f(z,y)h((x-z)/\sqrt{y})dy\,dz\ , \end{aligned}$$

Having computed the distribution of H it is not hard to guess the value of its mean. Clearly, $\mathrm{E}\,H/\sqrt{n}$ should converge to the expected value of the random variable Z, where $P(Z > x) = h(x)$ and $h(x)$ is given by Theorem 2. But $xh(x) \to 0$ as $x \to \infty$ (as a matter of fact Theorem 1 says that the probability that the actual height of a random tree is larger than x decreases exponentially with x), so

$$\mu = \mathrm{E}\,Z = \int_0^\infty h(x)dx.$$

Integrating both sides of the formula on $h(x)$ in Theorem 2, after elementary calculations, one obtains

$$\mu = \int_0^\infty \int_{1/4}^{1/2} xf(x,y)dy\,dx + \mu \int_0^\infty \int_{1/4}^{1/2} \sqrt{y}f(x,y)dy\,dx.$$

Consequently,

$$\mu = \frac{\int_0^\infty \int_{1/4}^{1/2} xf(x,y)dy\,dx}{1 - \int_0^\infty \int_{1/4}^{1/2} \sqrt{y}f(x,y)dy\,dx}\ .$$

Finally, one proves the following result.

THEOREM 3. *The average height obtained by the greedy algorithm is*

$$\lim_{n\to\infty} \frac{\mathrm{E}\,H}{\sqrt{n}} = \mu\ ,$$

where

$$\mu == \frac{\int_0^\infty \int_{1/4}^{1/2} xf(x,y)dy\,dx}{1 - \int_0^\infty \int_{1/4}^{1/2} \sqrt{y}f(x,y)dy\,dx} = \frac{\sqrt{2\pi}}{2\sqrt{2} - \ln(3+2\sqrt{2})} = 2.353139\ldots.$$

This completes our presentation of main results of the talk. More details can be found in [2].

Bibliography

[1] Flajolet (Philippe), Gao (Zhicheng), Odlyzko (Andrew), and Richmond (Bruce). – *The Distribution of Heights of Binary Trees and Other Simple Trees.* – Research Report n° 1749, Institut National de Recherche en Informatique et en Automatique, September 1992. 12 pages. Accepted for Publication in *Combinatorics, Probability, and Computing.*

[2] Luczak (T.). – A greedy algorithm estimating the height of random trees. – Preprint, 1993.

[3] Rényi (A.) and Szekeres (G.). – On the height of trees. *Australian Journal of Mathematics*, vol. 7, 1967, pp. 497–507.

Some results about quadtrees

Louise Laforest
UQAM, Montréal

June 7, 1993

[summary by Bruno Salvy]

Introduction

The quadtree data structure is a natural generalization of binary search trees in higher dimension used to store multidimensional data. The average-case complexity of algorithms operating on quadtrees is directly related to the expectation of some parameters such as path length, number of leaves, number of nodes with k children, and so on.

Parameters studied here are *additive parameters* that can be computed recursively by adding a toll number p_n depending only on the size n of the tree to the values of the parameter on the subtrees. For instance the number of leaves is obtained with $p_n = \delta_{n,1}$. The expectation of such a parameter e_n obeys the following classical recurrence [2, 4]

$$e_n = p_n + 2^d \sum_{k=0}^{n-1} \pi_{n,k} e_k, \tag{1}$$

where d is the dimension ($d = 2$ for standard quadtrees) and $\pi_{n,k}$ is the probability that a quadtree of size n has its first subtree of size k. This probability is given by the following explicit formula [1, 2, 4]

$$\begin{aligned} \pi_{n,k} &= \frac{1}{n} \sum_{k<i_1\le i_2\le\cdots\le i_d\le n} \frac{1}{i_1\cdots i_n}, \\ &= \binom{n-1}{k} \sum_{j=0}^{n-1-k} \binom{n-1-k}{j} \frac{(-1)^j}{(k+j+1)^d}. \end{aligned}$$

In dimension 2, this reduces to

$$\pi_{n,k} = \frac{1}{n}[H_n - H_k],$$

H_n denoting the n-th harmonic number.

Taking generating functions, formula (1) can be seen to be equivalent to a simple integral equation,

$$e(z) = p(z) + 2^d \mathbf{J}^{d-1}\mathbf{I}e(z), \tag{2}$$

where $\mathbf{J}$ and $\mathbf{I}$ are the following integral operators

$$\mathbf{I}f(z) = \int_0^z f(t)\frac{dt}{1-t}, \quad \mathbf{J}f(z) = \int_0^z f(t)\frac{dt}{t(1-t)}.$$

Equation (2) is easily translated into a linear differential equation of order d. Combined with singularity analysis, this differential equation is the basis of most of the analysis in [2].

1. A simplifying remark

At this stage, G. Labelle and L. Laforest [3] introduce the following change of variable and unknown function:

$$e(z) \mapsto e^\star(z) = (1-Z)e(Z), \quad Z = 1 - \frac{1}{1-z}.$$

This transformation is involutive, i.e., $e^{\star\star} = e$. Under this transformation, Equation (2) is translated into

$$(1-Z)e^\star(Z) = (1-Z)p^\star(Z) + 2^d \mathbf{J}^{d-1}\mathbf{I}(1-Z)e^\star(Z).$$

The integral operators $\mathbf{I}$ and $\mathbf{J}$ have a nice action on the variable $Z(z)$:

$$\mathbf{I}(1-Z(z))f(Z(z)) = -\int_0^{Z(z)} f(u)\,du, \quad \mathbf{J}f(Z(z)) = \int_0^{Z(z)} f(u)\frac{du}{u},$$

so that their action on the Taylor expansion of *f in the variable Z* is particularly simple: the first one negates the coefficients and shift them by 1 while the second one divides the nth Taylor coefficient by n. Taking coefficients of Z^n on both sides of the above equation thus yields *a linear recurrence of order 1*,

$$e^\star_n - e^\star_{n-1} = p^\star_n - p^\star_{n-1} - 2^d\frac{e^\star_{n-1}}{n^d}. \tag{3}$$

2. Characteristic constants

The real object of study is of course e_n for various p_n. Consider $\lambda_{\nu,d}$ defined as the limit of e_n/n when $p_n = \delta_{n,\nu}$ and n tends to infinity. The parameter e_n then records the number of trees of size ν in a tree of size n. These constants play a role in the analysis of storage allocation strategies. They can also be used to derive other asymptotic behaviours by linear combination.

Applying twice the involutive transformation mentioned above, plus manipulations on recurrence (3), the theorem is that

$$e(z) = p(z) + \int_0^1 K_d(z,t)p(tz)\,dt,$$

where K is a polynomial of degree $d-1$ in $\log t$ whose coefficients are power series in z and t. Unfortunately, these power series have known sums only for $d = 1, 2$. From these sums one deduces

$$\lambda_{\nu,1} = \frac{2}{(\nu+1)(\nu+2)}, \quad \lambda_{\nu,2} = 3 - 18\nu + 6\nu(3\nu+1)\psi'(\nu+1),$$

where ψ is the logarithmic derivative of Euler's Γ function. Taking $\nu = 1$ yields the expected asymptotic proportion of leaves in a 2-dimensional quadtree: $\lambda_{1,2} = 4\pi^2 - 39$.

The existence of a linear differential equation for the generating function makes it possible to compute values of e_n in linear time, so that the values of the characteristic constants can be numerically determined for large values of ν and small values of d.

Other constants can be obtained explicitly in dimension 2. For instance, the proportion of nodes having exactly one or two children are given respectively by

$$24\zeta(3) - 26\pi^2 + 228, \quad -132\zeta(3) + 24\pi^2\ln 2 + \frac{67}{2}\pi^2 - 336.$$

Bibliography

[1] Devroye (Luc) and Laforest (Louise). – An analysis of random d-dimensional quad trees. *SIAM Journal on Computing*, vol. 19, 1990, pp. 821–832.

[2] Flajolet (Philippe), Gonnet (Gaston), Puech (Claude), and Robson (J. M.). – Analytic variations on quadtrees. *Algorithmica*, n° 7, December 1993.

[3] Labelle (Gilbert) and Laforest (Louise). – Étude de constantes universelles pour les arborescences hyperquaternaires de recherche. In *Séries formelles et combinatoire algébrique*. – 1993. Proceedings of FPACS'5, Florence (Italy).

[4] Laforest (Louise). – *Étude des arbres hyperquaternaires*. – Technical Report n° 3, LACIM, UQAM, Montreal, November 1990. (Author's PhD Thesis at McGill University).

Data Compression and Digital Trees

W. Szpankowski
Purdue University

October 5, 1992

[summary by Mireille Régnier]

Abstract

In this talk, the author shows the relationship between two classical data compression algorithms due to Lempel and Ziv [9], and well-known data structures, namely Digital Search Trees and Suffix Trees. Hence, the performance evaluation of these data compression algorithms reduces to the analysis of some tree parameters. Second-order properties are derived. A normal limiting distribution is conjectured. Also, some open problems are given.

1. Introduction

Section 2 briefly presents data compression and the relationship to trees. Then, in Section 3, we study the relationship between tree parameters and data compression performance; we formulate some mathematical problems. Section 4 deals with second order properties, and notably describes the approach of the author. Finally, we provide in Section 5 a small list of open problems. Most of these results appear in INRIA research report [11] and in [6].

2. Lempel and Ziv data compression algorithms

The data compression problem is the following. Some "known" string of length n, the so-called database, is given. One must find the longest substring of the database string that is identical to a yet "unknown" sequence (to be manipulated). Lempel and Ziv algorithms realize a partition of the database sequence into blocks. This is called *parsing*. The parsing satisfies the following properties:

(i) blocks are pairwise distinct;
(ii) each block that occurs in the parsing has already been seen somewhere to the left.

Example. Let us consider sequence

$$11001010001000100$$

In the first algorithm, LZ1, overlapping is not allowed, that is a previous occurrence is not taken into account if it is shared between two consecutive occurrences. Overlapping is allowed in the second one, LZ2. This leads to the two partitions:

$$(1)(10)(0)(101)(00)(01)(000)(100) \ : \ LZ1$$

and

$$(1)(10)(0)(101)(00)(01)(000100) \ : \ LZ2$$

Note that difference occur at position 12. Sequence 000 occurred before, but is split between blocks 5 and 6.

LZ1 is associated to a digital search tree built on the block sequence read from left to right. LZ2 is associated to a suffix tree. We present on Figure 2 the tree associated to LZ1.

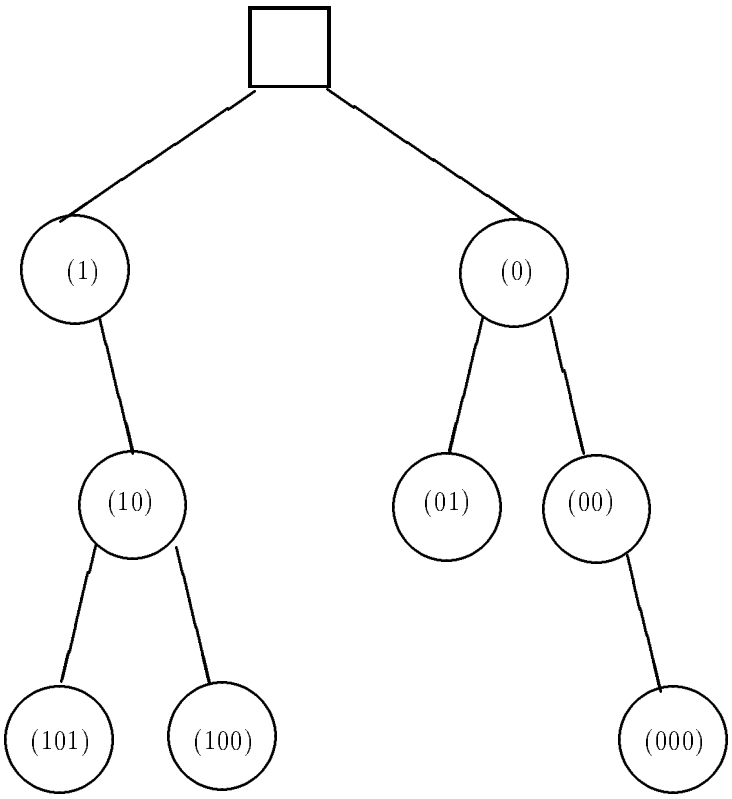


FIGURE 1. A digital tree representation of Ziv's parsing for the string 11001010001000100 ...

3. Relevant parameters

The relevant parameters for data compression are:

- M_n: number of phrases built over a (random) sequence of length n;
- $M_n(k)$: number of phrases of length k;
- l_m: length of the m-th phrase;
- H_n: length of the longest phrase;
- $\tilde{I}_n$: longest substring that can be duplicated;
- N_l: size of a database having two copies of some substring of length l.

The relevant parameters for a digital search tree are given below. We consider a tree built over n strings.

- $D_n(m)$: depth of the m-th string;
- D_n: depth of a randomly selected string:

$$Pr(D_n \leq k) = \frac{1}{n} \sum_{m=1}^{n} Pr(D_n(m) \leq k);$$

- $I_n = D_{n+1}(n+1)$: depth of insertion;
- H_n: height of the tree, i.e. $\max_{1 \leq m \leq n}(D_n(m))$;
- S_n: shortest path in the tree, e.g. $\min_{1 \leq m \leq n}(D_n(m))$;
- L_n : external pathlength

$$L_n = \sum_{m=1}^{n} D_n(m);$$

- Z_n : size of the tree, i.e. number of internal nodes.

We now provide a list of relationships between data compression and tree parameters.

Non-overlapping parsing algorithm LZ1.

$$Z_{M_n} = M_{n+1}, \tag{1}$$

$$L_{M_n-1} < n \leq L_n, \tag{2}$$

$$l_m = D_m(m) = I_m, \tag{3}$$

$$M_n(k) = \#\text{ of internal nodes at level}k. \tag{4}$$

Parsing algorithm LZ2.

$$l_k = I_{\sum_{r=1}^{k-1} l_r} = D_{\sum_{r=1}^{k-1} l_r}(\sum_{r=1}^{k-1} l_r), \tag{5}$$

$$\tilde{I}_n = I_n = D_n(n), \tag{6}$$

$$D_{N_l}(1) = l. \tag{7}$$

Unfortunately, there exists no simple relationship between M_n and L_n. We only have:

$$\sum_{k=1}^{M_n} l_k = n.$$

4. Deriving limiting distributions

First order properties, i.e. average values, convergence in probability or almost sure have now been derived for many classes of trees. See notably [1, 8, 10] for Digital Search Trees and [13] for suffix trees.

Second order properties, e.g. variances, large deviation results and limiting distributions are less known. Most results are derived for tries [2, 4, 5, 7]. Digital Search Trees were open.

The first result presented is the limiting distribution of the number of phrases of length k, in LZ1, i.e. $M_n(k)$ or D_n. One proves:

THEOREM 1. *(i) For the symmetric Bernoulli model the limiting distribution of D_m is*

$$\lim_{m\to\infty} \Pr\{D_m = x + \log_2 m\} = 2^{x-1}\left(1 + \frac{1}{Q_\infty}\sum_{i=0}^{\infty}(-1)^{i+1}\frac{-2^{-i(i+1)/2}}{Q_i}e^{-2^{-(x-1-i)}}\right) \tag{8}$$

for such real x that $x+\log_2 m$ is integer, with $Q_k = \prod_{j=1}^{k}(1-2^{-j})$. (ii) In the asymmetric case, the limiting distribution of D_m is normal, that is,

$$\frac{D_m - ED_m}{\sqrt{\text{Var } D_m}} \to N(0,1) \tag{9}$$

where ED_m and Var D_m *are given by (10) and (11), respectively.*

$$ED_m = \frac{1}{h}\left(\log m + \gamma - 1 + \frac{H}{2h} + \theta + \delta(m)\right) + O(\log m/m) \tag{10}$$

$$\text{Var } D_m = \frac{H-h^2}{h^3}\log m + A + \Delta(m) + O(\log^2 m/m) \tag{11}$$

Moreover, the moments of D_m converges to the appropriate moments of the normal distribution. More precisely, for any complex ϑ

$$e^{-\vartheta c_1 \log m}E(e^{\vartheta D_m}) = e^{c_2\frac{\vartheta^2}{2}\log m}\left(1 + O(\frac{\vartheta}{\sqrt{\log m}})\right) \tag{12}$$

where $c_1 = 1/h$ *and* $c_2 = (H - h^2)/h^3$.

PROOF. One considers the generating functions $B_n(z)$, where $[z^k]B_n(z)$ is the average number of internal nodes at level k. One proves the recurrence equation:

$$B_m(u) = m - (1-u)\sum_{k=2}^{m}(-1)^k \binom{m}{k} Q_{k-2}(u) \tag{13}$$

where

$$Q_k(u) = \prod_{j=1}^{k}(1 - u2^{-j}). \tag{14}$$

Since the formula for $Q_k(u)$ is relatively simple, we can extract coefficients of $B_m(u)$ "by hand".

Note that $Q_k(u) = Q_\infty(u)/Q_\infty(u2^{-k})$, and, as in Louchard [10],

$$\frac{1}{Q_\infty(u)} = \sum_{i=0}^{\infty}\frac{u^i}{2^i Q_i}, \quad Q_\infty(u) = -\sum_{i=0}^{\infty} u^i R_i \tag{15}$$

where

$$R_i = (-1)^{i+1}\frac{2^{-i(i+1)/2}}{Q_i} \tag{16}$$

with $Q_i = Q_i(1)$. Let now $[u^k]f(u)$ denote the coefficient at u^k of $f(u)$. Note that

$$[u^n]Q_{k-2}(u) = -\sum_{l=0}^{n}\frac{R_{n-l}}{Q_l 2^{l(k-1)}}.$$

Hence applying this to our basic solution (13) we obtain

$$\begin{aligned}[u^{j+1}]B_m(u) &= \sum_{l=0}^{j+1}\frac{2^l R_{j+1-l}}{Q_l}\left((1-2^{-l})^m - 1 - m/2\right) \\ &- \sum_{l=0}^{j}\frac{2^l R_{j-l}}{Q_l}\left((1-2^{-l})^m - 1 - m/2\right).\end{aligned}$$

Finally, after some tedious algebra one obtains an explicit formula as in Louchard [10], and taking $m \to \infty$ we easily derive part (i) of Theorem 1 (see also Mahmoud [12], Ex. 6.12).

Alternatively, Mellin-like or Rice method can be used to find an asymptotic solution. Then, one may use Cauchy formula to extract coefficient $M_n(k)$. In the asymmetric case, one considers $D_m(u) = B_m(u)/m$. □

We come now to the second result: the limiting distribution of the number of phrases M_n in LZ1.

THEOREM 2. *(i) The length of a randomly selected phrase for the symmetric Bernoulli model has the following limiting distribution*

$$\lim_{n\to\infty}\Pr\{D_n^{LZ} = x + \log_2(n/\log_2 n)\} = 2^{x-1}\left(1 + \frac{1}{Q_\infty}\sum_{i=0}^{\infty}(-1)^{i+1}\frac{2^{-i(i+1)/2}}{Q_i}e^{-2^{-(x-1-i)}}\right) \tag{17}$$

for such real x *that* $x + \log_2(n/\log_2 n) = j$ *is an integer.*

(ii) For the asymmetric Bernoulli model the typical depth D_n^{LZ} *is normally distributed. More precisely,*

$$\frac{D_n^{LZ} - c_1\log(nh/\log n)}{\sqrt{c_2\log(nh/\log n)}} \to N(0,1) \tag{18}$$

provided our Conjecture is true. In fact, the rate of convergence is $1 + O(1/\sqrt{\log n})$.

PROOF. The author expresses this random variable D_n^{LZ} as a function of the r.v. D_m of the previous theorem. □

The third result is about external path length. In [6], it is proven that:

THEOREM 3. *Consider a digital search tree under the asymmetric Bernoulli model. Then,*

$$\frac{L_m - c_1 m \log m}{\sqrt{c_2 m \log m}} \to N(0,1), \tag{19}$$

where $c_1 = 1/h$ *and* $c_2 = (H - h^2)/h^3$ *with* $h = -p\log p - q\log q$ *being the entropy of the alphabet and* $H = p\log^2 p + q\log^2 q$. *That is, for* x *real we have* $\lim_{m\to\infty} \Pr\{L_m < c_1 m\log m + x\sqrt{c_2 m \log m}\} = 1/\sqrt{2\pi}\int_{-\infty}^{x} e^{-t^2/2}dt$. *Moreover,*

$$EL_m = c_1 m \log m + O(m) \tag{20}$$

$$\text{Var } L_m = c_2 m \log m + O(m), \tag{21}$$

and all moments of L_m *converge to the appropriate moments of the normal distribution. In the symmetric case (i.e.,* $p = q = 0.5$*), the internal path length* L_m^{sym} *still satisfies (19) with* $EL_m^{sym} \sim \log_2 m$ *and*

$$\text{Var } L_m^{sym} \sim (C + \delta(\log_2 m))m \tag{22}$$

where $C = 0.26600\ldots$ *and* $\delta(x)$ *is a fluctuating continuous function with period 1 (cf.* [8]*). In this case, the convergence in moments also holds.*

PROOF. The scheme of the proof is similar to [3]: the bivariate generating function for the external path length is defined by two equations:

$$L_{m+1}(u) = u^m \sum_{k=0}^{m} \binom{m}{k} p^k q^{m-k} L_k(u) L_{m-k}(u). \tag{23}$$

with $L_0(u) = 1$. Hence, also

$$\frac{\partial L(z,u)}{\partial z} = L(pzu, u)L(qzu, u) \tag{24}$$

with $L(z, 0) = 1$.

