RANDOM MAPPING STATISTICS

Philippe Flajolet
INRIA Rocquencourt,
F–78150 Le Chesnay (France)

Andrew M. Odlyzko
AT&T Bell Laboratories,
Murray Hill, NJ 07974 (USA)

Abstract. Random mappings from a finite set into itself are either a heuristic or an exact model for a variety of applications in random number generation, computational number theory, cryptography, and the analysis of algorithms at large. This paper introduces a general framework in which the analysis of about twenty characteristic parameters of random mappings is carried out: These parameters are studied systematically through the use of generating functions and singularity analysis. In particular, an open problem of Knuth is solved, namely that of finding the expected diameter of a random mapping. The same approach is applicable to a larger class of discrete combinatorial models and possibilities of automated analysis using symbolic manipulation systems ("computer algebra") are also briefly discussed.

1 Introduction

Random maps occur in many problems of discrete probability. Consider for instance the following assertions:

1. Throw n balls into m urns at random. Then, a proportion of about $e^{-n/m}$ of the urns will usually be empty. [Hashing].

2. A room contains 23 persons. It is a good idea (the odds are 50.7% in your favour!) to bet that two persons in the room have the same birthdate. [Birthday paradox].

3. You buy chocolate bars that contain coupons and there are n different possible coupons. Expect to buy (and possibly eat!) about $n \log n$ chocolate bars in order to obtain a full collection. [Coupon collector problem].

4. When using a middle–square random number generator (or some other "randomly" designed random number generator) operating with ℓ digits, the generator is likely to cycle after about $2^{\ell/2}$ steps. ["Random" random number generators].

5. Pollard's integer factorization algorithm is likely to find a factor of a composite integer n within $\approx n^{1/4}$ steps. [Pollard's rho–method].

6. There are n spies that attend a cryptography conference and leave their hats at the cloakroom. When the lecture is over, each spy picks up a hat at random. Then, there is a probability close to e^{-1} that nobody has his hat on his head. [Derangement problem].

These assertions are all classical. A moment's reflection shows that they convey some information on (random) functions from a finite set to a finite set. We thus let $\mathcal{F}_n^{<m>}$ denote the collection of all functions from a finite n–set domain to a finite m-set range, and use $\mathcal{F}_n \equiv \mathcal{F}_n^{<n>}$ to denote the special case where $m = n$, in which situation we merely consider an arbitrary function of a finite set into itself.

Situations where we deal with $\mathcal{F}_n^{<m>}$ are commonly known as *occupancy problems* in discrete probability theory. Models where we consider random elements of $\mathcal{F}_n$ are known as *random mappings* models.

Assertions 1 and 2 are typical of statistical properties of random elements of $\mathcal{F}_n^{<m>}$, i.e., occupancy problems. Assertion 1 is typical of a whole range of problems that present themselves when analyzing the expected performance of hashing algorithms [22]. Assertion 2 is the classical "birthday paradox" and it owes its celebrity to the rather counterintuitive low value of 23. Assertion 3 constitutes the classical "coupon collector problem". It is slightly more complicated than the earlier ones, since now m is itself a random variable in the process. However, if we look at the probability that a fixed number m of bars suffice for a full collection, it reduces to a standard statistical problem over $\mathcal{F}_n^{<m>}$.

Assertion 4 brings us closer to the subject of this paper, since it deals with the iteration structure of a finite set into itself. It is an assertion concerning $\mathcal{F}_n^{<m>}$ with $m = n = 2^\ell$. What it says in essence is that a random *mapping* $f \in \mathcal{F}_n$ will tend to "cycle" after about $\sqrt{n}$ steps. As is quite well known, this fact, combined with an idea of Floyd for testing random number generators, gave rise to Pollard's rho–method [33] for integer factoring (cf. Assertion 5). This eventually led to the factorization of the eighth Fermat number $F_8 = 2^{2^8} + 1$, see [3].

The last assertion, number 6, is related to random permutations which form a special subset of $\mathcal{F}_n$.

The model of random functions —where every function from $\mathcal{F}_n^{<m>}$ or $\mathcal{F}_n$ is taken equally likely— may be either "exact" (# 1,2,3,6) or "heuristic" in which case (# 4,5) we postulate, on the basis of simulations, that properties of a special class of functions (e.g. quadratic function models) should be asymptotically the same as properties of the class of *all* functions[1].

Our purpose here is to describe a unified framework for analyzing a number of statistical[2] properties of random mappings. A probabilistic problem to be analyzed is first specified symbolically in terms of a collection of suitable combinatorial constructions. If this specification succeeds, then combinatorial theory guarantees that *generating functions* for parameters of interest can be found. We then recover *asymptotic* information from these generating functions using *complex analysis*, and more precisely, using the local behaviour of generating functions around their singularities.

This approach is effective in analyzing a large number of "decomposable" parameters of random mappings. With it, we are able to derive in a uniform manner a number of results otherwise obtained by a variety of probabilistic or combinatorial arguments. We also demonstrate the effectiveness of our approach by solving an open problem of Knuth [23], namely that of estimating the expected diameter of random mappings.

Note. We refer to Knuth's book [23] for background information on random number generators. Random mappings are the subject of a vast collection of works; Mutafčiev's survey [26] cites 113 references! For general presentations, we direct the reader to the classic paper of Harris [19], the papers by Arney and Bender [1], and Stepanov [44]. In this area, the contribution of the "Russian school" which uses essentially probabilistic methods, as shown by Kolchin's book *Random Mappings* [24], is notable.

For completeness, we mention several recent papers not referenced in [24], namely [4, 7, 11, 20, 21, 30, 32]. In addition, there is now a growing literature on random mapping patterns, and we refer to [27] for a comprehensive list of references on this subject.

This paper is an (extended!) abstract. In particular, statements of Section 4 regarding extremal statistics should be taken as preliminary announcements of results: Several of the proofs there (Theorems 7,8) are extremely delicate and, at the time of this writing, have not appeared in full detail. The reader interested in quantitative estimates on random mappings rather than methodology can proceed directly to the self contained statements of Theorems 2–8.

---

[1] In the case of Pollard's algorithms and iteration of quadratic functions modulo integers, a notable advance is due to Bach [2] who proved recently that—in *initial* stages— quadratic functions behave asymptotically like random functions. Bach's result ultimately relies on the Weil–Deligne theorem establishing the truth of the "Riemann hypothesis" for zeta functions of algebraic curves!

[2] The term "statistics" is to be understood in the sense of discrete probability.

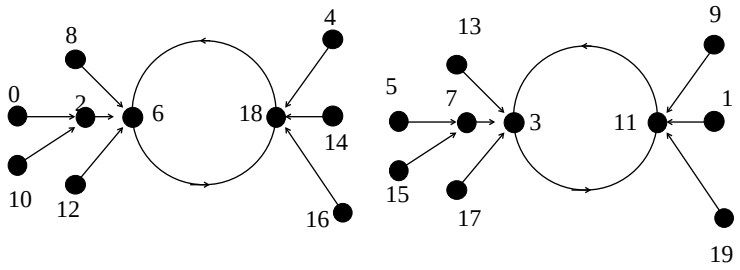

Figure 1. The functional graph associated to the map $\varphi(x) = x^2 + 2 \pmod{20}$. The functional graph comprises two connected components each containing a cycle of length 2. The function $x^2 + 2 \pmod{n}$ is one of a restricted set of polynomial functions whose iteration structure can be precisely described. For general polynomials, essentially, the only known approach is heuristic where one postulates that a polynomial behaves like a random mapping. (See however [2] for one of the very few rigorous results in this domain.)

2 Methods

Any element of $\mathcal{F}_n^{<m>}$ can be viewed as a word over an m–ary alphabet of length m. Thus, there are m^n mappings from an n–set into an m–set. Specializing this observation, we find that the cardinality of $\mathcal{F}_n \equiv \mathcal{F}_n^{<n>}$ is n^n. We are going to rederive this trivial result by means of generating functions. If $\{f_n\}_{n\geq 0}$ is a sequence of numbers, then its (exponential) *generating function* (GF) is defined to be

$$f(z) = \sum_{n\geq 0} f_n \frac{z^n}{n!}. \tag{1}$$

Proceeding in such a simple case as the enumeration of $\mathcal{F}_n$ via generating functions may seem a complicated detour. However, it has the advantage of illustrating, without unnecessary complications, a complete chain in the approach we propose to follow for appreciably harder problems. In this way, we shall be able to give a unified presentation of a number of problems otherwise treated by a variety of *ad hoc* methods.

As is well known, there are two components in the use of generating functions.

A. First, it is classical that a number of *combinatorial constructions* translate directly into generating function equations. Thus, by properly specifying a counting problem by means of these constructions, we are able to derive mechanically a collection of generating function equations that —in principle, at least— solve our problem exactly.

B. Second, the *singularities* of generating functions (now treated as analytic objects) condense most of the *asymptotic* information needed to recover their coefficients.

We refer to [18, 43] for background knowledge related to combinatorial analysis (Part A). General references for asymptotic methods can be found in [6, 29] and our approach follows closely our paper [13].

Our treatment of random mappings is based not on the direct representation of mappings by sequences of choices but instead on their decomposition as *functional graphs*.