(1) one first analyzes the Poisson model that is characterized by the exponential bivariate generating function $L(z, u)$ satisfying (24).
(2) In order to solve (24) one tries to transform it into an additive functional equation by considering $\log L(z, u)$. This is only possible if one proves the existence of $\log L(z, u)$. Hence, one proves that there is a convex cone around the real axes such that for some $\kappa(u)$ we have $\log L(z, u) = \Theta(z^{\kappa(u)})$.
(3) Next, one uses Taylor expansion of $\log L(z, u)$ in the convex cone to show that for large z the generating function $L(z, u)$ appropriately normalized converges to the generating function of the normal distribution.
(4) The final effort is to de-Poissonize the latter result, that is, to transform the normal distribution of the Poisson model into the normal distribution of the Bernoulli model.

□

5. Open problems

Many problems remain open. One would like to extend first and second order results in the case of Markovian distributions. Also, the variance of the external path length is of interest for asymmetric Bernoulli model and various classes of trees: Digital Search Trees, tries, Patricia tries.

Bibliography

[1] Flajolet (P.) and Sedgewick (R.). – Digital search trees revisited. *SIAM Journal on Computing*, vol. 15, n° 3, August 1986, pp. 748–767.

[2] Jacquet (Ph.) and Régnier (M.). – Normal limiting distribution of the size of tries. In Courtois (P.-J.) and Latouche (G.) (editors), *Performance'87*. pp. 209–223. – North-Holland, 1987. 12-th IFIP WG International Symposium on Computer Performance, Bruxelles.

[3] Jacquet (Ph.) and Régnier (M.). – *Normal limiting distribution of the size and external path length of tries.* – Research report n° 827, Institut National de Recherche en Informatique et en Automatique, 1988.

[4] Jacquet (Ph.) and Régnier (M.). – New results on the size of tries. *IEEE Transactions on Information Theory*, vol. 35, n° 1, 1989, pp. 203–205.

[5] Jacquet (Ph.) and Szpankowski (W.). – Analysis of digital tries with Markovian dependency. *IEEE Transactions on Information Theory*, vol. 37, 1991, pp. 669–675.

[6] Jacquet (Ph.) and Szpankowski (W.). – *A Functional Equation Arising in the Analysis of Algorithms.* – Technical report, Institut National de Recherche en Informatique et en Automatique, 1993.

[7] Jacquet (Philippe) and Régnier (Mireille). – Trie partitioning process: Limiting distributions. In Franchi-Zanetacchi (P.) (editor), *CAAP'86*, *Lecture Notes in Computer Science*, vol. 214, pp. 196–210. – 1986. Proceedings of the 11th Colloquium on Trees in Algebra and Programming, Nice France, March 1986.

[8] Kirschenhofer (P.), Prodinger (H.), and Szpankowski (W.). – Digital search trees again revisited: The internal path length perspective. *SIAM Journal on Computing*, 1993.

[9] Lempel (A.) and Ziv (J.). – On the complexity of finite sequences. *IEEE Transactions on Information Theory*, vol. 22, n° 1, 1976, pp. 75–81.

[10] Louchard (G.). – Exact and asymptotic distributions in digital and binary search trees. *RAIRO Theoretical Informatics and Applications*, vol. 21, n° 4, 1987, pp. 479–495.

[11] Louchard (G.) and Szpankowski (W.). – *Average Profile and Limiting Distribution for a Phrase Size in the Lempel-Ziv Parsing Algorithm.* – Research Report n° 1886, Institut National de Recherche en Informatique et en Automatique, 1993.

[12] Mahmoud (Hosam). – *Evolution of Random Search Trees.* – John Wiley, New York, 1992.

[13] Szpankowski (W.). – A generalized suffix tree and its (un)expected behaviors. *SIAM Journal on Computing*, 1993.

On the number of heaps

Hsien-Kuei Hwang
LIX, École polytechnique

February 8, 1993

[summary by Hsien-Kuei Hwang]

Abstract

The main interest in this talk is the asymptotic behaviour of the number of heaps of size n as $n \to \infty$. For special sequences of n, like $\{2^k\}_k$ or $\{2^k-1\}_k$, the result is easily obtained by resolving linear recurrences of first order. In order to obtain a general asymptotic formula, we need to introduce some oscillating digital sums (depending on the digits of the binary representation of n) whose behaviours can only be grasped by their summatory functions which are more manageable.

1. Heap Recurrences

A (max-)*heap* is an array with elements a_j, $1 \le j \le n$, satisfying the *path-monotone property*: $a_j \le a_{\lfloor j/2 \rfloor}$, $j = 2, 3, \ldots, n$. It can be viewed as a binary tree where the value of each element is not smaller than that of its children. A characteristic property of a heap, when viewed as a binary tree, is that at least one of the two sub-trees of the root node is complete (i.e., it contains $2^k - 1$ elements for some non-negative integer k). And this property recursively applies to each node. Given a heap $\mathcal{H}_n$ of size n and an additive cost function φ on heaps, we have the relation

$$\varphi[\mathcal{H}_n] = \tau[\mathcal{H}_n] + \varphi[\mathcal{H}_L] + \varphi[\mathcal{H}_R], \tag{1}$$

for some cost function τ, where $\mathcal{H}_L$ and $\mathcal{H}_R$ denote the left and right sub-heaps of the root node of $\mathcal{H}_n$ with sizes L and R, respectively. Since at least one of $\mathcal{H}_L$ or $\mathcal{H}_R$ is complete, the relation (1) can be written into a more precise form as follows. For $k \ge 0$ and $\{t_n\}_{n\ge 1}$ a given non-negative sequence,

$$\begin{cases} f_{2^k+j} = t_{2^k+j} + \begin{cases} f_{2^{k-1}-1} + f_{2^{k-1}+j}, & \text{if } 0 \le j < 2^{k-1}, \\ f_{2^k-1} + f_j, & \text{if } 2^{k-1} \le j < 2^k, \end{cases} \\ f_0 = 0, \end{cases} \tag{2}$$

which we call the *additive heap recurrence* [3]. The associated generating functions are not very suggestive for further investigations.

$$f(z) = \sum_{n\ge 1} t_n z^n + \frac{1}{1-z} \sum_{k\ge 1} f_{2^k-1} \left(z^{3\cdots 2^{k-1}} - z^{3\cdots 2^k} \right) + \sum_{k\ge 1} \left(z^{2^k} + z^{2^{k-1}} \right) \sum_{2^{k-1} \le j < 2^k} f_j z^j,$$

where $f(z) = \sum_{n\ge 1} f_n z^n$.

Let h_n denote the total number of ways to rearrange the integers $\{1, 2, \ldots, n\}$ into a heap. Then it is obvious that h_n satisfies the *multiplicative heap recurrence*:

$$h_{2^k+j} = \begin{cases} \binom{2^k+j-1}{2^{k-1}-1} h_{2^{k-1}-1} h_{2^{k-1}+j}, & \text{if } 0 \le j < 2^{k-1}, \\ \binom{2^k+j-1}{2^k-1} h_{2^k-1} h_j, & \text{if } 2^{k-1} \le j < 2^k. \end{cases}$$

The sequence

$$\{h_n\}_{n\geq 2} = 1,2,3,8,20,80,210,896,3360,19200,79200,506880,2745600,$$
$$21964800,108108000,820019200,5227622400,48881664000...$$

is not in Sloane's book. Let $f_n = \log(n!/h_n)$, then f_n satisfies the additive heap recurrence. We require then to find the general solution of (2).

Let us first fix some notations.

- n is a positive integer, and $n = (b_L b_{L-1}...b_0)_2$, where $L = \lfloor \log_2 n \rfloor$ and $b_L = 1$.
- $n_j = (1b_{j-1}...b_0)_2$ for $j = 1...L$; $n_0 = 1$.
- $\nu(n)$ denotes the number of 1-digits in the binary representation of n.

Before solving (2), we note that there is another very similar type of recurrences [2]

$$\phi_{2^k+j} = \tau_{2^k+j} + \begin{cases} \phi_{2^{k-1}} + \phi_{2^{k-1}+j}, & \text{if } 0 \leq j \leq 2^{k-1}; \\ \phi_{2^k} + \phi_j, & \text{if } 2^{k-1} \leq j \leq 2^k, \end{cases} \tag{3}$$

which occurs as the solution of the following equation

$$\phi_n = \tau_n + \min_{1\leq j\leq \lfloor n/2 \rfloor} (\phi_j + \phi_{n-j}),$$

when the sequence $\{\tau_n\}_{n\geq 0}$ is strictly concave, namely $\tau_{n+2} - 2\tau_{n+1} + \tau_n < 0$ for all $n \geq 0$.

Recall that the backward difference is defined by $\nabla f_n = f_n - f_{n-1}$. Let $\varphi_n = \nabla f_n$, and $\tau_n = \nabla t_n$, then we obtain a slightly different recurrence

$$\varphi_{2^k+j} = \tau_{2^k+j} + \begin{cases} \varphi_{2^{k-1}+j} & 0 \leq j < 2^{k-1}, \\ \varphi_j & 2^{k-1} \leq j < 2^k, \end{cases}$$

together with $\varphi_0 = 0$. Equivalently, this recurrence can be re-written as $\varphi_n = \varphi_{n_L} = \tau_n + \varphi_{n_{L-1}} = \sum_{0\leq j\leq L} \tau_{n_j}$.

2. Explicit Formula

To solve the heap recurrence explicitly, we first observe that when $n = 2^{m+1} - 1$, we have a linear recurrence: $f_{2^{m+1}-1} = t_{2^{m+1}-1} + 2f_{2^m-1}$, which can be solved easily by iteration. From this, we can find the solution for the sequences $\{2^m\}$, $\{2^m + 2^{m-1} - 1\}$, ... But this process does not lead readily to a general solution. Hence, we begin with another way.

LEMMA 1. *For $n \geq 1$, we have, for the solution of (2),*

$$f_n = \sum_{1\leq j\leq L} \left(\left\lfloor \frac{n}{2^{j-1}} \right\rfloor - \left\lfloor \frac{n}{2^j} \right\rfloor - 1 \right) t_{2^j-1} + \sum_{0\leq j\leq L} t_{n_j}. \tag{4}$$

The two sums correspond, respectively, to the contribution of complete sub-heaps and non-complete sub-heaps.

Similarly, the solution for the recurrence (3) is expressed by ($\phi_0 = 0$)

$$\phi_n = \sum_{0\leq j\leq L} \left(\left\lfloor \frac{n}{2^{j-1}} \right\rfloor - \left\lfloor \frac{n}{2^j} \right\rfloor - 1 \right) \tau_{2^j} + \sum_{0\leq j\leq L} \tau_{n_j}. \tag{5}$$

An immediate consequence of Lemma 1 is the following

LEMMA 2. *Let $t_n > 0$ and $t_n = O(n^{1-\alpha})$ for fixed $\alpha > 0$, then the solution f_n of (1) satisfies $f_n \sim cn$, as n tends to infinity, for some constant c. Moreover, the constant c is given by*[1]

$$c = \sum_{j\geq 1} \frac{t_{2^j-1}}{2^j}. \tag{6}$$

[1]The series $\sum_{j\geq 1} \frac{t_{2^j-1}}{2^j}$ is easily seen to be convergent.

This result says that without loss of generality, we can, under the hypotheses of Lemma 2, consider only the special sequence $\{2^m-1\}_m$, as far as the first asymptotic term is concerned.

For recurrence (3), constant c is modified to be $c=\sum_{j\ge 0}\tau_{2^j}/2^j$, under the same conditions.

3. The Number of Heaps

Let $f_n=\log(n!/h_n)$, then f_n satisfies (2) with $t_n=\log n$. Lemma 2 gives the first-order estimate of f_n

$$f_n\sim n\sum_{j\ge 1}\frac{\log(2^j-1)}{2^j}=n\left(2\log 2+\sum_{j\ge 1}\frac{1}{2^j}\log(1-\frac{1}{2^j})\right)=0.945755\ldots n.$$

Let $\alpha=2\log 2+\sum_{j\ge 1}2^{-j}\log(1-2^{-j})$ be the coefficient. Using Lemma 1, we obtain the main result of this talk.

THEOREM 1.

$$h_n\sim 2Q\sqrt{2\pi}P(\log_2 n)R(n)\,n^{n+\frac{3}{2}}\,e^{-\alpha n-n}\qquad(n\to\infty),$$

where $Q=\prod_{j\ge 1}\left(1-2^{-j}\right)=0.288788\ldots$,

$$P(u)=2^{2^{\{u\}}-\{u\}}\prod_{0\le j\le u}\frac{2^{\{2^{u-j}\}}}{1+\{2^{u-j}\}},$$

and

$$R(n)=\prod_{j\ge 1}\left(\frac{1-2^{-j-1}}{1-2^{-j}}\right)^{\{n/2^j\}}.$$

The two functions P and R are oscillating in nature. We can prove that, for all $n\ge 1$,

$$1\le R(n)\le\exp\left(-\sum_{j\ge 1}2^{-j}\log(1-2^{-j})\right)=1.553544\ldots$$

and

$$0<2^{-\{\log_2 n\}+c_0\,\nu(n)}<P(\log_2 n)\le 2,$$

where $c_0=1-c_1/\log 2=-0.253522\ldots$ with $c_1=\sum_{j\ge 1}\log(1+2^{-j})=0.868876\ldots$.

To further investigate the properties of the two functions R and P, we observe that R is bounded for all n. For P, let $p(n)=\log P(\log_2 n)$, then

$$p(n)=\nu(n)-\{\log_2 n\}-\sum_{0\le j\le\log_2 n}\log_2(1+\{n/2^j\}),$$

so that p oscillates between $O(\log n)$ and $O(1)$. Since the first two terms on the right-hand side are "known", only the last sum needs special treatments. Set $\pi(n)=\sum_{0\le j\le\log_2 n}\log(1+\{n/2^j\})$. Then, for x not an integer, we have the convergent Fourier series

$$\log(1+\{x\})=2\log 2-1+\sum_{k\ne 0}\frac{e^{2k\pi ix}}{2k\pi i}\left(\mathrm{Ei}(-4k\pi i)-\mathrm{Ei}(-2k\pi i)-\log 2\right).$$

For x an integer, the series converges to $\frac{1}{2}\log 2$. $\mathrm{Ei}(z)$ is the exponential integral. Now summing all such series for $j=1,2,\ldots,L$, we obtain

$$\pi(n)=(2\log 2-1)\,L-\frac{\log 2}{2}\,v_2(n)+\sum_{k\ne 0}\frac{\mathrm{Ei}(-4k\pi i)-\mathrm{Ei}(-2k\pi i)-\log 2}{2k\pi i}\sum_{1\le j\le L}e^{2k\pi ni/2^j},$$

which is a mere translation of $\pi(n)$ into trigonometric sums. Here $v_2(n)$ denotes the exponent of 2 in the prime decomposition of n. Yet the formula still says something about the average order of $\pi(n)$:

$$\frac{1}{n}\sum_{1\le m\le n}\pi(m) = (2\log 2 - 1)\log_2 n + O(1) \qquad (n\to\infty),$$

which can be obtained by the following "Ergodic-type" result.

LEMMA 3. *For any real continuous function $\varphi(x)$ on $[0,1]$, define $\phi(m) = \sum_{0\le j\le \log_2 m}\varphi(\{m/2^j\})$. We have the asymptotic formula*

$$\frac{1}{n}\sum_{1\le m\le n}\phi(m) = \left(\int_0^1 \varphi(x)\,dx\right)\log_2 n + O(1) \qquad (n\to\infty).$$

In words, the lemma says that the average order of the function $\phi(m)$ is asymptotically equal to $\log_2 n$ times the mean value of the function φ on $[0,1]$.

4. The Cost of Constructing Heaps

Given a random permutation π_n of size n, let ξ_n denote the number of exchanges used to construct a heap from π_n using Floyd's algorithm. Then $\mathbf{E}\xi_n$ satisfies the heap recurrence with $t_n = n^{-1}\sum_{1\le j\le n}\lfloor\log_2 j\rfloor = L + (L+2)/n - 2^{L+1}/n$. Applying Lemma 1, we get the following refined result of Sprugnoli [3], who considered only special sequences of n.

THEOREM 2. *The expected number of exchanges $\mathbf{E}\xi_n$ used in Floyd's heap construction algorithm satisfies*

$$\mathbf{E}\xi_n = c_2 n - \lfloor\log_2 n\rfloor - \nu(n) + 2\varpi_1(n) + \varpi_2(n) + O\left(\frac{\log n}{n}\right) \qquad (n\to\infty),$$

where $c_2 = -2 + \sum_{j\ge 1} j(2^j-1)^{-1} = 0.744033\ldots$, $\varpi_1(n)$ oscillates between $O(\log n)$ and $O(1)$,

$$\varpi_1(n) = \sum_{0\le j\le L}\frac{\{n/2^j\}}{1+\{n/2^j\}},$$

and $\varpi_2(n) = O(1)$ is given by

$$\varpi_2(n) = -1 - \sum_{j\ge 1}\frac{j}{2^j-1} + \sum_{j\ge 1}\frac{j+2}{2^j(1+\{n/2^j\})} + \sum_{j\ge 1}\left\{\frac{n}{2^j}\right\}\frac{j2^j - 2^j + 1}{(2^j-1)(2^{j+1}-1)}.$$

In particular, we have the inequalities $\frac{1}{2}(\nu(n) - n/2^L) \le \varpi_1(n) \le c_3\nu(n)$ for all n, so that

$$c_2\, n - L + O(1) \le \xi_n \le c_2\, n - L + (2c_3 - 1)\,\nu(n) + O(1),$$

for all n, where $c_3 = \sum_{j\ge 1}(2^j+1)^{-1} = 0.764499\ldots$ and $2c_3 - 1 = 0.528999\ldots$

By Lemma 3, the average order of the arithmetic function $\varpi_1(n)$ is $(1-\log 2)\log_2 n + O(1)$.

For the variance, we take

$$\begin{aligned} t_n &= \frac{1}{n}\sum_{1\le j\le n}\lfloor\log_2 j\rfloor^2 - \left(\frac{1}{n}\sum_{1\le j\le n}\lfloor\log_2 j\rfloor\right)^2 \\ &= 6\frac{2^L}{n} - \frac{L^2}{n} - \frac{6}{n} - 4\frac{L}{n} - \frac{4}{n^2} - 4\frac{L}{n^2} + \frac{2^{L+3}}{n^2} - \frac{L^2}{n^2} + \frac{2^{L+2}L}{n^2} - \frac{4^{L+1}}{n^2}. \end{aligned}$$

With the help of Maple, we obtain the following result.

THEOREM 3. *The variance of the number of exchanges satisfies the asymptotic expression*

$$\mathrm{Var}(\xi_n) = c_4 n + \varpi_3(n) + \varpi_4(n) + O\left(\frac{\log^2 n}{n}\right) \qquad (n \to \infty),$$

where $c_4 = 2 - \sum_{j\geq 1} j^2(2^j-1)^2 = 0.261217\ldots$, $\varpi_3(n)$ *oscillates between* $O(\log n)$ *and* $O(1)$*:*

$$\varpi_3(n) = -2 \sum_{0\leq j\leq L} \frac{\{n/2^j\}}{1+\{n/2^j\}} + 4 \sum_{0\leq j\leq L} \frac{\{n/2^j\}}{(1+\{n/2^j\})^2},$$

and $\varpi_4(n) = O(1)$*:*

$$\varpi_4(n) = \sum_{j\geq 1} \frac{j^2 2^j}{(2^j-1)^2} + \sum_{j\geq 1} \left\{\frac{n}{2^j}\right\} \frac{2^j(j^2+4j+2) - 4^{j+1}(2j+1) - 2\cdots 8^j(j^2-2j-1)}{(2^j-1)^2(2^{j+1}-1)^2}.$$

The average order of $\varpi_3(n)$ is $(6\log 2 - 4)\log_2 n + O(1)$.

Finally, from the probability generating function of ξ_n derived in [1], it is not hard to show that the distribution of ξ_n is asymptotically Gaussian.

THEOREM 4. *We have*

$$\Pr\{\frac{\xi_n - c_2 n}{\sqrt{c_4 n}} < x\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{1}{2}t^2}\, dt + O\left(\frac{\log n}{\sqrt{n}}\right) \qquad (n \to \infty),$$

uniformly with respect to x*.*

Bibliography

[1] Doberkat (E. E.). – An average case analysis of Floyd's algorithm to construct heaps. *Information and Control*, vol. 61, n° 2, 1984, pp. 114–131.

[2] Hammersley (J. M.) and Grimmett (G. R.). – Maximal solutions of the generalized subadditive inequality. In Harding (E. F.) and Kendall (D. G.) (editors), *Stochastic Geometry*, Chapter 4. – John Wiley and Sons, 1974.

[3] Sprugnoli (R.). – Recurrence relations on heaps. – Manuscript, 1991.

A lower bound for parallel string matching

Dany Breslauer
INRIA and Columbia University

April 26, 1993

[summary by Mireille Regnier]

Abstract

This talk presents the derivation of an $\Omega(\log\log m)$ lower bound on the number of rounds necessary for finding occurrences of a pattern string $P[1..m]$ in a text string $T[1..2m]$ in parallel using m comparisons in each round. The parallel complexity of the string matching problem using p processors for general alphabets follows.

1. Introduction

Better and better parallel algorithms have been designed for string-matching. All are on CRCW-PRAM with the weakest form of simultaneous write conflict resolution: all processors which write into the same memory location must write the same value of 1. The best CREW-PRAM algorithms are those obtained from the CRCW algorithms for a logarithmic loss of efficiency. Optimal algorithms have been designed: $O(\log m)$ time in [8, 17] and $O(\log\log m)$ time in [4]. (An optimal algorithm is one with $pt = O(n)$ where t is the time and p is the number of processors used.) Recently, Vishkin [18] developed an optimal $O(\log^* m)$ time algorithm. Unlike in the case of the other algorithms this time bound does not account for the preprocessing of the pattern: the preprocessing takes $O(\frac{\log^2 m}{\log\log m})$. Vishkin's super fast algorithm raised the question whether an optimal constant-time algorithm is possible.