Let φ be an element of $\mathcal{F}_n$. Consider the directed graph whose nodes are the elements $[1..n]$ and whose edges are the ordered pairs $\langle x, \varphi(x)\rangle$, for all $x \in [1..n]$. If we start from any u_0 and keep iterating φ, i.e., we consider the sequence $u_1 = \varphi(u_0), u_2 = \varphi(u_1) \ldots$, we are going to find, before n iterations, a value u_j equal to one of $u_0, u_1, \ldots, u_{j-1}$. In graphical terms, starting from any u_0, the iteration structure of φ is described by a simple path that connects to a cycle. The length of the path (measured by the number of edges) is called the *tail length* of u_0 and is denoted by $\lambda(u_0)$. The length of the cycle (measured by the number of edges or nodes) is called the *cycle length* of u_0 and is denoted by $\mu(u_0)$. We also call *rho-length* of u_0 the quantity $\rho(u_0) = \lambda(u_0) + \mu(u_0)$ which is the length of the non repeating trajectory of the point u_0.

If we now consider all possible starting points u_0, paths exhibit confluence and form into trees; these trees, grafted on cycles, form components; finally, a collection of (connected) components forms a functional graph (see Fig. 1).

2.1 Combinatorial Enumerations

Looking at Figure 1, a computer scientist could be tempted to give a description of functional graphs of the following form

```
type    FunGraph   = set(Component);
        Component  = cycle(Tree);
        Tree       = Node * set(Tree);
        Node       = Latom(1).  %Comment: atom of size 1 (labelled)
```

In other words a functional graph is a *set* of connected components; a component is a *cycle* of trees; a tree is recursively defined by appending a node to a *set* of trees; a node is a basic atomic object (of size 1), and labelled by an integer.

Let us adopt here the convention that if $\mathcal{C}$ is a class of combinatorial structures, then C_n (or c_n) denotes the number of elements in the class which have size n —i.e., n nodes. As seen already, we let

$$C(z) = \sum_{n \geq 0} C_n \frac{z^n}{n!}$$

denote the corresponding (exponential) generating function. Thus, we use the same letters or groups of letters to denote structures ($\mathcal{C}$), counting sequences (C_n or c_n) and generating functions ($C(z)$ or $c(z)$).

Recent formalization of the process of combinatorial counting (see e.g., [18]) offers the possibility of translating directly specifications of the type above into generating function equations. Here, they provide for the collection of equations:

$$\begin{aligned} \mathit{FunGraph}(z) &= \exp(\mathit{Component}(z)); \\ \mathit{Component} &= \log(1 - \mathit{Tree}(z))^{-1}; \\ \mathit{Tree}(z) &= \mathit{Node}(z) \times \exp(\mathit{Tree}(z)); \\ \mathit{Node}(z) &= z. \end{aligned} \tag{2}$$

Comparison between the formal specification and the collection of equations reveals that we have used the translation mechanism

$$\begin{aligned} \texttt{set} &\mapsto \exp(.) \\ \texttt{cycle} &\mapsto \log(1 - (.))^{-1} \\ * &\mapsto \times \text{ (ordinary product)} \end{aligned} \tag{3}$$

This mechanism (3) is quite powerful and of course completely general [17]. We will not attempt here to redo the whole theory that underlies such derivations. Let us just indicate that if $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are three classes of labelled structures related by $\mathcal{F} = \mathcal{G} * \mathcal{H}$, then the corresponding counting sequences satisfy

$$f_n = \sum_{k=0}^{n} \binom{n}{k} g_k h_{n-k}.$$

In the equation above, index k selects the size of the $\mathcal{G}$ component (there are g_k possibilities for this component and h_{n-k} possibilities for the $\mathcal{H}$ component), and the binomial coefficient represents the number of ways of distributing labels $[1..n]$ between the the two components. At the GF level, this

relation on coefficients gives $f(z) = g(z) \cdot h(z)$. The rule for sets, for instance, follows from similarly interpreting the expansion

$$\exp(g(z)) = 1 + \frac{1}{1!}(g(z))^1 + \frac{1}{2!}(g(z))^2 + \frac{1}{3!}(g(z))^3 + \cdots$$

as meaning that a set over $\mathcal{G}$ has either 0 or 1 or 2 or 3, etc. elements.

If we abbreviate our generating functions for `FunGraph`, `Component` and `Tree` by $f(z)$, $c(z)$ and $t(z)$, we obtain a more readable form of our basic set of equations (3):

$$\left\{ \begin{array}{rcl} f(z) & = & e^{c(z)} \\ c(z) & = & \log \dfrac{1}{1-t(z)} \\ t(z) & = & z e^{t(z)} \end{array} \right. \tag{4}$$

which expresses generating functions of interest in terms of the implicitly defined tree function $t(z)$.

We briefly digress here to indicate how exact counting results are hidden behind such equations. Function $t(z)$ was considered by Eisenstein and Cayley (amongst others). The Lagrange inversion theorem furnishes the number of trees of size n in the form $t_n = n^{n-1}$ (Cayley's theorem); the same theorem gives the explicit expansion of $f(z) = (1 - t(z))^{-1}$, and one gets as expected $f_n = n^n$.