We show that a CRCW-PRAM with m processors requires $\Omega(\log\log m)$ time to perform string matching. Thus, our $O(\log\log m)$ optimal parallel algorithm cannot be improved and Vishkin's algorithm crucially depends on a slower preprocessing. Our result is the first lower bound for parallel algorithms that solve the string matching problem. More precisely, the exact parallel complexity of string matching for general alphabets on the CRCW-PRAM is: $\Theta(\lceil\frac{m}{p}\rceil + \log\log_{\lceil 1+p/m\rceil} 2p)$.

Our model is similar to Valiant's parallel comparison tree model [16]. We assume the only access the algorithm has to the input strings is by comparisons which check whether two symbols are equal or not. The algorithm is allowed p comparisons in each round, after which it can proceed to the next round or terminate with the answer. We give a lower bound on the minimum number of rounds necessary in the worst case. We show also that our bound holds even if the algorithm is allowed to perform order comparisons which can result in a *less than*, *equal* or *greater than* answers.

As the execution can be partitioned into comparison rounds followed by computation rounds, our lower bound immediately translates into a lower bound for the time of the CRCW-PRAM.

If the pattern is given in advance and any preprocessing is free, then this lower bound does not hold, as Vishkin's $O(\log^* m)$ algorithm shows. The lower bound also does not hold for CRCW-PRAM over a fixed alphabet strings. Similarly, finding the maximum in the parallel decision tree model has the same lower bound [16], but for small integers the maximum can be found in constant time on a CRCW-PRAM [7].

2. A lower bound for finding the period of a string and string matching

Given a string $S[1..m]$, we say that k is a *period length* of S if $S[i+k] = S[i]$ for $i = 1, \ldots, m-k$. We call k *the period length* of S if it is the minimal period length of S. In this section we prove a lower bound for

the problem of finding the period length of a string $S[1..m]$ using m comparisons in each round. Our lower bound also holds for determining whether such a string has a period of length smaller than $\frac{m}{2}$.

We show a strategy for an adversary to answer $\frac{1}{4}\log\log m$ rounds of comparisons after which it still has the choice of fixing the input string S in two ways: in one the resulting string has a period of length smaller than $\frac{m}{2}$ and in the other it does not have any such period. This implies that any algorithm which terminates in less rounds can be fooled. Also, let S be a string of length $2m$ generated by this adversary. Assume we present to some string matching algorithm pattern $S[1..m]$ and text $S[2..2m]$. The choice left open above determines the occurrence or not of P in T. Thus, the lower bound holds also for any string matching algorithm.

At the beginning of round i the adversary will maintain an integer k_i which is a possible period length. I.e. we can fix S consistently with answers to previous comparisons in such a way that k is a period length of S. For such k to be a period length we need each residue class modulo k to be fixed to the same symbol, thus if $l \equiv j \mod k$ then $S[l] = S[j]$. We say that k_i *forces* this comparison.

The adversary answers the comparisons of round i in such a way that some k_{i+1} is a possible period length and few symbols of S are fixed. Hence, few comparisons are forced. It maintains the following invariants which hold at the beginning of round number i:

(1) k_i satisfies $\frac{1}{2}K_i \leq k_i \leq K_i$ and the number of fixed symbols f_i satisfies $f_i \leq K_i$.
(2) If $S[l]$ was fixed then for every $j \equiv l \mod k_i$ $S[j]$ was fixed to the same symbol.
(3) If a comparison was answered as equal then both symbols compared were fixed to the same value.
(4) If a comparison was answered as unequal, then
    (a) it was between different residues modulo k_i;
    (b) if the symbols were fixed then they were fixed to different values.

Note that invariants (3) and (4) imply consistency of the answers given so far. Joined with invariant (2), they imply that k_i is a possible period length: we fix all symbols in each unfixed residue class modulo k_i to a new symbol, choosing them different for different residue classes.

We start at round number 1 with $k_1 = K_1 = 1$: invariants hold initially. Now, all multiples of k_i in the range $\frac{1}{2}K_{i+1} \ldots K_{i+1}$ are candidates for the new k_{i+1}. The proof relies on the existence of a "good candidate":

LEMMA 1. *There exists a candidate for k_{i+1} in the range $\frac{1}{2}K_{i+1} \ldots K_{i+1}$ that forces at most $\frac{4mK_i \log m}{K_{i+1}}$ comparisons.*

PROOF. The number of prime multiples of k_i that satisfy $\frac{1}{2}K_{i+1} \leq k_{i+1} \leq K_{i+1}$ is greater than $\frac{K_{i+1}}{4K_i \log m}$. From [15], the number of primes between $\frac{1}{2}n$ and n is greater than $\frac{1}{4}\frac{n}{\log n}$. Also, let $p, q \geq \sqrt{\frac{m}{k_i}}$ be relatively prime, and l, q be two different integers: $1 \leq k < l \leq m$. The double condition $l \equiv k \mod pk_i$, $l \equiv k \mod qk_i$ implies $l \equiv k \mod pqk_i$, hence $l = k$, a contradiction. Hence, a comparison $S[l] = S[k]$ is forced by at most one of pk_i and qk_i. As the total number of comparisons forced by all these candidates is at most m, there is a candidate that forces at most $\frac{4mK_i \log m}{K_{i+1}}$ comparisons. □

We are now ready to prove that the adversary can answer the comparisons in round i so that the invariants also hold at the beginning of round $i+1$. Since our "good candidate" k_{i+1} is a multiple of k_i, the residue classes modulo k_i split; each class splits into $\frac{k_{i+1}}{k_i}$ residue classes modulo k_{i+1}. Note that if two indices are in different residue classes modulo k_i, then they are also in different residue classes modulo k_{i+1}; if two indices are in the same residue class modulo k_{i+1}, then they are also in the same residue class modulo k_i. For each comparison forced by k_{i+1} involving two positions (l, j) in the same residue class modulo k_{i+1}, the adversary fixes the residue class modulo k_{i+1} to the same new symbol (a different symbol for different residue classes). The adversary answers comparisons between fixed symbols based on the value they are fixed to. All other comparisons involve at least one unfixed symbol: They are always answered as unequal.

We show that the invariants still hold.

(1) This is clear by simple induction computation.

(2) Residue classes previously fixed satisfied (2). This is maintained by the splitting process into several residue classes. Any symbol fixed at this round causes its entire residue class modulo k_{i+1} to be fixed to the same symbol.

(3) Equal answers of previous rounds are not affected. Equal answers of this round are either between symbols which were fixed before to the same value or are within the same residue class modulo k_{i+1} and the entire residue class is fixed to the same value.

(4) (a) Unequal answers of previous rounds are between different residue classes modulo k_{i+1} since residue classes modulo k_i split. Unequal answers of this round are between different residue classes because comparisons within the same residue class modulo k_{i+1} are always answered as equal.

(b) Unequal answers which involve symbols which were fixed before this round are consistent because fixed values dictate the answers to the comparisons. Unequal answers which involve symbols that are fixed at the end of this round and at least one was fixed at this round are consistent since a new symbol is used for each residue class fixed.

THEOREM 1. *Any comparison-based parallel algorithm for finding the period length of a string $S[1..m]$ using m comparisons in each round requires $\frac{1}{4}\log\log m$ rounds.*

PROOF. The choice is still open after each round. □

THEOREM 2. *The lower bound holds also for order comparisons.*

PROOF. The adversary gradually defines the linear order of the symbols. He does it in such a way that the answers to comparisons in round i are determined at the round or before. The order is determined by a lexicographic order on a name given to each symbol and is extended for unfixed symbols at each round. □

From the remark at the beginning of this section:

THEOREM 3. *The lower bound holds also for any comparison-based string matching algorithm.*

3. More comparisons in each round

One can use the trivial algorithm to solve the string matching problem in constant time if m^2 comparisons are available in each round on a CRCW-PRAM. Therefore, no more than m^2 processors are necessary. If the number of processors p is smaller than $\frac{m}{\log\log m}$ then one can slow down the $\log\log m$ algorithm in [4] to run in $O(\frac{m}{p})$ time. Additionally:

THEOREM 4. *Any comparison-based parallel algorithm for finding the period length of a string $S[1..m]$ using p comparisons, $m \leq p \leq m^2$, in each round requires at least $\Omega(\log\log_{\frac{2p}{m}} p)$ rounds.*

PROOF. We change m to p in the appropriate places of the proof. In particular we choose $K_i = p^{1-4^{-(i-1)}}$. The adversary can go on as long as $K_i \leq \frac{m}{2}$, i.e. $i = \Theta(\Omega(\log\log_{\frac{2p}{m}} p))$. □

Bibliography

[1] Apostolico (A.), Iliopoulos (C.), Landau (G. M.), Schieber (B.), and Vishkin (U.). – Parallel construction of a suffix tree with applications. *Algorithmica*, vol. 3, 1988, pp. 347–365.

[2] Borodin (A. B.), Fischer (M. J.), Kirkpatrick (D. G.), Lynch (N. A.), and Tompa (M.). – A time-space tradeoff for sorting on non-oblivious machines. In *Proceedings 20th IEEE Symposium on Foundations of Computer Science*, pp. 294–301. – 1979.

[3] Boyer (R. S.) and Moore (J. S.). – A fast string searching algorithm. *Communications of the ACM*, vol. 20, 1977, pp. 762–772.

[4] Breslauer (D.) and Galil (Z.). – An optimal $O(\log\log n)$ parallel string matching algorithm. *SIAM Journal on Computing*, vol. 19, n° 6, 1990, pp. 1051–1058.

[5] Crochemore (M.). – String-matching and periods. *Bulletin of the EATCS*, October 1989.

[6] Crochemore (M.) and Perrin (D.). – *Two Way Pattern Matching.* – Technical report, LITP, 1989.

[7] Fich (F. E.), Ragde (R. L.), and Wigderson (A.). – Relations between concurrent-write models of parallel computation. In *Proceedings of the 3rd ACM Symposium on Principles of Distributed Computing*, pp. 179–189. – 1984.

[8] Galil (Z.). – Optimal parallel algorithms for string matching. *Information and Control*, vol. 67, 1985, pp. 144–157.

[9] Galil (Z.) and Seiferas (J.). – Saving space in fast string-matching. *SIAM Journal on Computing*, n° 2, 1980, pp. 417–438.

[10] Galil (Z.) and Seiferas (J.). – Time-space-optimal string matching. *Journal of Computer System Science*, vol. 26, 1983, pp. 280–294.

[11] Geréb-Graus (M.) and Li (M.). – Three one-way heads cannot do string matching. – Manuscript.

[12] Knuth (D. E.), Morris (J.), and Pratt (V.). – Fast pattern matching in strings. *SIAM Journal on Computing*, vol. 6, 1977, pp. 323–350.

[13] Li (M.). – *Lower bounds on string-matching.* – Technical Report n° TR 84-636, Department of Computer Science, Cornell University, 1984.

[14] Li (M.) and Yesha (Y.). – String-matching cannot be done by a two-head one-way deterministic finite automaton. *Information Processing Letters*, vol. 22, 1986, pp. 231–235.

[15] Rosser (J. B.) and Schoenfeld (L.). – Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, vol. 6, 1962, pp. 64–94.

[16] Valiant (L. G.). – Parallelism in comparison models. *SIAM Journal on Computing*, vol. 4, 1975, pp. 348–355.

[17] Vishkin (U.). – Optimal parallel pattern matching in strings. *Information and Control*, vol. 67, 1985, pp. 91–113.

[18] Vishkin (U.). – Deterministic sampling: A new technique for fast pattern matching. In *STOCS'90*, vol. 22, pp. 170–179. – 1990. Baltimore, MD.

Algorithmes de contrôle de réseaux à hauts débits

Philippe Jacquet
INRIA Rocquencourt

April 26, 1993

[résumé par Philippe Jacquet]

1. Introduction : les réseaux à hauts débits

Une problématique des réseaux à hauts débits proches de la norme ATM est introduite. Les composants rapides qui sont directement en contact avec le support optique du réseau présentent des capacités d'intégration limitées : à hautes vitesses, faibles capacités de mémoire. Au dessus de ces composants très rapides se trouvent les composants ordinaires de la station connectée : grandes capacités de mémoire pour des vitesses modérées.

Un paquet est constitué d'un nombre variable de cellules de taille fixe qui sont les composants élémentaires des données qui circulent sur le réseau. Les cellules trouvent leur place sur des slots.

Au cours de la réception d'un paquet dans une station, le composant rapide procède au transfert des cellules du réseau vers un buffer rapide (faible capacité). Le composant lent transfère les cellules des buffers rapides vers des buffers lents (mais à grande capacité). En phase d'émission, le processus est inverse : le composant lent dépose les cellules dans les buffers rapides et le composant rapide assure le transfert des buffers au réseau lui même.

La faible capacité des buffers rapides liée à la lenteur des composants à grande capacité constitue le maillon critique du système et nécessite des algorithmes de contrôle de flux originaux. Cet exposé résume un rapport de recherche de Paul Mühlethaler et Philippe Jacquet.

2. L'algorithme de contrôle de flux

La problématique des réseaux à haut débit introduit la nouveauté suivante : les délais de propagation sont trop importants pour permettre le blocage des stations pendant l'aller et retour d'une simple requête d'émission. L'algorithme proposé permet à la station de continuer à transmettre entre deux requêtes. Les délais de propagation d'aller et retour sont supposés identiques entre chaque paire de stations comme c'est le cas sur les architectures en anneau.

Algorithme proposé :

(1) chaque fois qu'une station a un paquet à transmettre elle envoie une cellule de requête à l'adresse de la destination ; la cellule de requête contient la durée prévue de la transmission du paquet entre sa première et sa dernière cellule (nombre de cellules multiplié par l'intervalle inter-cellulaire) ; en attendant le retour de la requête le paquet reste en buffer lent ;

(2) la station source sépare chacune de ses requêtes, sans regard de leurs destinations, d'un intervalle de temps de durée au moins égale au temps présumé de transmission des paquets annoncé ;

(3) à chaque requête reçue, la station destinatrice renvoie vers la source une cellule de réponse contenant la valeur d'un compteur appelé compteur de transmission ; ensuite, sans regard sur la provenance de cette requête, la station destination augmente son compteur de transmission de la quantité contenue dans la cellule de requête ;

(4) la destination décrémente son compteur à chaque unité de temps : le compteur de transmission s'identifie à la longueur d'une file d'attente virtuelle ;

(5) la station source commence la transmission de son paquet (c'est-à-dire le dépile de ses buffers lents) à la date d'échéance c'est-à-dire la date de réception de la cellule de réponse plus la valeur du compteur de transmission qu'elle contient.

Le paquet reste stocké dans la mémoire de masse de la source (c'est-à-dire au niveau du composant lent) jusqu'à la date d'échéance. À la date d'échéance, le composant lent procède au transfert des cellules vers la mémoire du composant rapide. La fréquence de ce transfert en fait détermine la durée de l'intervalle inter-cellulaire, qui est supposé être identique pour toutes les stations du réseau. La variation introduite par les problèmes d'accès multiple au niveau du médium physique est négligée.

Comme la source ne s'abstient pas de transmettre pendant le délai d'acheminement de la requête, d'autres échéances peuvent expirer entre temps, de façon à ce que la station soit déjà en phase de transmission de paquet lorsqu'expire la dernière date d'échéance. Dans ce cas le dernier paquet reste en mémoire de masse et gagne une file d'attente. Ce genre de collision entre deux phases de transmission simultanées n'est susceptible d'avoir lieu que lorsque au moins deux destinations différentes sont concernées. La file d'attente ci-dessus décrite est appelée *file de sortie*.

La file d'attente dont il s'agit d'optimiser la longueur est la mémoire du composant rapide de la destination, appelée *file d'entrée*. Pour chaque paquet les cellules arrivent dans cette mémoire à la même fréquence qu'elles en sont extraites : c'est-à-dire la vitesse de transfert du composant lent. Donc si un paquet est unique en phase de réception ses cellules n'occuperont pas de manière significative la mémoire rapide. Si plus de deux paquets arrivent, leurs cellules cumuleront une fréquence d'arrivée double de la fréquence d'extraction et la file d'attente d'entrée s'allongera d'au moins un paquet. C'est ce genre de collision en file d'arrivées que l'algorithme cherche à éviter.

Exemples : Supposons qu'une source envoie tous ses paquets vers une seule destination. Les différents compteurs de transmission reçus n'entrent jamais en collision et la file de sortie reste toujours vide. Si toutes les sources d'une station visent cette station comme destinataire unique, il n'y a collision ni sur les files de sortie ni sur la file d'entrée.

3. Les files d'attente de La Palice : définition et propriétés

Le modèle mathématique qui convient à l'algorithme de contrôle de flux ci-dessus décrit est le modèle des files d'attente de La Palice. Une file de La Palice est une file classique FIFO, avec un serveur en général unique, dans laquelle les clients arrivent selon une loi particulière au modèle :

(1) chaque client a un temps de service S et une date de rendez-vous, S est une variable aléatoire ;
(2) les dates de rendez-vous de deux clients successifs sont séparées par un laps de temps de durée supérieure ou égale au temps de service du premier des deux clients ;
(3) chaque client arrive dans la queue avec un retard spécifique D, D est une variable aléatoire.

Ces files d'attente de La Palice (introduites dans [1] et [2]) ont des propriétés intéressantes. Le paramètre intéressant est le délai d'attente W en file ou la charge Q. W et Q sont des variables aléatoires (respectivement associées au client et au temps).

Une première propriété (la plus évidente, origine de l'attribution du nom de La Palice) est que si le retard D est identiquement nul ou constant, alors il n'y a pas de file d'attente à proprement parler : W et Q sont identiquement nuls.

Une seconde propriété un peu moins évidente est que si D et S sont des variables aléatoires bornées, par exemple respectivement par Δ et Σ, alors W et Q sont des variables aléatoires bornées par $\Delta + \Sigma$.

La dernière propriété, de loin la moins évidente, suppose l'indépendance de S et D plus quelques conditions de stabilité de la loi d'arrivée des clients, comme par exemple : l'écart entre deux dates de rendez-vous est en moyenne strictement supérieure à la moyenne du temps de service. La propriété nécessite aussi l'introduction d'une nouvelle terminologie. Une variable aléatoire est sous-exponentiellement Ax^α si $-\log \Pr\{X > x\}$ est supérieur à Ax^α quand $x \to \infty$. Dans la file de La Palice stabilisée, si le temps de service S est sous-exponentiellement Ax^α et le retard D est sous-exponentiellement Bx^β, avec A, B, α et β supérieurs à zéro, alors W et Q sont sous-exponentiellement Cx^γ, pour certains C et γ explicites :

(i) si $\alpha > \beta$ et $\alpha > 1$ alors $\gamma = \beta + 1 - \beta/\alpha$ et $C = \frac{(A\alpha)^{1/\alpha}}{\gamma}(B(1-1/\alpha))^{1-1/\alpha}$;
(ii) si $\alpha < \beta$, alors W et Q s'alignent sur le temps de service S avec $\gamma = \alpha$ et $C = A$;
(iii) si la variable aléatoire S est bornée par une constante Σ (équivalent à $\alpha = \infty$), alors $\gamma = \beta + 1$ et $C = \frac{B}{(\beta+1)\Sigma}$.

Le point (iii) sera utilisé pour une modélisation de l'algorithme de contrôle de flux.

4. Algorithme de contrôle de flux et files de La Palice

Les files de sortie et d'entrée peuvent être vues comme des files de La Palice.

La file de sortie : les temps de service S des paquets sont leur durée de transmission. Les paquets ont des dates de rendez-vous qui sont les dates de retour des requêtes : comme les requêtes sont séparées de plus du temps de service S et que les délais de propagation sont tous identiques, les dates de rendez-vous obéissent au modèle de La Palice. Le retard D est égal à la valeur du compteur de transmission reçu dans la cellule de réponse. On appelle W le délai d'attente du paquet dans la file de sortie.

La file d'entrée : Le temps de service est toujours S mais la date de rendez-vous est maintenant la date d'échéance, c'est-à-dire la date de retour de requête plus la valeur du compteur de transmission. Le retard est le délai W subi dans la file de sortie.

Dans le modèle qui suit on suppose un cas le pire : les destinations des sources et les sources des destinations sont complètement indépendantes et les trafics sont uniformément distribués. Il est intuitif qu'une destination ou une source plus favorisée ne peut qu'améliorer les performances de l'algorithme comme l'illustrent déjà les exemples décrits plus haut. Cette indépendance des sources et destinations fait que les paquets subissent dans la file de sortie des retards D indépendants, et dans la file d'entrée, des retards W indépendants.

Nous faisons l'hypothèse simplificatrice de paquet de durée égale à une unité de temps. Soit λ le taux d'arrivée des paquets par unité de temps. Les compteurs de transmission se comportent comme des longueurs de files d'attente M/D/1 et ont donc un comportement exponentiel : $\Pr\{D > n\} \sim \lambda^n$.

En d'autres termes D est sous-exponentiel $(-\log\lambda)x$. En conséquence l'analyse des files d'attente de La Palice dans le cas S borné par l'unité (cas (iii)) nous donne W sous-exponentiel $\frac{-\log\lambda}{2}x^2$. En fait une analyse plus précise peut nous donner $\Pr\{W > n\} \sim \lambda^{n(n+1)/2}$.