2.2 Asymptotic Analysis

Probabilistic problems on random mappings are usually more complicated than the plain enumeration results that we have just discussed. Fortunately fairly synthetic methods exist that also permit one to extract directly the asymptotic form of coefficients of a complicated generating function from its singularities.

These methods take their roots in the work of Darboux in the last century [29] and we shall make use here of the approach called *singularity analysis* which originates in [28] and [12], and which is exposed by us in [13].

If we first observe the asymptotic form of coefficients[3] of standard functions

$$[z^n]\frac{1}{1-3z} = 3^n, \tag{5}$$

$$[z^n]\frac{1}{1-4z} = 4^n, \tag{6}$$

$$[z^n]\frac{1}{\sqrt{1-4z}} \sim \frac{4^n}{\sqrt{\pi n}}, \tag{7}$$

we notice from (5,6) that the location of a singularity of the function (at $\frac{1}{3}$ or $\frac{1}{4}$) determines the dominant exponential behaviour of its coefficients (as 3^n or 4^n). Comparison of (6) and (7) reveals further that a singularity of a square–root type yields a subexponential factor also of a square root type, namely $1/\sqrt{\pi n}$.

Our previous observations were based on functions with Taylor coefficients of a simple explicit form. What is of interest in our context, is that it is sufficient to determine local *asymptotic* expansions near a singularity, and such expansions can be "transferred" to coefficients in the same way as before. This is the heart of the method called singularity analysis in [13]. The precise formulation of one of the results of that paper that we shall need is as follows:

Theorem 1 (Singularity Analysis) *Let $f(z)$ be a function analytic in a domain*

$$\mathcal{D} = \{z \mid |z| \le s_1,\ |\mathrm{Arg}(z - s)| > \frac{\pi}{2} - \eta\},$$

[3] We let as usual $[z^n]\, f(z)$ denote the coefficient of z^n in the expansion of $f(z)$

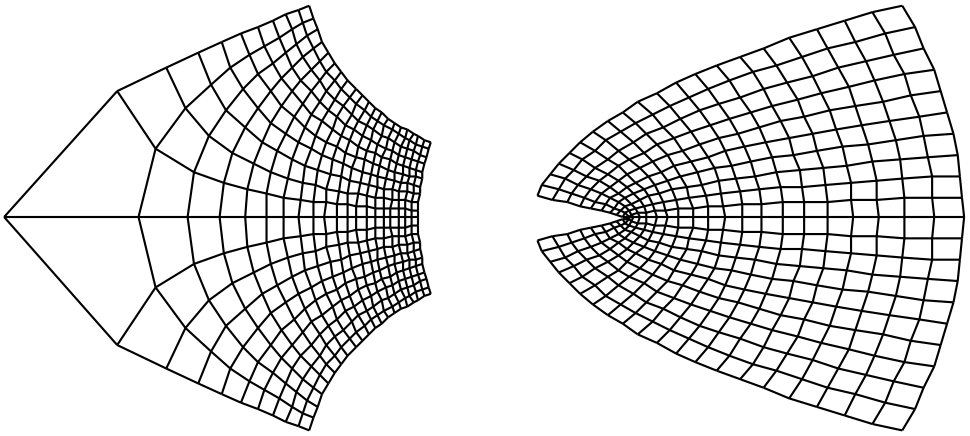

Figure 2. Two conformal representations by

$$f(z) = (1-z)^{1/2} \quad \text{and} \quad g(z) = (1-z)^{9/5}$$

of the unit square $\mathcal{Q} = \{z = x + iy \mid -1 \le x \le +1,\ -1 \le y \le +1\}$. The two different types of singular behaviours at $z = 1$ (left "angles" on the diagrams) are reflected by different growths of coefficients, namely

$$f_n \equiv [z^n]\, f(z) \approx n^{-1-1/2} = n^{-3/2} \quad \text{and} \quad g_n \equiv [z^n]\, g(z) \approx n^{-1-9/5} = n^{-14/5}.$$

---

where s, $s_1 > s$, and η are three positive real numbers. Assume that, with $\sigma(u) = u^\alpha \log^\beta u$ and $\alpha \notin \{0, -1, -2, \ldots\}$, we have

$$f(z) \sim \sigma\Big(\frac{1}{1 - z/s}\Big) \qquad \textit{as } z \to s \textit{ in } \mathcal{D}.$$

Then, the Taylor coefficients of $f(z)$ satisfy

$$[z^n]\, f(z) \sim s^{-n} \frac{\sigma(n)}{n\Gamma(\alpha)}.$$

For instance, using Theorem 1, we find:

$$[z^n] \frac{e^z}{\sqrt{1-4z}} \quad \sim \quad e^{1/4} \frac{4^n}{\sqrt{\pi n}}, \tag{8}$$

$$[z^n] \sqrt{\frac{1}{4z} \log(1-4z)^{-1}}\, \frac{1}{\sqrt{1-4z}} \quad \sim \quad \sqrt{\log n}\, \frac{4^n}{\sqrt{\pi n}}. \tag{9}$$

To obtain the first relation (8), observe that the only singularity of $h(z) = e^z/\sqrt{1-4z}$ is at $z = \frac{1}{4}$, and there $h(z) \sim e^{1/4}/\sqrt{1-4z}$, the asymptotic form of the coefficients being then given by (7). The second relation (9) illustrates the variety of singular behaviours that can be treated by singularity analysis, and here a $\sqrt{\log}$ on the function transfers into a $\sqrt{\log}$ on the coefficients.

Random Mappings. Let us apply this technology to functions involved in the analysis of random mappings. We are then required to determine the singularities of the function $t(z)$ which determines all other functions in (4). We have seen that

$$t(z) = z \exp(t(z)), \tag{10}$$

which defines $t(z)$ *implicitly*.

Proposition 1 *The tree function $t(z)$ defined by (10) is analytic in the domain $\mathcal{D}$ formed by the complex plane slit along $(e^{-1}, +\infty)$. For z tending to e^{-1} in $\mathcal{D}$, $t(z)$ admits the singular expansion,*

$$t(z) = 1 - 2^{1/2}\sqrt{1-ez} - \frac{1}{3}(1-ez) + O((1-ez)^{3/2}). \tag{11}$$

Proof. In fact, implicitly defined functions normally have square root type singularities. Equation (10) is a particular case of the general scheme

$$F(z, y(z)) = 0, \tag{12}$$

which determines $y(z)$ as a function of y. It is known —by the *implicit function theorem*— that, if we have a solution (z_0, y_0) of (12), then we can "continue" it in a neighbourhood of (z_0, y_0) provided that

$$\frac{\partial}{\partial y} F(z, y)\Big|_{\substack{z=z_0 \\ y=y_0}} \neq 0. \tag{13}$$

In other words, if $F(z_0, y_0) = 0$ and $F_y(z_0, y_0) \neq 0$, then a branch of $y(z)$ satisfies $y(z_0) = y_0$, and that branch is regular at z_0. Observe also that locally, the dependency between z and y is expressed by

$$(z - z_0)F_z(z_0, y_0) + (y - y_0)F_y(z_0, y_0) \sim 0 \tag{14}$$

corresponding, as expected, to a locally linear dependence between z and y.

In contrast, if condition (13) ceases to be valid, then the dependence between z and y assumes the form

$$(z - z_0)F_z(z_0, y_0) + \frac{1}{2}(y - y_0)^2 F_{yy}(z_0, y_0) + \text{smaller order terms} = 0. \tag{15}$$

Solving (15) for y, we thus find between z and y a square–root dependency:

$$y \sim y_0 \pm \left(2\frac{F_z(z_0, y_0)}{F_{yy}(z_0, y_0)}\right)^{1/2} \sqrt{z_0 - z}. \tag{16}$$

The brief discussion above shows the paradigm of a singularity analysis of implicitly defined functions [10, Chap V]. The fundamental ideas, in the realm of asymptotic counting, seem to go back to Pólya, and Meir and Moon derived in this way a number of statistical properties of random trees (see e.g., [25]).

In the case of the tree function $t(z)$, we can apply our previous discussion with $F(z, y) = y - ze^y$. The singularities of $t(z)$ are thus amongst numbers z_0 which satisfy the system of two equations in two unknowns,

$$y_0 - z_0 e^{y_0} = 0 \quad \text{and} \quad 1 - z_0 e^{y_0} = 0$$

which provides $y_0 = 1$ and $z_0 = e^{-1}$. The singularity of $t(z)$ that we need to consider is thus $z = e^{-1}$; around this point, the singular expansion (11) is easily derived from the model (15,16). ■

We can now apply singularity analysis to $t(z)$ and the functions that depend on it. By Theorem 1, considering functions $t(z)$, $1/(1 - t(z))$, etc., we find

$$\begin{aligned} \frac{t_n}{n!} &= [z^n]\, t(z) &\sim \frac{e^n}{\sqrt{2\pi n^3}} \\ \frac{c_n}{n!} &= [z^n]\, c(z) &\sim \frac{e^n}{2n} \\ \frac{f_n}{n!} &= [z^n]\, f(z) &\sim \frac{e^n}{\sqrt{2\pi n}}. \end{aligned} \tag{17}$$

The result concerning f_n is expected, and by a complicated detour, we have rediscovered Stirling's formula! In view of Cayley's result that $t_n = n^{n-1}$, the first line is also equivalent to Stirling's formula. However, the asymptotic form of c_n already represents a non obvious asymptotic result.