Dans la file d'entrée, le retard W étant maintenant sous-exponentiel $\frac{-\log\lambda}{2}x^2$, alors la charge Q de la file (exprimée en paquets stockés) est sous-exponentielle $\frac{-\log\lambda}{6}x^3$. Une analyse plus spécifique conduit à $\Pr\{Q > n\} \sim \lambda^{n(n+1)(n+2)/6}$. Noter le gain appréciable par rapport à λ^n que l'on aurait sans contrôle de flux. Une variante déterministe existe dans laquelle on recommence toute requête dès que le délai W dépasse un certain seuil constant. Dans ce cas on applique la propriété numéro deux des files de La Palice.

Bibliographie

[1] Jacquet (Philippe). – *More than exponential tail distribution in La Palice queues.* – Research Report n° 1465, Institut National de Recherche en Informatique et en Automatique, 1991.

[2] Jacquet (Philippe) et Mühlethaler (Paul). – *A very simple algorithm for flow control on high speed networks via La Palice queueings: description and analysis.* – Research Report n° 1371, Institut National de Recherche en Informatique et en Automatique, 1991.

Variations on the Stack Protocol for Collision Resolution

Nikita Vvendenskaya
Academy of Sciences, Moscow

June 24, 1993

Abstract

The problem considered is that of protocol design and analysis for regulating access to a channel shared by many users. A collision resolution protocol called the stack algorithm was discovered by N. Vvendenskaya and B. Tsybakov near 1980 and achieves this goal. The algorithm bears strong relations to the tree protocol proposed independently by Capetanakis. Like the Ethernet protocol, the stack algorithm permits to resolve probabilistically collisions on a shared communication channel. Unlike the Ethernet protocol, it appears to have good stability properties.

Bibliographical data

The original stack algorithm is described by Tsybakov, Mikhailov and Vvedenskaya in [4, 5]. The idea is to separate recursively colliders into groups based on random coin flippings. (In contrast, Ethernet uses increasing delays determined probabilistically in the case of a collision.)

Early results on such random access methods are presented in the book edited by Longo [3]. It has been established that the protocol (in the slotted time model and under Poisson arrivals) is stable for arrival rates till $\lambda = 0.34$ (blocked arrivals), $\lambda = 0.36$ (continuous arrivals), see [1, 2] for detailed analyses based on functional equations and Mellin transforms. (In contrast, Ethernet is known to be unstable for any $\lambda > 0$, a result due to Aldous.) Various improvements due to Gallager, Massey, Greenberg, and others permit to come close to the limit of $\lambda = 0.5$.

The special issue of the *IEEE Transactions on Information Theory* on *Random Access Communication* edited by Jim Massey (*IEEE-IT* **31**(2), March 1985) contains a complete survey that still serves as a reference in the field.

Bibliography

[1] Fayolle (G.), Flajolet (P.), and Hofri (M.). – On a functional equation arising in the analysis of a protocol for a multiaccess broadcast channel. *Advances in Applied Probability*, vol. 18, 1986, pp. 441–472.

[2] Fayolle (G.), Flajolet (P.), Hofri (M.), and Jacquet (P.). – Analysis of a stack algorithm for random access communication. *IEEE Transactions on Information Theory*, vol. IT-31, n° 2, March 1985, pp. 244–254. – Special Issue on Random Access Communication, J. Massey (editor).

[3] Longo (G.) (editor). – *Multi-User Communication Systems*. – Springer-Verlag, *CISM Courses and Lecture Notes*, vol. 265, 1981.

[4] Tsybakov (B.) and Mikhailov (V.). – Free synchronous packet access in a broadcast channel with feedback. *Problems of Information Transmission*, vol. 14, 1978, pp. 259–280.

[5] Tsybakov (B.) and Vvedenskaya (N.). – Random multiple access stack algorithms. *Problems of Information Transmission*, vol. 16, 1978, pp. 230–243.

Ergodic Theory and Average Case Analysis of Euclid's Algorithm

Hervé Daudé
Université de Caen

March 22, 1993

[summary by Philippe Flajolet]

Abstract

This presentation proposes a transfer principle from the continuous to the discrete in the context of the average case analysis of the Euclidean GCD algorithm. By this principle, it is possible to transfer a central limit theorem on the denominators of convergents associated with continued fraction expansions of real numbers to rational fractions naturally associated to the Euclidean GCD algorithm. There results an estimation of small and large deviation probabilities for the Euclidean algorithm. Ergodic theory permits to place these results in a wider perspective.

Bibliographical data

The history of the analysis of the Euclidean algorithm till about 1980 appears in Knuth's book *"Seminumerical Algorithms"* [7].

The worst case of the algorithm on fractions $\frac{p}{q}$ with p, q bounded by N is about $\log_\varphi N$ (with $\varphi = (1+\sqrt{5})/2$) and is related to Fibonacci numbers, as discovered by Lamé in 1845.

The average case is asymptotic to

$$\frac{12 \log 2}{\pi^2} \log N,$$

as was discovered independently by Dixon [3] and Heilbronn [4] near 1970. Asymptotic refinements of the average case formula have been given by Porter and Knuth, see [7].

While Heilbronn's approach is number–theoretic, Dixon's proof is based on properties of continued fraction expansions of real numbers. It had been conjectured by Gauß that the kth iterate in the continued fraction expansion of a random uniform $x \in [0,1]$ has a distribution that tends to the so–called Gauß law with density

$$\frac{1}{\log 2} \frac{1}{1+x}.$$

As Gauß himself said: *"Tam complicatæ evadunt ut nulla spes superesse videatur"*.

Gauß's problem was only solved by Paul Lévy in 1929, with successive refinements introduced by Kuzmin and Wirsing who characterized the speed of convergence (as a decaying exponential), and eventually by Babenko who gave an exact spectral decomposition [1] of the distribution of the kth iterate as an infinite sum of decreasing exponentials.

The existence of a limit distribution can be connected to ergodic theory as was noted after Khinchin's work [6] and part of the talk followed this thread. In this context, Gauß's law is nothing but the invariant measure associated with the continued fraction transformation:

$$T(x) = \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor.$$

In another direction, it had been proved by Philipp [10] using probabilistic methods that the logarithm of the denominator of a random $x \in [0,1]$ follows a Gaussian law in the limit. Dixon and Daudé make use of this result by transferring properties of the continuous model of continued fractions to the discrete model of rational fractions that underlies the Euclidean algorithm.

Daudé [2, Chap. 1] establishes in this context two results: one that indicates that the probability of "small deviations" is large enough (this resembles a partial limit density estimate for the Euclidean algorithm), another dual one that the probability of "large deviations" is small. Daudé's thesis also contains corresponding results for the variant of the Euclidean algorithm based on the centered quotient–remainder transformation.

Recently, these results have been made more precise by Hensley [5] who established a central limit theorem for the number of steps of the Euclidean algorithm. Hensley's approach depends on functional properties of an operator $\mathcal{G}_s$, closely associated with continued fractions:

$$\mathcal{G}_s[f](z) = \sum_{n=1}^{\infty} \frac{1}{(n+z)^s} f(\frac{1}{n+z}).$$

The functional analysis approach to these problems itself takes its roots in earlier works of Wirsing [12], Babenko [1] and Mayer [8, 9].

The techniques of the talk prove useful for the average case analysis of a lattice reduction algorithm in dimension 2 also due to Gauss, see [2, Chap. 2] and [11].

Bibliography

[1] Babenko (K. I.). – On a problem of Gauss. *Soviet Mathematical Doklady*, vol. 19, n° 1, 1978, pp. 136–140.

[2] Daudé (Hervé). – *Des fractions continues à la réduction des réseaux: analyse en moyenne.* – PhD thesis, Université de Caen, 1993.

[3] Dixon (J. D.). – The number of steps in the Euclidean algorithm. *Journal of Number Theory*, vol. 2, 1970, pp. 414–422.

[4] Heilbronn (H.). – On the average length of a class of continued fractions. In Turan (Paul) (editor), *Number Theory and Analysis*. pp. 87–96. – New York, 1969.

[5] Hensley (Doug). – The number of steps in the Euclidean algorithm, 1993.

[6] Khinchin (A. I.). – *Continued Fractions*. – University of Chicago Press, Chicago, 1964. A translation of the Rusian original published in 1935.

[7] Knuth (Donald E.). – *The Art of Computer Programming*. – Addison-Wesley, 1981, 2nd edition, vol. 2: Seminumerical Algorithms.

[8] Mayer (D.) and Roepstorff (G.). – On the relaxation time of Gauss's continued fraction map. I. The Hilbert space approach. *Journal of Statistical Physics*, vol. 47, n° 1–2, April 1987, pp. 149–171.

[9] Mayer (D.) and Roepstorff (G.). – On the relaxation time of Gauss's continued fraction map. II. The Banach space approach (transfer operator approach). *Journal of Statistical Physics*, vol. 50, n° 1–2, January 1988, pp. 331–344.

[10] Philipp (W.). – Ein zentraler Grenzwertsatz mit Anwendungen auf die Zahlentheorie. *Zeitschrift für Wahrscheinlichkeitstheorie*, vol. 8, 1967, pp. 195–203.

[11] Vallée (Brigitte) and Flajolet (Philippe). – Gauss' reduction algorithm: An average case analysis. In *Proceedings of the 31st Symposium on Foundations of Computer Science*. pp. 830–839. – IEEE Computer Society Press, October 1990.

[12] Wirsing (E.). – On the theorem of Gauss-Kusmin-Lévy and a Frobenius-type theorem for function spaces. *Acta Arithmetica*, vol. 24, 1974, pp. 507–528.

The development of a randomized algorithm for the dynamic closest-pair problem

Mordecai Golin
INRIA Rocquencourt

14 Décembre 1992

Abstract

This talk describes the development of new randomized data structure, the *sparse-grid partition*, for solving the dynamic closest-pair problem. Using this data structure the closest pair of a set of n points in k-dimensional space, for any fixed k, can be found in constant time. The data structure supports insertions into and deletions from the set in expected $O(\log n)$ time and requires expected $O(n)$ space (assuming the updates are chosen by an adversary who does not know the random choices made by the data structure).
If time permits we will also discuss a new randomized incremental algorithm for the closest-pair problem that uses only O(1) expected time per insertion/deletion.
The above is joint work with with Rajeev Raman, Christian Schwarz and Michiel Smid.

Transformation of Parallel Programs Guided by Micro-Analysis

Aline Weitzman
Brandeis University

October 5, 1992

[summary by Paul Zimmermann]

Abstract

In this talk A. Weitzman provides a summary of the past work done at Brandeis in micro-analysis, and outlines some new research directions which are the subject of her dissertation. The overall goal is to develop program manipulation and analysis tools which help a user in transforming parallel programs so as to render them more efficient for execution in a variety of parallel machines. One of the original contributions of this work is in the usage of symbolic processing and constraint logic programming to analyse and manipulate parallel programs for parallel computers. In the talk A. Weitzman provides: 1. a description of micro-analysis applicable to sequential programs, 2. micro-analysis approach for SIMD programs, 3. micro-analysis approach for MIMD programs, 4. automatic transformation scheme for translating SIMD programs to MIMD programs, guided by micro-analysis.

1. Introduction

Two different approaches are possible in order to establish the performance of a computer program: either make some *benchmarks*, that is measure the time used by the program on some input data, or try to derive some general formulæ (*time-formulæ*) that express the execution time of the program in terms of the time to perform basic (elementary) instructions, such as an addition of two registers, or a comparison between two variables. The second approach, which is called *micro-analysis*, has two main advantages. First it does not depend on a specific machine, because the time-formulæ are valid for any machine; only times to perform each basic instruction have to be determined for a given computer, but only *once* for each machine. Secondly the time-formulæ can be derived automatically, without running the program. The micro-analysis approach enables us to estimate the performance of programs on machines yet to be built, or to evaluate the effect of program changes.

Thus, the aim of micro-analysis is to derive from a program a *time-formula*, which is a symbolic formula for the execution time of the program. The symbolic variables of the time-formula are the *time-variables*, which represent the time to perform common elementary operations (addition, assignment, subscripting, loop overhead, ...). For example, the statement

```
a[i,k] := b*(c+d+e)
```

has the time-formula $t_{subs2} + t_{assign} + t_{mult} + 2t_{add}$, and the loop

```
for i := 1 to n do
   a[i,k] := b*(c+d+e)
```

has the time-formula $n(t_{foroh} + t_{subs2} + t_{assign} + t_{mult} + 2t_{add})$.

2. Analysis of sequential programs

The heart of micro-analysis is the *time-formula generator*. It takes as input the program to be analyzed, and interactively asks the user to provide

- the probabilities with which branches of conditionals (*if then else*) are executed. These probabilities can be fixed (numeric or symbolic values) or can be specified as functions of given parameters;
- the number of times **while**-loops are performed. This number may also be symbolic or a function of given parameters.

For example, with the following program as input,

```
z=0; j=1;
while (j<=n) {
   if (x[j]==1) z=z+y;
   j=j+1; y=2*y;
}
```

the time-formula generator asks for the probability that `x[j]==1` becomes true and the number of times the `while` loop is executed, the user answer respectively p and n. Then the system outputs the following time-formula, with the help of MAPLE:

$$Formula = n(t_{whileoh} + t_{lesseq} + t_{mult} + (p+2)t_{assign} + (p+1)t_{add} + t_{cond} + t_{subs1} + t_{equal}) + 2t_{assign}.$$

Determining loop invariants. In some cases, the number of times loops are performed can be determined automatically. This is done by the *finite-difference equations generator*. The idea is to produce a set of finite-difference equations for the variables that are of interest in a given loop. Then, using the termination condition of the loop together with initial conditions provided by the program or the user, one uses a symbolic algebra system like MAPLE to solve the difference equations. Consider for example the loop

```
i=a; j=b;
while (i+j<n) {
   ...
   j=2*i; i=i+c;
}
```

The finite-difference equations generator outputs the solution

```
i(zz) = a + c * zz, j(zz) = 2 * a + 2 * c * zz - 2 * c
```

where zz is the number of times the loop has been executed (0 at the beginning). This result gives the number of iterations of the loop:

$$N = \left\lceil \frac{n - 3a + 2c}{3c} \right\rceil.$$

Determining values of time-variables. Once the time-formula of a given program has been derived, to obtain an estimation of the time complexity for a particular machine, one has to determine the numeric values of the time-variables $(t_{add}, t_{mult}, \dots)$ corresponding to this machine. For this aim, the first method that comes to mind is to execute N times an elementary instruction op, for example in a *for* loop, to measure the time used T, and to use the approximation

$$t_{op} \sim \frac{T}{N}.$$

A more accurate method has been proposed by T. Hickey. The idea is to use a set of *benchmark* programs $P_1, \dots, P_m$. One first runs all programs on the machine with counters for each elementary instruction. One thus obtains a set of vectors $c_1, \dots, c_m$. Each vector c_j contains the values of the elementary instruction counters for the benchmark P_j. One runs once more every benchmark, but this time without the counters, and one measures the time t_j of the program P_j. Then one sets the following system of equations

$$(t_{foroh}, t_{add}, t_{mult}, \dots) \cdot c_j = t_j(1 + \epsilon_j), \quad 1 \le j \le m,$$

and one approximates the time-variables by the numeric values that minimize the sum

$$\sum_{1}^{m} |\epsilon_j|.$$

With this method, the author was able to determine the values of twenty different time-variables for two different machines (HP 9000 and Sun 3), with an error of at most 4%.

3. Analysis of parallel programs for SIMD machines

A SIMD (Single Instruction Multiple Data) machine is a parallel architecture where each processor has its own memory. The same program is executed synchronously on each processor, thus there is an instance of each variable of the program in every processor (they are called *parallel variables*). The processors communicate to each other with *send* or *get* instructions. In what concerns micro-analysis, the situation is very similar to sequential programs, except one has to consider the cost of communication instructions.

On the Connection Machine (CM-2) for example, there are two kinds of communications:

- grid communication: every processor, say number j, sends a value to a processor at a fixed distance d, thus to processor $j+d$. Experiments made by the author show that the cost of grid communication depends on the decomposition of the distance d into a sum (or difference) of powers of two. For example, $T_{\text{grid}}(42) = T_{\text{grid}}(32) + T_{\text{grid}}(8) + T_{\text{grid}}(2)$, and $T_{\text{grid}}(60) = T_{\text{grid}}(64) + T_{\text{grid}}(4)$. The lowest time is about $500\mu s$ on the CM-2;
- general communication: any processor j is allowed to send any value to a processor at any distance d_j. The cost of general communication is constant by hardware considerations: it is about $1500\mu s$ on the CM-2.

Thus the micro-analysis of SIMD programs is essentially the same as for sequential programs, except one has to introduce some new time-variables like t_{send}, t_{scan} to scan processors where a parallel variable has a given value, t_{pcoord} to get the processor number, t_{pvar_read} to read a parallel variable.

4. Analysis of parallel programs for MIMD machines

A MIMD (Multiple Instruction Multiple Data) machine is a parallel architecture where each processor executes its *own* set of instructions. An example is the Butterfly computer, where the main program, executed on one processor, can start some new processes on other processors, and wait for their answer. This architecture is asynchronous, thus the time-formulæ are of the form

$$Time = T_a + \max(T_b, T_d) + T_c$$

where T_a, T_b, T_c, T_d are time-formulæ themselves. Thus it is possible to determine conditions on time-variables such that the maximum of T_b and T_d is T_b, and *vice-versa*. Finally, one obtains a time-formula of the form

$$Time = \begin{cases} f_1 & \text{if } c_1 \\ f_2 & \text{if } c_2 \\ & \vdots \\ f_k & \text{if } c_k \end{cases}$$

where the f_j are time-formulæ without any *max* function, and the c_j are sets of linear constraints involving the time-variables.

5. Transformation of SIMD into MIMD programs

The micro-analysis of SIMD and MIMD programs suggests to the author the following two-step algorithm to translate a SIMD program into a MIMD program:

- first translate the SIMD program into an intermediate sequential program, by replacing all parallel variables by arrays (the index represents the processor number), and regrouping instructions that do not need synchronization in blocks as large as possible.
- then translate the intermediate sequential program into a MIMD program, by dividing the iterations of synchronization-free loops between the MIMD processors. The optimal number of processors is computed using micro-analysis tools (because of the overhead for starting a new process, the optimal number is not necessarily the maximum).

Appendix: on the cost of grid communication for the CM-2

A. Weitzman found the following interpolation formulæ for the communication time $F(n)$ for distance n. F_i represents F on the interval $[2^i, 2^{i+1}]$. The function F has a recursive representation defined by the following formula:

$$\begin{aligned} F_5 &= -|18(n-48)| + 801 \quad \text{if } 2^5 \le n \le 2^6 \\ F_6 &= -|18(n-96)| + 1089 \quad \text{if } 2^6 \le n \le 2^7 \end{aligned}$$

$$F_i = \left\{ \begin{array}{ll} \Delta & \text{if } 2^i \le n \le 2^i + 2^5 \\ \Delta' & \text{if } 2^{i+1} - 2^5 \le n \le 2^{i+1} \\ F_k + 576 & \text{if } \left(\begin{array}{l} 2^i + 2^k \le n \le 2^i + 2^{k+1} \quad \text{or} \\ 2^{i+1} - 2^{k+1} \le n \le 2^{i+1} - 2^k, \\ \text{where } 5 \le k \le i-2 \end{array} \right) \end{array} \right\} \quad \text{if } 2^i \le n \le 2^{i+1},\ i \ge 7$$

where :

$$\begin{aligned} \Delta &= 18(n+28) \\ \Delta' &= 18(-n+28) \end{aligned}$$

For example, F_8 is $\Delta \diamond F_5 \diamond F_6 \diamond F_6 \diamond F_5 \diamond \Delta'$, where $f \diamond g$ represents the juxtaposition of f and g. In fact, F_i can be represented as $\Delta \diamond F_5 \diamond F_6 \diamond \cdots \diamond F_{i-2} \diamond F_{i-2} \diamond \cdots \diamond F_6 \diamond F_5 \diamond \Delta'$. The function F_i can be approximated using the central limit theorem:

$$F_i \approx 172i - 146 \quad \text{if } 2^i \le n \le 2^{i+1},\ i \ge 5$$

We can define the optimal cost $F(n)$ of grid communication between two processors at distance n on the Connection Machine as follows:

$$\begin{aligned} F(0) &= 0 \\ F(2^k) &= 1 \\ F(n) &= 1 + \min(F(n-2^k), F(2^{k+1} - n)) \quad \text{for } 2^k < n < 2^{k+1} \end{aligned}$$

This function can be easily defined in MAPLE:

```
F := proc(n)
local k;
    k := log2(n);
    if n=2^k then 1 else 1+min(F(n-2^k),F(2^(k+1)-n)) fi;
end:

log2 := proc(n) if n=1 then 0 else 1+log2(iquo(n,2)) fi end:

> seq(F(i),i=1..50);

 1, 1, 2, 1, 2, 2, 2, 1, 2, 2, 3, 2, 3, 2, 2, 1, 2, 2, 3, 2, 3, 3, 3, 2, 3, 3,

     3, 2, 3, 2, 2, 1, 2, 2, 3, 2, 3, 3, 3, 2, 3, 3, 4, 3, 4, 3, 3, 2, 3, 3
```

where `iquo(n,2)` is the MAPLE notation for the integer quotient of n by 2, and the auxiliary function `log2` computes the floor of the logarithm in base 2. The smallest n such that $F(n) = 4$ is $43 = 2^5 + 2^3 + 2^1 + 2^0$.

This function F appears in several fields of computer science. For example, in arithmetics and number theory, $F(n)$ is the minimal number of multiplications or divisions needed to compute a^n, once we know $a, a^2, a^4, a^8, \ldots$. This is the well-known problem of addition-subtraction chains which was studied by F. Morain and J. Olivos [2] to speed up the computations on an elliptic curve.

The sequence $(f_n = F(n))$ is also interesting because it is 2-regular, that is that the sub-sequences (f_n), (f_{2n}), (f_{2n+1}), (f_{4n}), (f_{4n+1}), (f_{4n+2}), (f_{4n+3}), $(f_{8n}), \ldots$ span a vector space of finite dimension. Namely, Ph. Dumas determined that $(f_n, f_{2n+1}, f_{4n+1}, f_{4n+3})$ is a basis of that vector space and that

$$f_{2n} = f_n, f_{8n+1} = f_{4n+1}, f_{8n+3} = f_{8n+5} = -f_n + f_{2n+1} + f_{4n+1}, f_{8n+7} = f_{4n+3}.$$

Philippe Dumas suggests that defining $\delta_n = \Delta f_n = f_{n+1} - f_n$ and using the Mellin-Perron formula as in

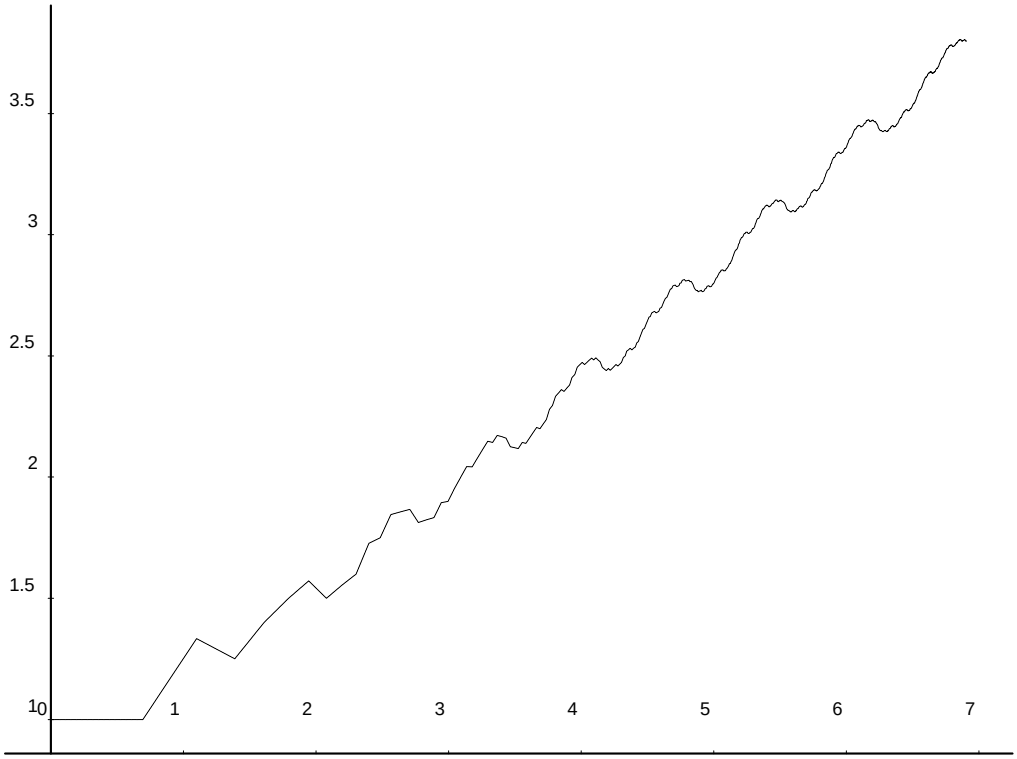


FIGURE 1. Plot of g_n/n as a function of $\log(n)$, for $1 \leq n \leq 1000$.

[1] would give some asymptotic estimates for the cumulated series $g_n = f_1 + \cdots + f_n$. In fact, Mordecai Golin already discovered a fractal form for g_n (figure 1) that looks like the fluctuations in the average case of Mergesort [1].

Bibliography

[1] Flajolet (Philippe) and Golin (Mordecai). – *Mellin Transforms and Asymptotics: The Mergesort Recurrence.* – Report, Institut National de Recherche en Informatique et en Automatique, January 1992. 11 pages.

[2] Morain (F.) and Olivos (J.). – Speeding up the computations on an elliptic curve using addition-subtraction chains. *RAIRO Technical Informatics and and Applications*, vol. 24, n° 6, 1990, pp. 531–543.

Probabilistic Recurrence Relations for Divide-and-Conquer Algorithms

Wolf Zimmermann
Brandeis University

September 21, 1992

[summary by Paul Zimmermann]

Abstract

Probabilistic recurrence relations occur frequently in the analysis of randomized algorithms. After an introduction to the work of Karp on probabilistic recurrence relations of the form

$$T(n) = a(n) + T(h(n)) \tag{1}$$

where $h(n)$ is a random variable, we discuss probabilistic recurrence relations for divide-and-conquer algorithms. In (sequential and parallel) divide-and-conquer algorithms a problem of size n is usually divided in subproblems of size $h_1(n), \ldots, h_k(n)$ where the $h_i(n)$ are (not necessarily independent) random variables. The analysis of the time complexity of parallel divide-and-conquer algorithms or the space complexity of sequential divide-and-conquer algorithms leads to a recurrence of the form

$$T(n) = a(n) + \max(T(h_1(n)), \ldots, T(h_k(n))). \tag{2}$$

On the other hand, the analysis of the time complexity of sequential divide-and-conquer algorithms and the space complexity of parallel divide-and-conquer algorithms leads to a recurrence of the form

$$T(n) = a(n) + T(h_1(n)) + \cdots + T(h_k(n)).$$

For both types of probabilistic recurrences, we give an upper bound for the probability distribution on $a(n)$, if the distribution of the $h_i(n)$ is unknown. The only informations needed are upper bounds on the expected values of the $h_i(n)$. (Joint work with Marek Karpinski.)

The problem here is to find an upper bound for $T(n)$, with little information about the distribution of $h(n)$, $h_1(n), \ldots, h_k(n)$.

Karp studied Equation (1) with the following assumptions [1]:

(i) $a(n) \geq 0$,
(ii) $h(n)$ is a random variable over $[0, n]$,
(iii) $E[h(n)] \leq m(n)$ where $0 \leq m(n) < n$, and $m(n)$ and $m(n)/n$ are non-decreasing.

Under these conditions, if one defines $u(n)$ to be the least non-negative solution of

$$\tau(n) = a(n) + \tau(m(n)),$$

we have two results according to the function $a(n)$.

THEOREM 1. *If $a(n) = 0$ for $n < d$ and $a(n) = 1$ for $n \geq d$, let $c_t = \min\{x \mid u(x) \geq t\}$, then*

$$\Pr[T(n) \geq u(n) + n] \leq \left(\frac{m(n)}{n}\right)^{n-1} \frac{m(n)}{c_{u(n)}}.$$

THEOREM 2. *If $a(n)$ is continuous and strictly increasing, then $m(n)$ is continuous and*

$$\Pr[T(n) \geq u(n) + na(n)] \leq \left(\frac{m(n)}{n}\right)^{n}.$$

In the general case of equation 2, Wolf Zimmermann and Marek Karpinski obtained the following result [2].

THEOREM 3. *Let $a(n)$ be continuous, non-decreasing, and strictly increasing on $\{n \mid a(n) > 0\}$. Also let the $m_i(n)$ be strictly increasing. Then, for every instance z of size n and every positive integer j, we have*

$$\Pr[T(z) \geq u(n) + ja(n)] \leq \left(\frac{m_1(n) + \cdots + m_k(n)}{n}\right)^{j}.$$

Bibliography

[1] Karp (Richard M.). – Probabilistic recurrence relations. In *Proceedings of the Twenty Third Annual ACM Symposium on Theory of Computing*. pp. 190–197. – ACM Press, 1991.

[2] Karpinski (M.) and Zimmermann (W.). – *Probabilistic Recurrence Relations for Parallel Divide-and-Conquer Algorithms*. – Technical Report n° TR-91-067, ICSI, Berkeley, 1991.

Part V

Miscellany

Problems and results on polynomials

Andrzej Schinzel
Académie des Sciences de Pologne, Varsovie

January 25, 1993

[summary by Philippe Dumas]

The aim of the talk is to survey some problems on factorization of polynomials, polynomials with sparse powers, and irreducibility of binomials and trinomials.

1. Factorization of binomials

In 1895 Vahlen gave a necessary and sufficient condition for the reducibility of a binomial:

the binomial $X^n - a$ is reducible over $\mathbb{Q}$ iff
- $a = b^p$ with p a prime number which divides n and b is rational,
- or $a = -4\,b^4$, the number n is a multiple of 4 and b is rational.

Capelli extended the result two years later to the fields of characteristic 0 and Rédei treated the case of a positive characteristic. These results give the following theorem.

Theorem 1 (Capelli theorem). *The binomial $X^n - a$ has at least one irreducible factor whose number of nonzero coefficients is less or equal to three.*

One cannot improve the result since

$$X^4 + 4 = (X^2 - 2\,X + 2)(X^2 + 2\,X + 2).$$

2. Ritt theorems

Another type of factorization uses the composition instead of the product and Ritt published in 1922 an important work about the subject. At first if a complex polynomial f is prime and may be written $f = g \circ h$ then g or h has degree 1. Next the existence of such a factorization is obvious but there is no uniqueness because $g \circ h = (g \circ l) \circ (l^{[-1]} \circ h)$ if l has degree 1 and $l^{[-1]}$ is the functional inverse of l. One may hope for a result of quasi-uniqueness modulo linear functions, but the next example shows this is not the case.

$$\begin{gathered} f_1 = X^r\,P(X)^n, \qquad f_2 = X^n, \\ g_1 = X^n, \qquad g_2 = X^r\,P(X^n), \\ f_1 \circ f_2 = g_1 \circ g_2 = X^{rn}\,P(X^n)^n. \end{gathered}$$

Ritt showed the following theorem for the complex number field $\mathbb{C}$.

Theorem 2 (First Ritt theorem). *If a polynomial f admits the two factorizations*

$$f = f_1 \circ \cdots \circ f_r = g_1 \circ \cdots \circ g_s$$

then the two sequences of degrees

$$\deg f_1, \ldots, \deg f_r\,; \quad \deg g_1, \ldots, \deg g_s$$

have the same length and include the same terms.

In 1974 Dorey and Whaples extended the theorem to any field under the condition that the degree of f does not divide the characteristic (otherwise it is wrong).

Ritt also proved the difficult result which follows.

THEOREM 3 (SECOND RITT THEOREM). *There are only two cases which give an equality*

$$f_1 \circ f_2 = g_1 \circ g_2$$

with

$$\deg f_1 = \deg g_2 = m, \quad \deg f_2 = \deg g_1 = n$$

and $(n, m) = 1$. *The first is that of the example above and the second is*

$$\begin{aligned} f_1 &= D_m, \quad f_2 = D_n \\ g_1 &= D_n, \quad g_2 = D_m \end{aligned}$$

where D_k *is defined by*

$$D_k(X + X^{-1}) = X^k + X^{-k}.$$

Polynomials D_k are connected to Chebychev polynomials but they are defined even in characteristic 2 contrary to the latter. Zannier proved last year that the theorem is right for all algebraically closed fields in all characteristic under the condition that the derivatives f_1', f_2', g_1', g_2' are not the zero polynomial.

3. Polynomials with sparse powers

In 1947 Rényi built a polynomial of degree 23 the square of which has fewer nonzero coefficients than the polynomial itself. That looks paradoxical but Erdös proved that there exist an infinity of polynomials f the number of nonzero coefficients of which, $N(f)$, satisfies

$$N(f^2) < N(f)^c$$

with $c < 1$. Verdenius computed in 1949 a possible value of c,

$$c = \frac{\log 8}{\log 13},$$

using Erdös proof. Coppersmith and Davenport gave analogous results

$$N(f^k) < N(f)^c$$

but without improvement of the constant c. They proved that for each polynomial F there are positive constants C and c with $c < 1$ such that for any integer $N \geq 1$ there is a polynomial f, whose degree is N, such that $N = N(f) - 1$ (the polynomial f is complete) and

$$N(F(f)) < C\, N(f)^c.$$

On the other hand Schinzel proved in 1987 that

$$N(f^2) \gg \log\log N(f).$$

The proof is valid for $N(f^k)$ too, but does not give an inequality. One could look for an inequality

$$N(F(f)) > \varphi(N(f)),$$

where F is a polynomial like $F(x) = x^3 - x$.

4. Factorization of trinomials

Schinzel studied the reducibility of the trinomial

$$X^n + A\,X^m + B.$$

He gave a complete result for the case when $A,\ B \in \mathbb{K}(y)$ and an incomplete result for the case $A,\ B \in \mathbb{K}$, where $\mathbb{K}$ is an algebraic number field. Then the problem is almost solved for finite extensions.

The trinomial is reducible if and only if the reciprocal trinomial $B\,X^n + A\,X^{n-m} + 1$ is reducible so one may suppose that $n \geq 2\,m$. The first theorem concerns fields $\mathbb{K}(y)$ where y is a vector of variables, $\mathbb{K}$ is a field of characteristic $\kappa \geq 0$ which does not divide the product $nm(n-m)$ and we call n_1 and m_1 the quotients $n/(n,m)$ and $m/(n,m)$ respectively.

THEOREM 4 (FIRST SCHINZEL THEOREM). *If A and B are in $\mathbb{K}(y)^*$ and $A^{-n}B^{n-m}$ is not in $\mathbb{K}$ then the trinomial $X^n + A\,X^m + B$ is reducible over $\mathbb{K}(y)$ if and only if*

- *$X^{n_1} + A\,X^{m_1} + B$ has a proper factor of degree less than or equal to 2,*
- *or there exists an integer l such as satisfies the two following conditions: first $\{n/l,\ m/l\}$, which we call $\{\nu,\ \mu\}$, is one of $\{6,\ 1\}$, $\{6,\ 2\}$, $\{7,\ 1\}$, $\{8,\ 2\}$, $\{8,\ 4\}$, $\{9,\ 3\}$, $\{10,\ 2\}$, $\{10,\ 4\}$, $\{12,\ 2\}$, $\{12,\ 3\}$, $\{12,\ 4\}$, $\{15,\ 5\}$ or of the type $\{2\,p,\ p\}$ with p a prime number; next*

$$A = u^{\nu-\mu}A_{\nu,\mu}(v), \quad B = u^{\nu}B_{\nu,\mu}(v),$$

where u, v are in $\mathbb{K}(y)$ and polynomials $A_{\nu,\mu}$, $B_{\nu,\mu}$ are given in Table 1.

$\nu,\ \mu$	$A_{\nu,\mu}$	$B_{\nu,\mu}$
$2\,p,\ p$	$-[(1+\sqrt{1-4\,v}/2]^p - [(1-\sqrt{1-4\,v}/2]^p$	v^p
$6,\ 1$	$8\,v(v^2+1)$	$(v^2+4\,v-1)(v^2-4\,v-1)$
$6,\ 2$	$4\,(v+1)$	$-v^2$
$7,\ 1$	$-(2\,v+1)^4(4\,v^2-3\,v+1)$ $\times\,(v^3-2\,v^2-v+1)$	$v(2\,v-1)(2\,v+1)^5$ $\times\,(3\,v-2)(v^2-v-1)$
$8,\ 2$	$-v^2+8\,v-8$	$4\,(v-1)^2$
$8,\ 4$	$2\,v^2-8\,v+4$	v^4
$9,\ 3$	$v^3-81\,v+243$	$27\,(v-3)^3$
$10,\ 2$	$4\,v^3-8\,v+4$	$-(v^2-4\,v+2)^2$
$10,\ 4$	$v^5(-v^3+8\,v-8)$	$-4\,v^8(v-1)^4$
$12,\ 2$	$1024\,(v-4)^8(2\,v-3)$ $\times\,(v^2-6\,v+6)(3\,v^2-3\,v+1)$	$1024\,(v-4)^{10}(v^3-8\,v+8)$
$12,\ 3$	$-729\,v(v-1)^7(2\,v-1)$ $\times\,(3v^2-6\,v+2)(3\,v^2-3\,v+1)$	$729\,(v-1)^9(3\,v^3-3\,v+1)$
$12,\ 4$	$512\,(2\,v-1)(2\,v^2+2\,v-1)$ $\times\,(2\,v^2-2\,v+1)$	$1024\,(2\,v^2-4\,v+1)^4$
$15,\ 5$	$5\,(5\,v-5)^7(5\,v^4-5\,v^3-5\,v^2+5\,v-1)$ $\times\,(5\,v^4-10\,v^3+100\,v^2-5\,v+1)$	$(5\,v-5)^{10}(5\,v^2-5\,v+1)^5$

TABLE 1. Trinomials $X^{\nu l} + u^{\nu-\mu}A_{\nu,\mu}(v)\,X^{\mu l} + u^{\nu}B_{\nu,\mu}(v)$ are reducible.

The theorem presents a complete analogy with Capelli's theorem in which there is an exceptional case $a = -4\,b^4$ and an infinite sequence of exceptions corresponding to $a = b^p$. The proof rests on the existence of a lower bound for the genus of a certain algebraic curve except in a finite number of cases. Once this bound is known, the problem is solved by a method of indeterminate coefficients.

Schinzel gave a theorem for the algebraic function fields but it is too technical to be cited here and another theorem for the algebraic number fields (finite extension of $\mathbb{Q}$). The latter is rather complicated and we only comment it. Like the first Schinzel theorem it gives a criterion to recognize reducible polynomials. The

criterion is the disjunction of four conditions. The first two are similar to those of the preceding theorem. The third one looks like the second one with a list of pairs, {7, 2}, {7, 3}, {8, 1}, {9, 1}, {14, 2}, {21, 7} and formulae

$$A = u^{\nu-\mu} A_{\nu,\mu}(v,w), \quad B = u^{\nu} B_{\nu,\mu}(v,w),$$

but here (v,w) is a point on an elliptic curve $E_{\nu,\mu}(\mathbb{K})$. All curves but one (namely $E_{7,2}$, whose equation is $w^2 = v^3 + 16\,v^2 + 64\,v + 80$) are given by their canonical form of Weierstrass. For example, the curve $E_{7,3}$ is defined by the equation $w^2 = v^3 - 675\,v + 13662$. In the end the fourth condition uses all pairs of integers and formulae

$$A = u^{\nu-\mu} A_0, \quad B = u^{\nu} B_0,$$

where (A_0, B_0) lies in a finite set $F_{\nu,\mu}(\mathbb{K})$. However the proof does not furnish a way to compute $F_{\nu,\mu}(\mathbb{K})$ for it is based on Falting's theorem which is ineffective.

For the rational number field $\mathbb{K} = \mathbb{Q}$ one knows twenty exceptional trinomials which are reducible but do not satisfy any one of the first three conditions. Among those is the polynomial

$$X^8 + 3\,X^3 - 1 = (X^3 + X - 1)(X^5 - X^3 + X^2 + X + 1).$$

One may expect that for each algebraic field $\mathbb{K}$ there is only a finite number of exceptions. That conjecture is very difficult to prove; it suffices to think of Fermat theorem in which there is only one simple curve and one parameter. Here the curves are complicated and there are several parameters.

If the conjecture is right there exists constant $C_1(\mathbb{K})$ such that a reducible trinomial $X^n + A\,X^m + B$ satisfies the first condition (it has a proper factor of degree less than or equal to 2) or the condition $n_1 \leq C_1(\mathbb{K})$. For $\mathbb{K} = \mathbb{Q}$ it needs $C_1(\mathbb{K}) \geq 17$ as shows the example

$$X^{17} + 103X + 56 = (X^3 - X^2 + X + 1)(X^{14} + X^{13} - 2\,X^{11} - \cdots + 9\,X^2 + 47\,X + 56).$$

As another consequence of the conjecture there exists constant $C_2(\mathbb{K})$ such that every polynomial has an irreducible factor with at most $C_2(\mathbb{K})$ nonzero coefficients. Breman asserts the constant has value greater than or equal to 8. Moreover Chauder and Schinzel gave an explicit example of this.

Bibliography

[1] Coppersmith (D.) and Davenport (J.). – Polynomials whose powers are sparse. *Acta Arithmetica*, vol. LVIII, n° 1, 1991.

[2] Schinzel (A.). – *Selected topics on polynomials.* – Ann Arbor, 1982.

[3] Schinzel (A.). – On the number of terms of a power of a polynomial. *Acta Arithmetica*, vol. 49, 1987, pp. 55–70.

[4] Schinzel (A.). – On reducible trinomials. *Dissertationes Mathematicae*, 1993. – To appear.

[5] Zannier (U.). – Ritt's second theorem in arbitrary characteristic. *Journal für die reine und angewandte Mathematik*, 1993. – To appear.

Zeros of polynomials with 0,1 coefficients

A. M. Odlyzko
AT & T Bell Laboratories
Murray Hill, New Jersey 07974

September 3, 1992

[summary by Xavier Gourdon]

Abstract

Zeros of polynomials with 0,1 coefficients exhibit many interesting features, including fractal appearance. We describe here several of their properties [4].

1. Introduction

Zeros of polynomials with random coefficients occur in many scientific and engineering problems. There is an extensive literature on the subject. A general overview of the subject and references can be found in [2].

We consider here zeros of polynomials with 0,1 coefficients. Let P the set of polynomials with $0, 1$ coefficients and with constant term 1 (we exclude polynomials with constant term 0, as their zeros, other than 0, are those of polynomials of lower degree with coefficients 0,1). We define W as the set of all the complex zeros of the polynomials in P.

We are interested in results concerning locations of zeros and topological property of $\overline{W}$, the closure of W. The results are illustrated by pictures of zeros.