We shall see in the next section that, once this basis has been established, many asymptotic estimates follow very easily.

3 Additive Parameters

We now follow the approach of Section 2, in order to derive expected values of several parameters of interest in the study of random mappings: First, set up generating function equations; second, analyze locally the singularities of these generating functions. We consider here *additive parameters* whose values can be determined by simple (essentially additive) rules from the structural decomposition of random mappings into functional graphs. It proves convenient to subdivide additive parameters into two classes:

direct parameters (e.g., the number of connected components) represent the number of certain distinguished configurations in mappings;

cumulative parameters (e.g., expected distance to cycle, λ) represent characteristics of mappings as seen from a random point.

Note. Estimates given in this section are essentially classical. The first results on random mappings appear to have been found in the 1950's by a variety of methods including exact enumerations, discrete probability or generating functions. The paper by Harris [19] provides a first extensive approach to problems discussed in this section. Further results are given by Stepanov [44] or Arney and Bender [1], and our presentation follows similar lines.

3.1 Direct Parameters

Let $\xi[\varphi]$ be a parameter of functional graph (or equivalently, mapping) φ, such as the number of connected components. We introduce the quantities

$$\xi_n = \sum_{\varphi \in \mathcal{F}_n} \xi[\varphi] \qquad \text{and} \qquad \Xi(z) = \sum_{n \geq 0} \xi_n \frac{z^n}{n!}, \tag{18}$$

called respectively the total value (over $\mathcal{F}_n$) and the (exponential) generating function associated to parameter ξ. Observe that, with $\mathcal{F} = \cup_n \mathcal{F}_n$, the generating function $\Xi(z)$ has the alternative form

$$\Xi(z) = \sum_{\varphi \in \mathcal{F}} \xi[\varphi] \frac{z^{|\varphi|}}{|\varphi|\,!}, \tag{19}$$

and the expected value of ξ taken over $\mathcal{F}_n$ is nothing but

$$\mathbf{E}\{\xi \mid \mathcal{F}_n\} = \frac{\xi_n}{n^n} = \frac{n!}{n^n}\,[z^n]\,\Xi(z). \tag{20}$$

Thus, once $\Xi(z)$ is known, the expectation analysis of ξ becomes similar to counting problems encountered earlier.

Theorem 2 (Direct Parameters) *The expectations of parameters number of components, number of cyclic points, number of terminal points, number of image points, and number of k-th iterate image points*[4] *in a random mapping of size n have the asymptotic forms, as $n \to \infty$,*

(i)	*# Components*	$\frac{1}{2}\log n$
(ii)	*# Cyclic nodes*	$\sqrt{\pi n/2}$
(iii)	*# Terminal nodes*	$e^{-1}n$
(iv)	*# Image points*	$(1 - e^{-1})\,n$
(v)	*# k-th iterate image points*	$(1 - \tau_k)\,n,$

where the τ_k satisfy the recurrence $\tau_0 = 0$, $\tau_{k+1} = e^{-1+\tau_k}$.

[4]In the sequel, we use the term "point" as synonym for "node". Parameter *number of components* refers to the number of connected components; a point is *cyclic* if it belongs to a cycle; x is *terminal* if it has no preimage ($\varphi^{(-1)}(x) = \emptyset$), and it is an *image point* otherwise. A k–th iterate image point of φ is an image point of the k–th iterate $\varphi^{(k)}$ of φ. Clearly, (iii) and (iv) are equivalent results, and (iv) is a particular case of (v).

Proof. *The algebra of generating functions.* Introduce temporarily bivariate generating functions which for a given parameter ξ are defined as

$$\xi(u,z) = \sum_{\varphi\in\mathcal{F}} u^{\xi[\varphi]} \frac{z^{|\varphi|}}{|\varphi|\,!}. \tag{21}$$

We can view variable u as "*marking*" parameter ξ. The generating function associated to (mean value of) ξ is nothing but

$$\Xi(z) = \frac{\partial}{\partial u}\xi(u,z)\Big|_{u=1}. \tag{22}$$

We shall illustrate the method of proof in cases (i), (ii) and (iii). For the number of components and number of cyclic points, we find respectively as values of $\xi(u,z)$:

$$\begin{array}{rcl} \xi_1(u,z) & = & \exp\left(u\log\frac{1}{1-t(z)}\right) \\ \xi_2(u,z) & = & \exp\left(\log\frac{1}{1-u\,t(z)}\right). \end{array} \tag{23}$$

For the number of terminal nodes (points without preimages), we have instead a two level scheme,

$$\left\{\begin{array}{rcl} \xi_3(u,z) & = & \exp\left(\log\frac{1}{1-t(u,z)}\right) \\ t(u,z) & = & ze^{t(u,z)} + (u-1)z, \end{array}\right. \tag{24}$$

where $t(u,z)$ is the GF for trees with u marking leaves.