2. Bounds and locations

Figure 1 shows the zeros of polynomials in P of degree 14. Also drawn are the curves

$$C_1 = \left\{ z : \ |z| \le 1, \frac{|z|}{1-|z|} = \left| \frac{2-z}{1-z} \right| \right\} \quad \text{and} \quad C_2 = \left\{ z : \ |z| \le 1, \frac{|z|}{|z|-1} = \left| \frac{2-z}{1-z} \right| \right\}.$$

The curve C_1 is mapped to C_2 by $z \mapsto 1/z$. This mapping takes W into itself, since if $z \in W$, and z is a root of $f(z) \in P$ and $\deg(f) = d$, then $1/z$ is a root of $z^d f(1/z) \in P$. All $z \in W$ are enclosed strictly between C_1 and C_2. From this it follows that for all $z \in W$, we have

$$\frac{1}{\phi} < |z| < \phi, \quad \text{where} \quad \phi = \frac{1+\sqrt{5}}{2}.$$

Real zeros. On Figure 1, one can see that many zeros belong to the line segment $[-\phi, -\phi^{-1}]$. In fact, all this line segment in contained in $\overline{W}$. However, $-\phi \notin W$ and $-\phi^{-1} \notin W$. We do not have $]-\phi, -\phi^{-1}[\subset W$ since W is countable (because P is countable).

Further there is a constant $\delta > 0$ such that if $z \in W$, $|z| \le \phi^{-1} + \delta$, then z is purely real. Machine computations, using Rouché's theorem, show that a value of $\delta = 0.7 - \phi^{-1} \simeq 0.082$ is allowable.

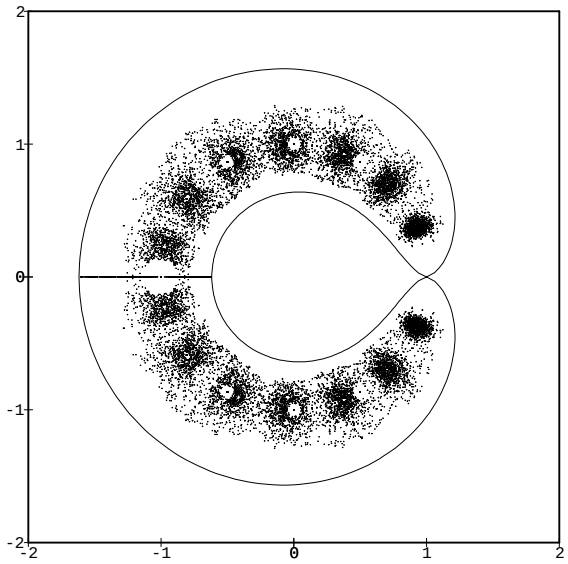


FIGURE 1. Zeros of 0,1 polynomials of degree 14 with constant term 1.

Multiple zeros. A polynomial $f(z) \in P$ can have multiple zeros. If $\zeta \neq 1$ is a d-th root of unity, then ζ is a zero of $g(z) = \sum_{j=0}^{d-1} z^j$, and therefore a zero of $g(z^k)$ for any k such that $d \mid k-1$. Hence it is a zero of multiplicity 2 for $g(z)g(z^k)$, a polynomial in P. Higher multiplicities can be obtained by iterating this procedure. On the other hand, we do not know whether any $z \in W$ that is not a root of unity can be a multiple root of any $f(z) \in P$.

"Holes" in Figure 1. Figure 1 shows several large "holes", which contain either just one or no zeros. These holes are usually centred at algebraic integers α of low degree and small height (i.e., algebraic integers α that satisfy polynomial equations with small integral coefficients). The most prominent of the holes are at the roots of unity, such as -1 and i. As one computes zeros of polynomials in P of increasing degrees, the large holes in Figure 1 fill up. However, there are other holes, such as visible in Figures 2–3, that are free of zeros even when the degree increases.

3. Topological properties of $\overline{W}$

First note that the set $\overline{W} \cap \{z : |z| < 1\}$ is the set of zeros of power series with 0,1 coefficients and with constant term 1. Since $z^{-1} \in W$ for all $z \in W$, it is sufficient to study $z \in W$, $|z| \leq 1$, and it is more convenient to deal with the above power series.

A neighbourhood of the unit circle. The set $\overline{W}$ has the following property. There exists an open neighbourhood of $\{z : |z| = 1, z \neq 1\}$ which is contained in $\overline{W}$. As for the behaviour of $\overline{W}$ near 1, the points of W near 1 come in tangent to the x-axis.

Connectedness. The set $\overline{W}$ is connected (that is, we cannot write $\overline{W} \subset U \cup V$ where U and V are open and disjoint). Furthermore, one can prove that $\overline{W}$ is path connected (that is, any two points in $\overline{W}$ can be linked with a continuous curve in $\overline{W}$). In contrast to this result, the Mandelbrot set is only known to be connected, although it is conjectured to be path connected [1, 3]. The methods used to prove the connectedness of $\overline{W}$ are simpler than those used to study the connectedness of the Mandelbrot set.

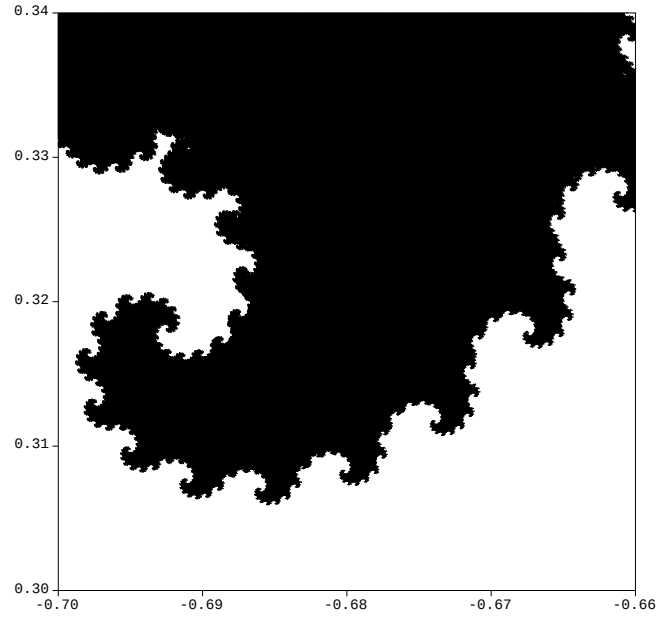


FIGURE 2. Section of $\overline{W}$, the set of zeros of power series with 0,1 coefficients with black denoting $z \in \overline{W}$.

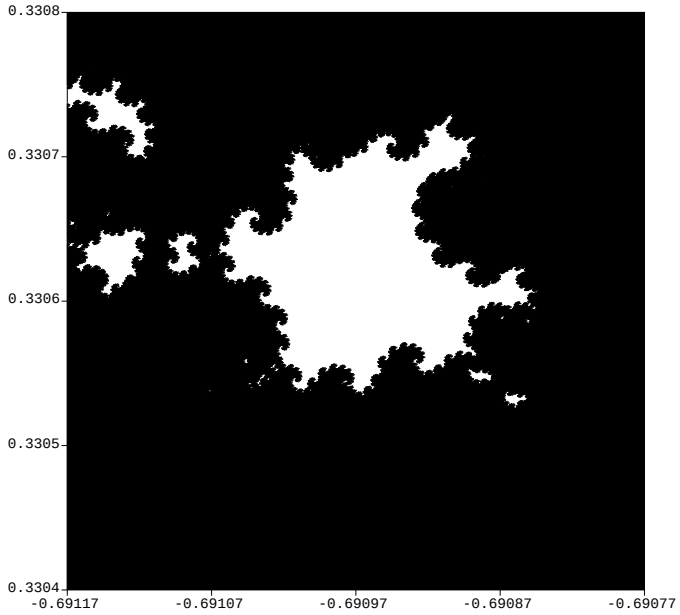


FIGURE 3. Section of $\overline{W}$. This is enlargement of a section of Figure 2 showing some of the holes contained in $\overline{W}$.

4. Computation of the graph of $\overline{W}$

Initial computations of zeros by A. M. Odlyzko and B. Poonen were performed in double precision on a Cray X-MP. In fact, these computations can be performed in a reasonable time on a workstation, using the same algorithms as Odlyzko and Poonen used.

Figure 1 was computed in MAPLE from a large set of random polynomial $f(z) \in P$ of degree 14.

Figures 2–3 were prepared differently. A program (in C) was written that checked whether a given w with $|w| < 1$ is in $\overline{W}$. It is easily shown that

$$\left| \sum_{k=0}^{+\infty} a_k \omega^k \right| \leq B = \frac{\max(1, |1+\omega|)}{1 - |\omega|^2},$$

where the a_k are any $0, 1$ coefficients. The program was to test all sets of 0,1 coefficients $a_1, \ldots, a_{120}$ to see whether they could be the initial segment of coefficient of a power series f with 0,1 coefficients, for which $f(\omega) = 0$. The procedure was to use a binary tree (with nodes $a_1, a_2, \ldots$) to check recursively whether

$$\left| 1 + \sum_{j=1}^{d} a_j \omega^j \right| > |\omega|^{d+1} B$$

at any stage. If this condition is satisfied, then ω is not a zero of any power series with 0,1 coefficients with initial coefficients $a_1, \ldots, a_d$, and the subtree of that node does not have to be explored. If all the leaves of our tree are discarded by this procedure, we have a rigourous proof that $\omega \notin \overline{W}$. Instead, the program assumed that $\omega \in \overline{W}$.

These computations were performed in double precision, and one can prove that they are close to reality. Figures 2–3 were produced by testing every point in a 2000×2000 grid. One can see fractal appearance on these figures. The small holes in Figure 2 are not due to technical imperfections, they really exist. Figure 3 is an enlargement of a section of Figure 2 showing such a hole. This proves that $\overline{W}$ is not simply connected.

Bibliography

[1] Barnsley (M.). – *Fractals Everywhere.* – Academic Press, 1988.
[2] Bharucha-Reid (A. T.) and Sambandham (M.). – *Random Polynomials.* – Academic Press, 1986.
[3] Devaney (R. L.). – *An Introduction to Chaotic Dynamical Systems.* – Addison-Wesley, 1989, 2nd edition.
[4] Odlyzko (A. M.) and Poonen (B.). – Zeros of polynomials with 0,1 coefficients. – Preprint.

Dessins d'enfants de Grothendieck, aspect calculatoire

J.-M. Couveignes
DMI, École Normale Supérieure, Paris

25 Janvier 1993

[résumé par Philippe Le Chenadec]

Résumé

Un dessin d'enfant est un graphe connexe fini plongé dans une surface lisse compacte orientée et sans bord, de sorte que les composantes connexes de son complémentaire soient homéomorphes au disque unité. Nous rassemblons ici quelques résultats théoriques sur ces dessins d'enfants. Essentiellement, nous exposons l'équivalence de Grothendieck entre classes d'homéomorphismes de dessins et classes d'isomorphismes de revêtements algébriques de la sphère de Riemann, ramifiés au-dessus de trois points, ainsi que l'existence, via cette correspondance, d'une action du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur les dessins.

1. Dessins d'enfants et groupe cartographique

Soit X un complexe cellulaire fini dont l'espace topologique sous-jacent est une surface topologique compacte connexe orientable et sans bord. Nous désignerons par X_i le squelette i-dimensionnel du complexe X, union des cellules de dimension inférieure ou égale à i. D'après un résultat connu [14, thm 19, §3.6] ou [6, thm 2.5, Ch. 3], le 1-squelette X_1 est connexe, X l'étant lui-même. On constate aisément que $X_1 \setminus X_0$ vide équivaut à X_0 et X_2 singletons, ainsi qu'à l'existence d'une 2-cellule f dont le bord $\partial f = \overline{f} \setminus f$ se réduit à un point. Lorsqu'il en est ainsi, X est homéomorphe à la sphère. La valence $v(a)$ d'une 0-cellule a est le nombre de composantes connexes de $(X_1 \setminus X_0) \cap W$, W un voisinage suffisamment petit de cette 0-cellule.

En vertu de phénomènes de ramification (cf. infra), un dessin peut contenir des arêtes qui ne possèdent pas de sommet à l'une de leurs extrémités, de telles arêtes étant alors repliées sur elles-mêmes. En conséquence, un dessin d'enfant est une paire (X, V), X comme ci-dessus mais non trivial, V un sous-ensemble de X_0 tel que les 0-cellules de $X_0 \setminus V$ aient une valence égale à 1 et, si $u \in X_0 \setminus V$ et e désigne l'unique 1-cellule telle que $u \in \overline{e}$, alors $v \in V$ où v est la 0-cellule définie par $\partial e = \{u, v\}$. Les éléments de V (resp. les composantes connexes de $X_1 \setminus V$, de $X_2 \setminus X_1$) sont appelés sommets du dessin (resp. arêtes, faces). Comme exemples, notons qu'il existe deux dessins associés au complexe possédant une seule face et une seule arête (donc deux 0-cellules distinctes). Leur support est la sphère. Celui qui ne possède qu'un seul sommet est appelé le dessin universel, et est noté $\perp$.

Supposons choisis un point par arête et un par face du dessin (X, V), appelés leur centre, de sorte que, si une 1-cellule e possède une 0-cellule u dans son bord ∂e qui ne soit pas dans V, le point choisi soit u, point de pliage de l'arête. Soit $\phi : (\mathrm{B}_2, \mathrm{S}_1) \to (\overline{f}, \partial f)$ un homéomorphisme relatif, f une face du dessin, B_2 la boule unité et S_1 la sphère unité de $\mathbb{R}^2$. On peut supposer sans perte de généralité que ϕ n'est pas constante sur les intervalles de S_1. Le centre de f détermine par ϕ un point unique c de l'intérieur de B_2. Pour un centre d'arête ou sommet a de ∂f, $\phi^{-1}(a)$ est un ensemble fini dont le nombre d'éléments est égal à la valence $v(a)$ de a dans f, c'est-à-dire au nombre de composantes connexes de $f \cap (W \setminus (X_1 \cap W))$, pour un voisinage suffisamment petit W de a, tel que $W \cap X_0 \subset \{a\}$. De plus, les points de S_1 envoyés par ϕ sur les sommets alternent avec les points de S_1 envoyés sur le centre d'une arête, comme on s'en rend compte aisément par des raisonnements topologiques élémentaires.

Considérons maintenant une triangulation de la boule B_2 par le point c et les points de S_1 juste définis, de sorte que B_2 ainsi triangulée soit homéomorphe à un polygone régulier muni de sa triangulation usuelle par son centre. Le sous-complexe $\overline{f}$ de X se trouve ainsi muni d'une nouvelle structure de complexe cellulaire, image par ϕ de la triangulation de B_2, qui est régulière mais non simpliciale en général, voir $\perp$ par exemple. On appelle triangle du dessin (X, V) une 2-cellule de cette nouvelle structure. La surface de (X, V) étant supposée orientée par l'intermédiaire d'un modèle différentiable de cette surface muni d'une orientation, chaque triangle possède une orientation induite. Un triangle sera dit positif si l'ordre de ses 0-cellules frontières, lues dans le sens direct, est centre de face – sommet – centre d'arête ; il sera dit négatif dans le cas contraire. Les triangles positifs et négatifs alternent alors autour des centres de faces et d'arêtes, et autour des sommets, lorsque chaque face du dessin a été ainsi divisée. Notons qu'un triangle est entièrement déterminé par son sommet frontière, son arête frontière et son signe. Désormais nous supposerons sauf exception qu'un dessin est muni d'une orientation. Lorsque cela ne soulève pas d'ambiguïté, un dessin (X, V) sera noté simplement X, et l'ensemble de ses triangles $T(X)$ (resp. $T^+(X)$, $T^-(X)$ pour les triangles positifs et négatifs). Cet ensemble $T(X)$ est toujours non-vide.

Un morphisme $\phi : (X, V) \to (X', V')$ entre deux dessins d'enfants (X, V) et (X', V') est une application cellulaire surjective qui est simultanément un revêtement ramifié, telle que $\phi(V) = V'$, $\phi(X_0 \setminus V) = X'_0 \setminus V'$, $\phi(X_1 \setminus X_0) = X'_1 \setminus X'_0$ et $\phi(X_2 \setminus X_1) = X'_2 \setminus X'_1$. On montre alors aisément que l'image d'une cellule est une cellule de même dimension, et qu'il existe, dans chaque cellule, au plus un point de branchement ou de ramification. Les dessins et leurs morphismes (resp. les dessins orientés et les morphismes respectant l'orientation) forment une catégorie $\mathcal{D}$ (resp. $\mathcal{D}^+$) dans laquelle le dessin universel $\perp$ est un objet terminal. Ceci motive la terminologie utilisée par Grothendieck de cartes pour les dessins, le réseau routier correspondant au 1-squelette, et les régions aux composantes connexes de son complémentaire, qui sont simplement connexes donc uniformisables simplement.

Il existe une caractérisation des classes d'isomorphie de dessins par l'intermédiaire du groupe cartographique C_2, défini par la présentation $\langle \sigma_0, \sigma_1, \sigma_2; \sigma_i^2 = (\sigma_0\sigma_2)^2 = 1, i = 0, 1, 2\rangle$. Le groupe cartographique orienté C_2^+ est son sous-groupe engendré par $\rho_0 = \sigma_2\sigma_1$, $\rho_1 = \sigma_0\sigma_2$ et $\rho_2 = \sigma_1\sigma_0$. C'est aussi le sous-groupe de C_2 dont les éléments sont représentés par les mots de longueur paire sur les lettres σ_0, σ_1 et σ_2. Il est donc d'indice 2, et un ensemble de relations de définition est donné par les équations $\rho_1^2 = \rho_2\rho_1\rho_0 = 1$. Le groupe C_2 agit sur $T(X)$, X un dessin, comme suit. Le générateur σ_0 échange deux triangles dont les côtés de type centre de face–centre d'arête sont identiques (resp. σ_1 et côtés centre de face–sommet identiques, σ_2 et côtés centre d'arête–sommet identiques). Les éléments de $C_2 \setminus C_2^+$ définissent donc des bijections entre $T^+(X)$ et $T^-(X)$, et le groupe orienté C_2^+ agit sur chacun de ces deux ensembles. Par suite, le générateur ρ_2 agit sur $T^+(X)$ comme la rotation en sens direct autour du centre d'un modèle-polygone régulier d'une face (resp. ρ_1 autour du centre d'une arête, ρ_0 autour d'un sommet), et C_2^+ agit sur les triangles négatifs par les rotations en sens inverse. La connexité de X_1 implique la transitivité de l'action de C_2 sur $T(X)$ (resp. de C_2^+ sur $T^\pm(X)$). La bijection de $T(X)$ induite par $\sigma \in C_2$ est un morphisme de σ-conjugaison : pour tout triangle T et $\tau \in C_2$, on a $\sigma(\tau T) = ({}^\sigma\tau)\sigma(T)$. A un isomorphisme C_2-équivariant près, l'ensemble $T(X)$ muni de son action est indépendant du choix des points-centres. Cette action est décrite dans la figure 1, où $\sigma_i(T) = T'_i$, $\rho_i(T) = T_i$, $i = 0, 1, 2$, et où $\circ$ dénote le centre d'une face, $\times$ celui d'une arête et $\bullet$ un sommet.

Appelons $\mathcal{E}$ la catégorie des C_2^+-ensembles finis transitifs avec comme morphismes les applications équivariantes. Un morphisme $\phi : X \to X'$ de dessins induit une application $T(\phi) : T(X) \to T(X')$ (resp. $T^\pm(\phi) : T^\pm(X) \to T^\pm(X')$ lorsque ϕ conserve l'orientation), par exemple via la caractérisation d'un triangle T par le triplet (v, e, ϵ), v son sommet, e son arête et ϵ son signe, l'image de T par $T(\phi)$ est alors le triangle $(\phi(v), \phi(e), \epsilon_\phi\epsilon)$, où $\epsilon_\phi = \pm 1$ selon que ϕ respecte ou change l'orientation des dessins. On vérifie aisément que $T^+ : \mathcal{D}^+ \to \mathcal{E}$ est un foncteur covariant. Si $\phi, \psi : X \to X'$ sont deux morphismes de dessins, ils sont dits homotopes ssi il existe une application continue $F : X \times [0, 1] \to X'$ telle que $F(\_, t) : X \to X'$, $0 \leq t \leq 1$, soit un morphisme, $F(\_, 0) = \phi$ et $F(\_, 1) = \psi$. Par des résultats standards d'homotopie différentielle, si ϕ et ψ sont homotopes, elles respectent l'orientation toutes deux ou la changent toutes deux et $T(\phi) = T(\psi)$. Soit alors $\mathcal{G}$ la catégorie dont les objets sont les dessins et les morphismes les classes d'homotopie de morphismes de dessins (resp $\mathcal{G}^+$ pour la catégorie conservatrice). Le foncteur T^+ passe au quotient et définit une équivalence de catégories $T^+ : \mathcal{G}^+ \to \mathcal{E}$ (l'action de C_2^+ sur $T^+(X)$ détermine celle de C_2 sur $T(X)$) :

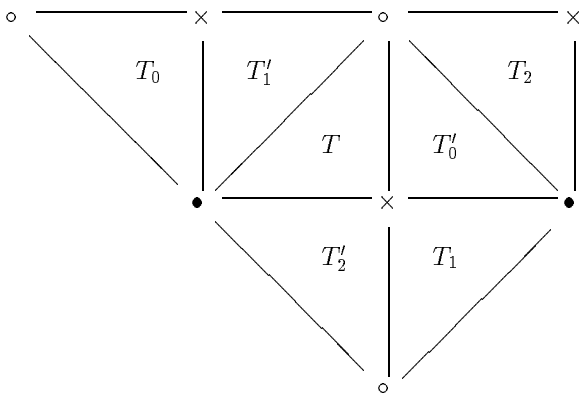


FIGURE 1. Action du groupe cartographique sur les triangles.

THÉORÈME 1 (MALGOIRE-VOISIN). *Il y a bijection entre classes d'isomorphie de dessins d'enfants et classes de C_2-conjugaison de sous-groupes d'indice fini du groupe cartographique orienté C_2^+.*

PREUVE. Soit X un dessin et B le stabilisateur d'un triangle. Par l'action de C_2^+ sur $T^{\pm}(X)$, nous avons $[\mathrm{C}_2^+ : B] = |T^{\pm}(X)| < +\infty$, et la classe de conjugaison de B dans C_2, par la transitivité de l'action de C_2 sur $T(X)$, ne dépend pas du triangle choisi, mais seulement de X. Deux dessins isomorphes définissent une même classe de conjugaison de stabilisateurs.

Réciproquement, soit B un sous-groupe de C_2^+ d'indice fini. Soit $H = \mathrm{C}_2/B$ l'ensemble des classes à gauche de B dans C_2, ensemble sur lequel C_2 agit par multiplication à gauche, ce qui induit une action de C_2^+ sur C_2^+/B et sur $H \setminus (\mathrm{C}_2^+/B)$. Construisons un 2-complexe X comme suit. Soit $X' = \bigsqcup_{h\in H} f_h$ le 2-complexe cellulaire union disjointe de 2-complexes f_h homéomorphes au 2-complexe standard Δ_2 de $\mathbb{R}^3$. À chaque sommet de f_h associons un générateur ρ_i de sorte que deux sommets distincts correspondent à deux générateurs distincts. De même, au côté de f_h d'extrémités associées à ρ_i et à ρ_j on associe l'élément σ_k, $k \neq i$, $k \neq j$, bien défini puisque $i \neq j$. Les orbites de H^+ sous l'action des ρ_i sont en bijection avec les orbites de H^- sous ces mêmes éléments par la correspondance :

$$\{\rho_i^n cB \mid n \in \mathbb{Z}\} \mapsto \{\rho_i^n \sigma_k cB \mid n \in \mathbb{Z}\} = \{\rho_i^n \sigma_l cB \mid n \in \mathbb{Z}\},$$

$$\text{où } \{i,k,l\} = \{0,1,2\}, \ \ c \in \mathrm{C}_2^+,$$

comme on le constate avec l'aide des identités :

$$\rho_i\sigma_j = \sigma_j\rho_i^{-1}, \ i \neq j, \ \text{ et } \ \rho_0\sigma_1 = \sigma_2, \ \rho_1\sigma_2 = \sigma_0, \ \rho_2\sigma_0 = \sigma_1.$$

L'espace X est le quotient topologique de X', obtenu en identifiant d'une part deux sommets v et v' de X', lorsqu'ils sont associés tous deux à un même élément ρ_i, et que de plus, si $v \in f_h$, $v' \in f_{h'}$, alors les orbites de h et h' sous ρ_i sont ou égales, ou associées par la correspondance bijective juste définie ; et d'autre part deux côtés $e \subset f_h$, $e' \subset f_{h'}$ tels que tous deux soient associés à σ_i, et que h forme avec h' une σ_i-orbite. Ces conditions impliquent, via la correspondance ci-dessus, que les extrémités de e et e' sont identifiées dans X, on impose alors que e et e' le soient via un homéomorphisme entre e et e' qui respecte ces identifications.

On vérifie que X ainsi défini est naturellement muni d'une structure de 2-complexe cellulaire dont les cellules sont les images de celles de X' sous la projection canonique de X' sur X. Par construction, le complexe X est régulier car X' l'est et les identifications des 0-cellules et des 1-cellules entre elles respectent leurs types σ_i ou ρ_j. De même, chaque 0-cellule de X appartient au bord d'au moins une 2-cellule, et chaque 1-cellule au bord de deux 2-cellules exactement puisque $\sigma_i^2 = 1$, ces 2-cellules peuvent d'ailleurs être égales. L'espace X est compact, la relation d'identification étant fermée. Il est connexe, l'action de C_2 sur H étant

transitive. Les 2-cellules de X sont d'autre part en bijection avec H, et donc munies d'une C_2-action. Si une paire de 2-cellules f_1 et f_2 forme une σ_i-orbite, les deux 1-cellules de type σ_j des bords de f_1 et f_2 ont en commun dans leur bord une 0-cellule étiquetée ρ_k, $\{i,j,k\} = \{0,1,2\}$ puisque $\rho_k^\epsilon(f_1) = \sigma_j(f_2)$, en vertu de l'identité $\rho_k^\epsilon = \sigma_j\sigma_i$, $\epsilon = \pm 1$. Les σ_i-orbites montrent que l'espace X est une pseudo-variété, et la remarque précédente montre qu'il est en fait une surface topologique, puisque les 2-cellules contenant une 0-cellule de type ρ_k dans leur bord forment une suite f, $\sigma_i f$, $\sigma_j\sigma_i f$, $\sigma_i\sigma_j\sigma_i f$, $\sigma_j\sigma_i\sigma_j\sigma_i f, \ldots$, deux éléments consécutifs ayant une 1-cellule de type σ_i ou σ_j en commun, ρ_k étant la 0-cellule commune à tous les bords de ces 1-cellules. Cette surface est sans bord, par la remarque précédente sur les 1-cellules qui bordent deux 2-cellules.

De même, supposons donnés des homéomorphismes $g_h : \Delta_2 \to f_h$, $h \in H$, ce qui est licite puisque X est régulier. On suppose ces homéomorphismes deux à deux compatibles :

$$g_h^{-1}|f_h \cap f_{h'} = g_{h'}^{-1}|f_h \cap f_{h'}, \quad h, h' \in H.$$

La relation dans X, définie par $a \sim b$ ssi $a \in f_h$, $b \in f'_{h'}$, $h, h' \in \mathrm{C}_2^+$ ou $h, h' \in \mathrm{C}_2 \setminus \mathrm{C}_2^+$, et $b = g_{h'} \circ g_h^{-1}(a)$, définit un espace quotient $X/\sim$ qui n'est autre que la sphère S_2 par examen des σ_i-orbites et des voisinages des points de $X/\sim$. Ceci fait de X un revêtement de S_2 ramifié au-dessus de trois points au plus, dont le lieu de branchement est inclus dans X_0, le 0-squelette de X pour sa structure cellulaire originelle. La surface X est donc orientable.

On reconstitue un dessin associé à X par les définitions suivantes : une face est la réunion des 2-cellules de X ayant une 0-cellule de type ρ_2 fixée dans leur fermeture, une arête est la réunion des 0- et 1-cellules ayant dans leur fermeture une 0-cellule de type ρ_1 fixée, sauf s'il n'existe qu'une seule telle 1-cellule, auquel cas l'arête est définie comme étant cette 1-cellule augmentée de la 0-cellule fixée ; enfin les 0-cellules du dessin sont les 0-cellules de type ρ_0, plus les 0-cellules de type ρ_1 et de valence 1 comme ci-dessus. On définit bien entendu V comme étant l'ensemble des 0-cellules de type ρ_0. Le couple (X, V), X muni de cette nouvelle structure de complexe cellulaire, est alors un dessin d'enfant.

Le stabilisateur du triangle du dessin associé à la classe à gauche B de H est évidemment B, lorsque $T(X)$ est défini via la structure cellulaire originelle de X. Réciproquement, soit X un dessin, T_0 un triangle de X, B_0 son stabilisateur. Le complexe cellulaire X dont les 2-cellules sont les triangles étant régulier, on peut se donner des homéomorphismes cellulaires $h_T : \Delta_2 \to \overline{T}$, $T \in T(X)$, Δ_2 le 2-simplexe standard de $\mathbb{R}^3$, qu'on suppose compatibles : $h_T^{-1}|T \cap T' = h_{T'}^{-1}|T \cap T'$. De même pour le dessin X_0 défini par B_0 : on suppose donnés des homéomorphismes cellulaires compatibles $g_u : \Delta_2 \to \overline{U}$, $U \in T(X_0)$, tels que de plus les types associés aux cellules de Δ_2 par h_T et g_U coïncident. Alors $\phi : X \to X_0$, défini par $\phi(x) = (g_{cB_0} \circ h_{cT_0}^{-1})(x)$, pour $c \in \mathrm{C}_2$ tel que $x \in \overline{cT_0}$, est un homéomorphisme de X sur X_0, qui est un isomorphisme de dessins.

Pour conclure, observons que pour tout $\sigma \in \mathrm{C}_2$, l'application

$$cB \mapsto (\sigma c \sigma^{-1})(\sigma B \sigma^{-1})$$

entre $H = \mathrm{C}_2/B$ et $H' = \mathrm{C}_2/\sigma B\sigma^{-1}$ est un isomorphisme de σ-conjugaison entre ces deux C_2-ensembles, l'homéomorphisme qu'il induit à homéomorphisme des 2-cellules près entre X' et $X'' = \bigsqcup_{h' \in H'} f_{h'}$ passe donc aux quotients, la construction du quotient de X'' étant effectuée à l'aide de générateurs de C_2, σ-conjugués des générateurs originaux σ_i. □

2. Ramification et rationalité

Soit X une courbe algébrique projective et lisse définie sur $\mathbb{C}$. Montrons que X est isomorphe à une courbe définie sur $\overline{\mathbb{Q}}$ ssi il existe une fonction rationnelle $f \in \mathbb{C}(X)$, non constante, dont toutes les valeurs critiques sont dans $\overline{\mathbb{Q}}$. Dans un sens c'est élémentaire : si X est définie sur $\overline{\mathbb{Q}}$, elle est isomorphe à la complétée X' d'une courbe affine lisse Y de $\mathbb{C}^n$, définie sur $\overline{\mathbb{Q}}$, $n \geq 1$. L'idéal $\mathcal{I}$ de Y, idéal premier de $\mathbb{C}[x_1, \ldots, x_n]$ de hauteur $n-1$, possède donc une base à coefficients dans $\overline{\mathbb{Q}}$. Soient g_i, $i = 1, \ldots, n-1$, les éléments d'une telle base. Soit également f une fonction rationnelle non constante de $\overline{\mathbb{Q}}(Y)$, représentée par une fraction rationnelle p/q, $p, q \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$, $p, q \notin \mathcal{I}$. L'équation $df = 0$ est équivalente aux n équations $q\partial p/\partial x_i - p\partial q/\partial x_i = 0$ et l'un au moins de ces derniers polynômes n'appartient pas à $\mathcal{I}$, sinon les fonctions

rationnelles $q^2\partial(p/q)/\partial x_i$, nulles sur Y, impliquerait $\partial(p/q)/\partial x_i$ nulle également sur Y, puisque $q \notin \mathcal{I}$ et $\mathcal{I}$ premier, et donc f constante, contrairement aux hypothèses. Les solutions du système $df = 0$, $g_i = 0$ sont alors en nombre fini et rationnelles sur $\overline{\mathbb{Q}}$, et le même raisonnement, appliqué aux homogénéisés, montre qu'un éventuel point à l'infini de Y, critique pour f, est aussi $\overline{\mathbb{Q}}$-rationnel. Les valeurs critiques correspondantes de f sont également dans $\overline{\mathbb{Q}}$. Ainsi la fonction f fournit, via l'isomorphisme entre X et X', une fonction rationnelle de X à valeurs critiques dans $\overline{\mathbb{Q}}$, puisqu'une transformation birationnelle entre courbes complètes est partout définie et birégulière [11, prop. 1, Ch. 7]. Un lemme désormais classique de Belyi [1] permet de raffiner ce résultat. Dorénavant, nous noterons $\mathbb{G}$ le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

LEMME 1 (BELYI). *Soit X une courbe lisse projective définie sur $\overline{\mathbb{Q}}$. Il existe dans $\overline{\mathbb{Q}}(X)$ une fonction rationnelle dont toutes les valeurs critiques sont dans $\{0, 1, \infty\}$.*

PREUVE. Soit f non constante dans $\overline{\mathbb{Q}}(X)$. Construisons $h \in \overline{\mathbb{Q}}(X)$ dont toutes les valeurs critiques sont dans $\mathbb{Q}$. Soit S_0 l'ensemble formé des valeurs critiques finies de f et de leurs $\mathbb{G}$-conjuguées. On définit successivement les polynômes $P_i(x) \in \mathbb{Q}[x]$ par $P_0(x) = \prod_{s\in S_0}(x - s)$ et $P_{i+1}(x) = \prod_{s\in S_{i+1}}(x - P_i(s))$, où S_{i+1} désigne l'ensemble des zéros de $P_i'(x)$, lorsque ce dernier polynôme est non identiquement nul. Ces polynômes sont bien à coefficients rationnels puisque $P_i'(s) = 0$ et $P_i(x) \in \mathbb{Q}[x]$ impliquent $(P_i'(s))^\sigma = P_i'(s^\sigma) = 0$, $\sigma \in \mathbb{G}$. De plus on a $\deg(P_{i+1}) < \deg(P_i)$. Il existe donc n tel que $\deg(P_n) = 0$. La fonction rationnelle $h = P_{n-1} \circ P_{n-2} \circ \cdots \circ P_0 \circ f$ de $\overline{\mathbb{Q}}(X)$ a ses valeurs critiques finies dans $\mathbb{Q}$. En effet, si $\phi : U \to V$ et $\psi : V \to W$ sont des morphismes non constants entre courbes, par la considération des points de branchement de $\psi \circ \phi$, on a $C_{\psi\circ\phi} = C_\psi \cup \psi(C_\phi)$, où C_ϕ et C_ψ désignent respectivement l'ensemble de toutes les valeurs critiques de ϕ et ψ. Alors l'égalité :

$$C_h = C_{P_{n-1}} \cup (P_{n-1}(C_{P_{n-2}})) \cup \cdots \cup (P_{n-1} \circ \cdots \circ P_1(C_{P_0})) \cup ((P_{n-1} \circ \cdots \circ P_0(C_f)),$$

l'observation que les zéros de $P_{i+1}(x)$ sont les valeurs critiques de $P_i(x)$ et l'observation analogue pour P_0 et f, impliquent le résultat cherché.

Si h possède au plus trois valeurs critiques, une homographie de $\mathrm{PSL}_2(\overline{\mathbb{Q}})$ fournit la fonction rationnelle souhaitée. Sinon nous pouvons supposer, toujours d'après la 3-transitivité de l'action de $\mathrm{PSL}_2(\overline{\mathbb{Q}})$ sur $\mathbb{P}_1(\mathbb{C})$, les points 0, 1 et ∞ valeurs critiques de h, et, comme h en possède au moins quatre, qu'elle en possède une de la forme $m/(m + n)$, avec m, n entiers positifs. Alors le polynôme :

$$B_{m,n}(x) = \frac{(m+n)^{m+n}}{m^m n^n}(1 - x)^n x^m$$

a $m/(m+n)$ comme point critique, de valeur critique 1, et éventuellement 0,1 comme autres points critiques finis, de valeur critique correspondantes 0. La fonction rationnelle $B_{m,n} \circ h$ est dans $\overline{\mathbb{Q}}(X)$, et ses valeurs critiques sont dans $\mathbb{Q}$, en nombre $k - 1$ où k est le cardinal de l'ensemble des valeurs critiques de h. Réitérer cette opération le cas échéant fournit le morphisme cherché. □

Ainsi toute courbe définie sur $\overline{\mathbb{Q}}$ peut être vue comme un revêtement de la sphère ramifié en 0, 1 et ∞ seulement. La réciproque utilise le résultat algébrique élémentaire suivant : si G est un groupe finiment engendré, le nombre de sous-groupes de G d'indice fini fixé est fini [2, exerc. 5, §5, Ch. 1]. Soit alors X une courbe projective et lisse définie sur $\mathbb{C}$, et qui est via $f : X \to \mathbb{P}_1(\mathbb{C})$ dans $\mathbb{C}(X)$ un revêtement de la sphère non ramifié en dehors de $\{0, 1, \infty\}$. Le revêtement non ramifié induit par f sur $X \setminus f^{-1}(\{0, 1, \infty\})$ est caractérisé par une classe de conjugaison de sous-groupes de $\pi_1(\mathbb{P}(\mathbb{C}) \setminus \{0, 1, \infty\})$, d'indice égal au degré de f, à isomorphisme de revêtements près. Les structures complexes associées étant également isomorphes et déterminant leur prolongement aux points de branchement [5, Satz 8.4, Kap. I], deux revêtements associés à des sous-groupes conjugués de ce π_1 seront isomorphes en tant que courbes algébriques sur $\mathbb{C}$.

Dans la construction qui suit, nous utiliserons librement soit le langage des schémas [7], soit le langage classique des variétés (voir [15], notamment pour les questions de rationalité et d'intersection), le passage de l'un à l'autre étant valide, par suite de l'équivalence de catégories entre schémas intègres séparés de type fini sur un corps algébriquement clos et variétés au sens classique sur ce corps, voir e.g. [8, prop. 4.10, Ch.

2] ou [13, thm 2, §II.3]. Suivant alors le point classique, la fonction f, identifiée à son graphe, est une sous-variété du produit $X \times \mathbb{P}_1(\mathbb{C})$, isomorphe à X puisque f est partout définie et birégulière. Elle est donc lisse, complète, et de même genre g que X.

Considérons alors l'action du groupe $G = \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, comme définie en [15, Ch. VII, §4], action qui conserve le degré et le genre. Par le résultat d'algèbre mentionné plus haut, l'orbite de f est finie modulo $\mathbb{C}$-isomorphie. Le genre étant constant sous l'action de G, d'après la remarque ci-dessus, cet ensemble forme un sous-ensemble fini de $\mathcal{M}_g(\mathbb{C})$, $\mathcal{M}_g(k)$ désignant l'espace des modules des courbes algébriques définies sur k, complètes et lisses de genre g. Le cas $g = 0$ est trivial. Et lorsque $g = 1$, les deux remarques suivantes impliquent la validité des conclusions du raisonnement ci-dessous, effectué pour $g \geq 2$: a) le corps $\mathbb{C}$, via l'invariant modulaire j, paramétrise les classes de courbes elliptiques, a pour compactifié $\mathbb{P}_1(\mathbb{C})$, défini sur $\mathbb{Z}$ et b) la courbe paramétrée par j est définie sur $\overline{\mathbb{Q}}$ ssi $j \in \overline{\mathbb{Q}}$ [9].

D'après les résultats de la théorie des modules, notamment ceux de Mumford [10, 12], il existe un schéma de module grossier M_g, $g \geq 2$, quasi-projectif sur $\mathbb{Z}$, et donc de type fini sur $\mathbb{Z}$. Par définition des schémas de modules grossiers, l'ensemble $\mathcal{M}_g(k)$, pour k algébriquement clos, est en bijection avec $\mathrm{M}_g(k)$, l'ensemble des points de M_g à valeurs dans k, égal par définition à $\mathrm{Hom}(\mathrm{Spec}(k), \mathrm{M}_g)$. L'orbite sous G de f étant finie à $\mathbb{C}$-isomorphisme près, la bijection ci-dessus associe donc à f un sous-ensemble fini de $\mathrm{M}_g(\mathbb{C})$. Or par la prop. 1.3.7, Ch. 0 [7], $\mathrm{M}_g(\mathbb{C})$ est isomorphe à $\mathrm{Hom}_U(U, \mathrm{M}_{g,\mathbb{C}})$, où $U = \mathrm{Spec}(\mathbb{C})$ et $\mathrm{M}_{g,k} = \mathrm{M}_g \times_{\mathbb{Z}} k$, k un corps. De même, $\mathrm{M}_g(\overline{\mathbb{Q}})$ est isomorphe à $\mathrm{Hom}_V(V, \mathrm{M}_{g,\overline{\mathbb{Q}}})$ où $V = \mathrm{Spec}(\overline{\mathbb{Q}})$. Par transitivité du changement de base, $\mathrm{M}_{g,\mathbb{C}} = \mathrm{M}_{g,\mathbb{Q}} \times_{\mathbb{Q}} \mathbb{C}$ et $\mathrm{M}_{g,\overline{\mathbb{Q}}} = \mathrm{M}_{g,\mathbb{Q}} \times_{\mathbb{Q}} \overline{\mathbb{Q}}$. Les deux corps $\mathbb{C}$ et $\overline{\mathbb{Q}}$ étant algébriquement clos, $\mathcal{M}_g(\mathbb{C})$ est donc en bijection avec l'ensemble des points clos de $\mathrm{M}_{g,\mathbb{C}}$, et $\mathcal{M}_g(\overline{\mathbb{Q}})$ avec celui des points clos de $\mathrm{M}_{g,\overline{\mathbb{Q}}}$ (voir par exemple [13, §II.6], les changements de base respectant la propriété d'être de type fini [7, prop. 6.3.4, Ch. 1]). Ainsi l'orbite quotientée de f est associée naturellement à un sous-ensemble algébrique du schéma $\mathrm{M}_{g,\mathbb{C}}$. Cet ensemble est stable sous l'action de G. En conséquence, l'idéal de cet ensemble (dans un ouvert affine le contenant, défini sur $\overline{\mathbb{Q}}$) est défini sur $\mathbb{Q}$, du fait que $\mathbb{C}^G = \mathbb{Q}$ [2, prop. 10, §14, Ch. 5] et [15, lemme 2, Ch. I, §7]. Cet ensemble est défini sur $\overline{\mathbb{Q}}$, ainsi que les points qui le composent puisqu'il est fini et que $\overline{\mathbb{Q}}$ est algébriquement clos [15, cor. 1 du thm 7, Ch. IV, §4]. Il nous reste donc à voir que l'image d'un tel point, par le morphisme $\mathrm{M}_{g,\mathbb{C}} \to \mathrm{M}_{g,\overline{\mathbb{Q}}}$ déduit du changement de base, est un point fermé de $\mathrm{M}_{g,\overline{\mathbb{Q}}}$. Or c'est évident puisque ces deux schémas sont issus de $\mathrm{M}_{g,\mathbb{Q}}$ par changement de base, que $\mathbb{C}$ est fidèlement plat sur $\overline{\mathbb{Q}}$ [3, Ch. 1]. En se plaçant dans un $\overline{\mathbb{Q}}$-ouvert affine $\mathrm{Spec}(R)$ du point considéré. Il y a équivalence de l'exactitude des deux suites :

$$0 \longrightarrow \mathcal{I} \otimes_{\overline{\mathbb{Q}}} \mathbb{C} \longrightarrow R \otimes_{\overline{\mathbb{Q}}} \mathbb{C} \longrightarrow \overline{\mathbb{Q}} \otimes_{\overline{\mathbb{Q}}} \mathbb{C} \longrightarrow 0,$$

$$0 \longrightarrow \mathcal{I} \longrightarrow R \longrightarrow \overline{\mathbb{Q}} \longrightarrow 0,$$

où $\mathcal{I} \otimes_{\overline{\mathbb{Q}}} \mathbb{C}$ est l'idéal maximal dans R du point considéré. Ainsi f est définie sur $\overline{\mathbb{Q}}$, et il en est de même bien entendu de la courbe X. Notons que non seulement la courbe X est définie sur un corps de nombres, mais la fonction rationnelle f elle-même est définie sur un tel corps. Ceci nous sera utile par la suite. Enfin le lemme de Belyi permet d'étendre le raisonnement précédent aux fonctions ramifiées au-dessus d'entiers algébriques en nombre quelconque, du fait que les polynômes et homographies apparaissant dans sa preuve sont à coefficients dans $\overline{\mathbb{Q}}$.