Eqs. (23,24) derive from a simple extension of the translation schemes of Section 2.1, introducing only an auxiliary variable u which "marks" configurations of interest.

Applying principle (22) to bivariate GF's (23,24), we find for the corresponding GF's of total values the forms

$$\begin{array}{rcl} \Xi_1(z) & = & \dfrac{1}{1-t(z)}\cdot\log\left(\dfrac{1}{1-t(z)}\right) \\ \Xi_2(z) & = & \dfrac{t(z)}{(1-t(z))^2} \\ \Xi_3(z) & = & \dfrac{z}{(1-t(z))^3}. \end{array} \tag{25}$$

The Analysis of Generating Functions. All GF's above are expressible in terms of the tree function $t(z)$. Singularity analysis as $z\to e^{-1}$ is now immediate from the discussion of Section 2.2. Consider for instance case (i) dealing with the number of components. From Eq. (11), we find *directly* for $\Xi_1(z)$ the singular expansion

$$\Xi_1(z) \sim \frac{1}{2\sqrt{2}}\frac{1}{\sqrt{1-ez}}\log\frac{1}{1-ez}. \tag{26}$$

Analytic continuation beyond the circle of convergence is guaranteed by continuation properties of $t(z)$ (cf. Section 2.2). Thus, we are justified in applying the singularity analysis theorem, and we get

$$[z^n]\,\Xi_1[z] \sim \frac{1}{2\sqrt{2}}\frac{e^n\log n}{\sqrt{\pi n}}, \tag{27}$$

from which part (i) of the theorem follows after normalization by $n!/n^n$.

Finally case (iv) is a direct variant of case (iii). Case (v) follows simply by adapting the argument used for counting terminal nodes, with the help of the GF's of trees of bounded height which we discuss in Section 4. ■

3.2 Cumulative Parameters

We now turn to the study of random mappings in $\mathcal{F}_n$ as seen from a random point (any of the n nodes in the associated functional graph is taken equally likely). Let now $\xi[\varphi, \nu]$ be a parameter of point ν in mapping $\varphi \in \mathcal{F}$. An example of such a parameter is the distance of point ν to its cycle in φ. We introduce the quantities

$$\xi_n = \sum_{\substack{\nu \in \varphi \\ \varphi \in \mathcal{F}_n}} \xi[\varphi, \nu] \qquad \text{and} \qquad \Xi(z) = \sum_{n \geq 0} \xi_n \frac{z^n}{n!}, \tag{28}$$

called again total value of ξ and generating function associated with ξ. The expected value of ξ is now to be taken over the set $[1..n] \times \mathcal{F}_n$ (which has cardinality n^{n+1}) and is

$$\mathbf{E}\{\xi \mid \mathcal{F}_n\} = \frac{\xi_n}{n^{n+1}} = \frac{n!}{n^{n+1}} [z^n] \Xi(z). \tag{29}$$

Theorem 3 (Cumulative Parameter Estimates) *Seen from a random point in a random mapping of $\mathcal{F}_n$, the expectations of parameters*[5] *tail length, cycle length, rho–length, tree size, component size, and predecessors size have the following asymptotic forms:*

(i)	*Tail length* (λ)	$\sqrt{\pi n/8}$
(ii)	*Cycle length* (μ)	$\sqrt{\pi n/8}$
(iii)	*Rho length* $(\rho = \lambda + \mu)$	$\sqrt{\pi n/2}$
(iv)	*Tree size*	$n/3$
(v)	*Component size*	$2n/3.$
(vi)	*Predecessors size*	$\sqrt{\pi n/8}.$

Proof. We shall just give the main steps in the proof in the case of the cycle length parameter (ii).

The algebra of generating functions. The bivariate GF

$$\log \frac{1}{1 - ut(z)}$$

is a GF of connected components, where variable u marks the number of cyclic elements. If we consider

$$z \frac{\partial^2}{\partial z \partial u} \log \frac{1}{1 - ut(z)} \bigg|_{u=1}, \tag{30}$$

then we have a generating function for weighted single–component mappings where a component of size n with k cyclic points has weight $n \cdot k$.

The expression in (30) is equal to $zt'/(1-t)^2$. We then cumulate these weights over all components of random mappings; we can prove generally that this operation corresponds to multiplication of the single–component generating function by $1/(1-t)$. Thus, the GF associated to cycle length is

$$\xi(z) = \frac{zt'(z)}{(1 - t(z))^3}.$$

The analysis of generating functions. From our basic expansion (Proposition 1 and (11)) of $t(z)$ around the singularity $z = e^{-1}$, we find that $t'(z) \sim 2^{-1/2} e (1 - ez)^{-1/2}$. Thus, we have

$$\xi(z) \sim \frac{1}{4}(1 - ez)^{-2} \qquad \text{as } z \to e^{-1},$$

and the result for cycle length follows from Theorem 1.