3. La correspondance de Grothendieck

Soit X un dessin d'enfant. Munissons-le d'une triangulation. Identifions le dessin universel $\perp$ avec $\mathbb{P}_1(\mathbb{C})$, de sorte que triangulé, son sommet soit 0, son arête le segment $]0, 1]$, et le centre de sa face soit ∞. L'unique morphisme $X \to \perp$ munit l'espace topologique X d'une structure complexe qui en fait une courbe algébrique, ramifiée au-dessus de $\{0, 1, \infty\}$ exclusivement, telle que tout point de branchement au-dessus de 1 ait un degré au plus égal à 2.

Appelons fonction ou morphisme de Belyi un morphisme f non-constant d'une courbe algébrique C, projective, lisse et définie sur $\mathbb{C}$, dans $\mathbb{P}_1(\mathbb{C})$, non ramifié en dehors de 0, 1 et ∞, et telle que le degré de branchement au-dessus de 1 soit au plus 2 en chaque point. Si ce degré est constamment égal à 2, le

morphisme de Belyi est dit propre. La paire (C, f) est dite de Belyi, propre lorsque f l'est. Deux paires de Belyi (C, f) et (C', f') sont dites isomorphes lorsqu'il existe un $\mathbb{C}$-isomorphisme $g : C \to C'$ tel que $f = f' \circ g$.

Nous venons de voir qu'à un dessin il est possible d'associer une paire de Belyi. Réciproquement, soit (C, f) une paire de Belyi. Posons $V = f^{-1}(0)$, $X_1 = f^{-1}([0,1])$, $X_0 = V \cup \{x \mid f(x) = 1,\ e_f(x) = 1\}$, $e_f(x)$ étant l'indice de branchement de f en x, et enfin X_2 est l'espace topologique sous-jacent à C. Munissons X_2 d'une structure de 2-complexe cellulaire X telle que son i-squelette soit X_i, $i = 0, 1, 2$. Soient N et S les hémisphères ouvertes nord et sud de $\mathbb{P}_1(\mathbb{C})$, i.e. les ensembles $\{z \mid \Im(z) > 0\}$ et $\{z \mid \Im(z) < 0\}$ respectivement lorsque $\mathbb{P}_1(\mathbb{C})$ est identifié au compactifié de $\mathbb{C}$. Les ouverts N et S sont les triangles positif et négatif associés à la triangulation naturelle de $\perp$ identifié à $\mathbb{P}_1(\mathbb{C})$. Définissons $T^+(X)$ comme étant l'ensemble des composantes connexes de $f^{-1}(N)$ (resp. $T^-(X)$ et $f^{-1}(S)$). Enfin définissons les centres d'arêtes et de faces comme éléments de $f^{-1}(1)$ et de $f^{-1}(\infty)$ respectivement. Les propriétés usuelles de la partition d'un revêtement ramifié en feuillets montrent que (X, V) est un dessin d'enfant, triangulé par $T(X) = T^+(X) \cup T^-(X)$.

Précisons toutefois ce dernier point en des données combinatoires. Soit donc C un revêtement connexe de degré fini de la sphère de Riemann, non ramifié en dehors de 0, 1 et ∞. La surface C est orientable et sans bord. Si nous supposons, comme dans le cas des dessins, que le degré de branchement au-dessus de 1 est au plus 2, le groupe de monodromie agissant sur la fibre du revêtement en un point de $\mathbb{P}_1(\mathbb{C}) \setminus \{0, 1, \infty\}$ est un groupe de permutation transitif de degré d égal à celui du revêtement, engendré par trois permutations σ_0, σ_1 et σ_∞ telles que $\sigma_0\sigma_1\sigma_\infty = \sigma_1^2 = 1$, qui sont les images des générateurs de $\pi_1(\mathbb{P}_1(\mathbb{C}) \setminus \{0, 1, \infty\})$ correspondant à des lacets tournant en sens direct autour de 0, 1 et ∞.

Montrons que, réciproquement, la donnée d'un tel groupe de permutations définit un revêtement de $\mathbb{P}_1(\mathbb{C})$. Soient donc deux permutations σ_0 et σ_1 du groupe symétrique de degré d, telles que $\langle \sigma_0, \sigma_1 \rangle$ soit transitif dans son action naturelle, c.-à-d. sur les entiers compris entre 1 et d. A chaque orbite c du sous-groupe $\langle \sigma_\infty \rangle$, $\sigma_\infty = (\sigma_0\sigma_1)^{-1}$ associons un polygone régulier P à n côtés, $n \geq 1$, n la taille de cette orbite. En les énumérant dans le sens direct, les côtés de P sont étiquetés successivement par les paires $(a, \sigma_1(a))$, puis $(\sigma_\infty(a), \sigma_1\sigma_\infty(a)), \ldots$, où a est un élément de l'orbite c. Les polygones sont recollés entre eux par l'identification de deux côtés étiquetés (a, b) et (b, a) respectivement, ces deux côtés étant juxtaposés en sens inverse l'un de l'autre. Ainsi, si ces paires sont distinctes, deux arêtes distinctes sont identifiées, sinon une arête est repliée sur elle-même.

Chaque arête étant identifiée avec exactement une autre, puisque $\sigma_1^2 = 1$, l'espace ainsi obtenu est une surface compacte C', connexe puisque les polygones le sont et que l'action est transitive, orientable car les polygones le sont et le choix du sens d'identification des arêtes respecte l'orientabilité. La partition de C' en intérieurs des polygones, intérieurs des côtés et sommets forme un dessin (C', V), V ensemble des images des sommets. Deux dessins (C, V) et (C', V') possédant même degré d et des fibres génériques munies d'actions de monodromie isomorphes, correspondent à des sous-groupes conjugués du groupe fondamental de $\mathbb{P}_1(\mathbb{C}) \setminus \{0, 1, \infty\}$ [2, thm 1, §I.5] et définissent donc des revêtements de $\mathbb{P}_1(\mathbb{C})$ isomorphes par le théorème de classification des revêtements. Il est alors immédiat que les dessins eux-mêmes sont isomorphes.

THÉORÈME 2 (CORRESPONDANCE DE GROTHENDIECK). *Il y a bijection entre classes d'isomorphisme de dessins et classes d'isomorphisme de paires de Belyi. De plus, chaque paire de Belyi est isomorphe à une paire définie sur $\overline{\mathbb{Q}}$, et donc chaque dessin est réalisable comme revêtement de la sphère de Riemann, défini sur un corps de nombres.*

PREUVE. A chaque classe de dessins est associée bijectivement une classe de conjugaison de sous-groupes d'indice fini de C_2^+ par le premier théorème. Ce groupe C_2^+ est isomorphe à $\pi_1(\mathbb{P}_1(\mathbb{C}) \setminus \{0, 1, \infty\})$ quotienté par le sous-groupe normal N engendré par l_1^2, l_1 un lacet en sens direct autour de 1, via l'isomorphisme défini par $\rho_0 \mapsto l_0$, $\rho_1 \mapsto l_1$, $\rho_2 \mapsto l_\infty$, où l_0 et l_∞ sont des lacets autour de 0 et ∞ en sens direct (modulo homotopie). La classe de conjugaison de sous-groupes de C_2^+ est alors bijectivement associée à une classe de conjugaison de sous-groupes d'indice fini de ce π_1, contenant chacun N. A son tour, cette classe est bijectivement associée à une classe d'isomorphie de revêtements finis de $\mathbb{P}_1(\mathbb{C})$, ramifiés uniquement au-dessus de 0,1,∞, d'indice au plus égal à deux au-dessus de 1, d'après l'étude précédant le théorème. La classe de la paire de Belyi correspondant à cette classe de revêtements est donc bijectivement associée à la classe de dessins. La seconde

partie du théorème est une paraphrase de la caractérisation des courbes définies sur $\overline{\mathbb{Q}}$ via le lemme de Belyi. □

Notons que si f est un isomorphisme entre les paires de Belyi (C,h) et (C',h'), et si les dessins associés à ces deux paires sont respectivement (X,V) et (X',V'), nous avons $f(X_1)=X'_1$, $f(V)=V'$ et $f(F)=F'$, où F, F' désignent les ensembles des centres d'arêtes de X et X'.

4. Action galoisienne sur les dessins

La propriété d'être définie sur $\overline{\mathbb{Q}}$ permet d'introduire une action galoisienne sur les morphismes de Belyi, et donc sur les dessins par la correspondance de Grothendieck. Soit en effet une paire (C,f) définie sur $\overline{\mathbb{Q}}$, de dessin associé X. Si $\sigma\in\mathbb{G}$, la paire (C^σ,f^σ) est de Belyi. En effet, la courbe C^σ est de même genre que C, f^σ a même degré que f (prop. 27, F-IV$_7$). De plus les points de branchement de f et f^σ se correspondent par σ, et comme $0,1,\infty$ sont $\mathbb{Q}$-rationnels, f^σ est ramifiée uniquement au-dessus de ces trois points. Si P est un point de branchement de f, P^σ l'est pour f^σ et de plus les indices de branchement $e_f(P)$ et $e_{f^\sigma}(P^\sigma)$ sont égaux. Pour voir ce dernier point, il suffit d'appliquer l'équivalence [15, Ch. IX, §4] :

$$f^*(Q)=\sum_i e_f(P_i)P_i \qquad\Longleftrightarrow\qquad (f^\sigma)^*(Q^\sigma)=\sum_i e_{f^\sigma}(P_i^\sigma)P_i^\sigma,$$

aux diviseurs égaux aux points de ramification, et à leurs images réciproques par f, égales à la somme des points de branchement au-dessus du point de ramification considéré, comptés avec leur multiplicité, tous ces diviseurs étant $\overline{\mathbb{Q}}$-rationnels. L'action de Galois préserve les points de branchement et leur degré. La paire (C^σ,f^σ) est donc de Belyi, et est propre ssi (C,f) l'est. Elle détermine un dessin qui est indépendant du choix de la paire (C,f) représentant X. En effet, si (C',f') est une autre paire de Belyi définie sur $\overline{\mathbb{Q}}$, et associée à X, il existe, par la correspondance de Grothendieck, un isomorphisme $g:C\to C'$ tel que $f=f'\circ g$. D'après le cor. 1 à la prop. 8, Ch. 5, [2], il existe, pour tout $\sigma\in\mathbb{G}$, au moins un automorphisme τ de $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ prolongeant σ. On a alors $f^\sigma=f'^\sigma\circ g^\tau$, et g^τ est un isomorphisme entre C^σ et C'^σ. Les deux dessins ainsi définis sont donc isomorphes, ce qui conduit à définir un dessin abstrait comme étant une classe d'isomorphisme de dessins d'enfants. Il existe alors une action galoisienne sur les dessins abstraits.

C'est bien une action de groupe, puisqu'elle est définie en dernière analyse par l'action naturelle de $\mathbb{G}$. Cette action conserve le genre, le degré ainsi que les listes de valence des sommets et des centres de face et d'arêtes du dessin. C'est sur cette propriété que se fonde la recherche de fractions rationnelles de Belyi en genre 0 développée par L. Schneps et J.-M. Couveignes. Pour X un tel dessin, on note $\mathbb{G}(X)$ le sous-groupe de stabilité de X : $\mathbb{G}(X)=\{\sigma\in\mathbb{G}\mid X^\sigma=X\}$. De même, si (C,f) est une paire de Belyi associée à X, que nous supposerons désormais définie sur un corps de nombres, on note $\mathbb{G}(C,f)$, ou plus simplement $\mathbb{G}(f)$, le sous-groupe de $\mathbb{G}(X)$ formé des éléments σ tels que $f^\sigma=f$. Le groupe $\mathbb{G}(X)$ est ouvert, puisque défini à partir d'une extension de degré fini de $\mathbb{Q}$ (un corps de définition d'une paire de Belyi pour X). Il est fermé puisque c'est le stabilisateur d'un point de l'ensemble des dessins abstraits, muni de la topologie discrète, où opère le groupe compact $\mathbb{G}$ [4, prop. 2 et 4, §4, Ch. 3]. On peut donc définir le corps du dessin comme étant le corps des invariants de $\mathbb{G}(X)$ (pour f, on retrouve la définition usuelle). Le corps de définition de X est donc de degré fini égal à $[\mathbb{G}:\mathbb{G}(X)]$ [2, cor. 5 au thm 4, §10, Ch. 5], et est inclus dans le corps de définition de f, puisque $\mathbb{G}(f)\subset\mathbb{G}(X)$. Naturellement, les orbites d'un dessin et d'une paire de Belyi sous $\mathbb{G}$ sont finies.

L'indice de minimalité d'un dessin est le nombre minimal de $\mathbb{G}$-conjugués de f, lorsque f parcourt l'ensemble des morphismes de Belyi associés à X. C'est aussi le minimum des degrés des extensions (corps de f)/(corps de X), par la correspondance de Galois.

Rappelons le formulaire suivant, où, pour un dessin (X,V), v est le cardinal de X_0, e le nombre d'arêtes, f celui de faces, g le genre de X :

$$v-e+f=2-2g \qquad \text{(formule d'Euler-Poincaré).}$$

Nous avons défini la valence $v(a)$ d'un sommet ou centre d'arête a. On peut de même définir la valence du centre d'une face comme étant le nombre d'arêtes bordant cette face. La valence d'une arête ou d'une face

est celle de son centre. Soit d le degré du dessin X :

$$d = \sum_{\text{sommets } s} v(s) = \sum_{\text{arêtes } e} v(e) = \sum_{\text{faces } f} v(f).$$

Enfin, si les $e_{i,j}$, $i = 0, 1, \infty$, $j = 1, \ldots, k_i$, désignent les longueurs des orbites dans $\pi_1(\mathbb{P}_1(\mathbb{C}) \setminus \{0, 1, \infty\})/B$ de l_0, l_1, l_∞ respectivement, où B est le stabilisateur d'un triangle de X, et si n_i, $i = 0, 1, 2$, est le nombre de cycles de σ_i agissant comme permutation de $T(X)$, la formule de Riemann-Hurwitz donne :

$$2g - 2 = -2d + \sum_{i \in \{0,1,\infty\}} \sum_j (e_{i,j} - 1) = d - n_0 - n_1 - n_2.$$

Si le dessin X est propre, on a $l = 2e$.

La méthode proposée par L. Schneps et développée par J.-M. Couveignes pour rechercher une fonction de Belyi d'un dessin propre est la suivante. Les points du dessin au-dessus d'un même point de ramification et de même indice de branchement sont regroupés comme ensemble des zéros, qu'on impose simples, d'un polynôme, à coefficients dans $\overline{\mathbb{Q}}$ puisque ces points sont $\overline{\mathbb{Q}}$-rationnels. Soient S_i, A_i et F_i les polynômes dont les racines sont respectivement les sommets, les centres d'arêtes et les centres de faces de valence égale à i ($A_i = 1$ si $i \neq 2$ lorsque le dessin est propre). La fraction rationnelle f recherchée vérifie :

$$f(z) = a \prod_i S_i(z)^i / \prod_j F_j(z)^j, \quad \text{et}$$

$$f(z) - 1 = b \prod_k A_k(z)^k / \prod_j F_j(z)^j, \quad a, b \in \overline{\mathbb{Q}}.$$

Il en résulte une identité de la forme :

$$a \prod_i S_i^i - \prod_j F_j^j = b \prod_k A_k^k.$$

Cette dernière fournit des équations algébriques entre a, b et les coefficients des polynômes S_i, A_k et F_j, qu'une spécialisation adéquate basée sur la 3-transitivité de PSL_2 transforme en un système à nombre fini de solutions, nécessairement dans $\overline{\mathbb{Q}}$. On trouvera dans leurs articles à paraître (resp. *Dessins d'enfants on the Riemann sphere* et *Calcul et rationalité de fonctions de Belyi en genre 0*) de nombreux exemples, des résultats relatifs aux indices de minimalité, à la fidélité de l'action de $\mathbb{G}$ sur les dessins, aux fonctions de Belyi des arbres, qu'on peut supposer polynômiales, et enfin aux automorphismes des dessins.

Le présent résumé n'est qu'une reformulation des préliminaires de ces deux articles, abâtardie par les laborieux démêlés de son auteur qui tient à remercier Marc Hindry et Jean-Marc Couveignes de leurs remarques et commentaires, ainsi que Philippe Flajolet et Bruno Salvy dont l'insistance a permis la rédaction de ce résumé.

Bibliographie

[1] Belyi (G. V.). – On Galois extensions of the maximal cyclotomic field. *Izvestiya Akademii Nauk SSSR*, vol. 43, n° 2, 1979, pp. 269–276.
[2] Bourbaki (N.). – *Algèbre*. – Masson, 1981.
[3] Bourbaki (N.). – *Algèbre commutative*. – Masson, 1985.
[4] Bourbaki (N.). – *Topologie générale*. – Masson, 1990.
[5] Forster (O.). – *Riemannsche Flächen*. – Springer-Verlag, 1977.
[6] Godbillon (C.). – *Éléments de Topologie Algébrique*. – Hermann, 1971.
[7] Grothendieck (A.) et Dieudonné (J.). – *Éléments de Géométrie Algébrique*. – Springer-Verlag, 1971.
[8] Hartshorne (R.). – *Algebraic Geometry*. – Springer-Verlag, 1987.
[9] Lang (S.). – *Elliptic Functions*. – Springer-Verlag, 1987.
[10] Mumford (D.). – The structure of the moduli spaces of curves and Abelian varieties. *In : Actes CIM*. pp. 457–465. – Gauthier-Villars, 1971.

[11] Mumford (D.). – *Algebraic Geometry I: Complex Projective Varieties.* – Springer-Verlag, 1981.
[12] Mumford (D.). – *Geometric Invariant Theory.* – Springer-Verlag, 1982.
[13] Mumford (D.). – *The red book of varieties and schemes.* – Springer-Verlag, 1988.
[14] Spanier (E. H.). – *Algebraic Topology.* – McGraw-Hill, 1966.
[15] Weil (A.). – *Foundations of Algebraic Geometry.* – AMS, 1967.

Cartographie physique globale du Génome humain

Jean-Jacques Codani *Bruno Lacroix*
INRIA Rocquencourt et CEPH/Généton

16 Novembre 1992

Résumé

Le séquençage direct de grandes régions d'ADN n'est pas à l'heure actuelle la manière la plus efficace de collecter ses informations structurales (coût élevé, outils d'interprétation peu performants, ...). Il est donc nécessaire, pour cibler le séquençage, de disposer d'une "carte" de plus faible résolution : la *carte physique*. Cette approche permet, en particulier, une accélération considérable de la localisation et l'isolement des gènes impliqués dans les maladies héréditaires. Il s'agit de construire un ordre d'intervalles (un intervalle étant un fragment d'ADN cloné), sachant que l'on ne dispose, pour chaque intervalle que d'informations parcellaires et entachées d'erreur.

Nous développons ici cette problématique, et détaillons les aspects théoriques, algorithmiques et informatiques (exploitation du parallélisme intrinsèque) de l'approche utilisée par Généton. À ce jour, 60% du génome est couvert par 1200 groupes de clones chevauchant (aussi appellés *contigs*) totalisant 10000 clones. Nous évoquons enfin les problèmes qui subsistent, parmi lesquels l'ordonnancement des contigs, l'intégration d'informations très différentes et la modélisation des caractéristiques expérimentales.

Géométrie fractale : état de l'art en France

Jacques Levy Vehel
INRIA Rocquencourt

16 Novembre 1992

Résumé

Cette conférence présentera à un niveau élémentaire les principes de base et les progrès récents en Géométrie Fractale, en insistant sur les applications dans divers domaines :
1. Sciences physiques : turbulence, percolation, propagation des ondes, phénomènes de croissance non linéaire, milieux poreux, astronomie.
2. Sciences de l'ingénieur : traitement du signal, analyse d'image.
3. Domaines divers comme l'économie ou l'urbanisme.

Contents