Analogous methods can be employed to cope with the other five cases. ■

[5] Tail length, cycle length and rho–length are defined at the beginning of Section 2. The *tree size* parameter of node ν means the size of the maximal tree (rooted on a cycle) containing ν; *component size* means the size of the connected component that contains ν. The *predecessors size* of ν is the size of the tree rooted at ν or equivalently the number of iterated preimages of ν.

3.3 Probability Distributions

Though this is not our main purpose here, it is also of interest to consider various characteristics of probability distributions of random mapping parameters. Variance and higher moments can be determined by the same methods as have been employed earlier in this section, though often at a higher computational cost.

Exact probability distributions in random mappings usually have (asymptotic) limit forms, a number of them, like in the case of simpler parameters of Section 3.1 being either Gaussian (with density $e^{-x^2/2}$) or Rayleigh (with density $xe^{-x^2/2}$) in the limit. Let us examine for instance the parameter number of components from Section 3.1; asymptotic normality was first derived by Stepanov [44]. First, the variance estimate is easily derived by differentiation of the function $\xi_1(u,z)$ given in (23) and we find that the standard deviation is $\sim \frac{1}{2}\log n$. In [16], the authors derive Stepanov's result as a particular case of a general law for coefficients of bivariate generating functions of the form $e^{uf(z)}$: The idea, which is applicable to several other parameters, is to extract the coefficient of z^n in the bivariate GF using singularity analysis, and taking u complex in the vicinity of 1, we estimate in this way the characteristic function of the discrete distribution of interest.

The methods we have already introduced can also be used to derive refined counting results like the number of cycles of size r (for a fixed integer r) in a random mapping.

Theorem 4 (r–configurations) *For any fixed integer r, the parameters[6] number of r-nodes, number of predecessor trees of size r, number of cycle trees of size r and number of components of size r, have the following asymptotic mean values:*

$$\begin{array}{lll} (i) & r\text{-nodes:} & ne^{-1}/r! \\ (ii) & r\text{-predecessor trees:} & nt_re^{-r}/r! \\ (iii) & r\text{-cycle trees:} & (\sqrt{\pi n/2})\cdot t_re^{-r}/r! \\ (iv) & r\text{-cycles:} & 1/r \\ (v) & r\text{-components:} & c_re^{-r}/r!, \end{array}$$

where t_r is the number of trees having r nodes, $t_r = r^{r-1}$, and $c_r = r![z^r]c(z)$ is the number of connected mappings of size r.

Proof. Generating functions result from the marking techniques of Section 3.1. For instance, the GF of functional graphs with u marking r–cycles (case (iv)) is

$$f(u,z) = \exp\left(\log\frac{1}{1-t(z)} + (u-1)\frac{t(z)^r}{r}\right).$$

Computation of the coefficients of

$$f_u(1,z) = \frac{1}{(1-t(z))^2}t_r\frac{z^r}{r}$$

by singularity analysis yields the result. ■

We thus see that node degrees in a random mapping are approximately Poisson distributed with parameter 1, a result consistent with our earlier estimate of the number of terminal nodes. The expected number of r–cycles decreases as $1/r$, a property similar to that of random permutations: For instance, a random mapping has on the average 1 fixed point. (Notice however that the implied error terms are not uniform; a random permutation has an average of $\log n$ cycles, while a random mapping has only $\frac{1}{2}\log n$.) Contour integration techniques will usually provide useful estimates when one needs to let r vary as a function of n.

---

[6] An *r–node* is a node of indegree r; a *cycle tree* is a tree rooted on a cycle; a *predecessor tree* is an arbitrary tree in the functional graph.

4 Extremal Statistics

The purpose of this section is to examine extremal statistics on random mappings. We consider questions which, in the perspective of random number generators are like: "*Are there good seed values that lead to long periods?*". In particular for ξ one of the parameters discussed in Section 3.2 —λ, μ, $\rho = \lambda + \mu$, tree size or component size— we consider $\xi^{\max}$ defined by

$$\xi^{\max}[\varphi] = \max_{\nu \in \varphi} \xi[\varphi, \nu]. \tag{31}$$

The generating function approach works fairly well for these parameters. As in Section 3.1, we introduce the generating function associated with an extremal parameter $\xi^{\max}$,

$$\Xi(z) = \sum_{n \geq 0} \xi_n \frac{z^n}{n!}, \qquad \text{where} \quad \xi_n = \sum_{\varphi \in \mathcal{F}_n} \xi^{\max}[\varphi]. \tag{32}$$

Thus $n!\, n^{-n}\, [z^n]\, \Xi(z)$ represents the expectation $\mathbf{E}\{\xi^{\max} | \mathcal{F}_n\}$.

The approach to the determination of Ξ goes through a class of generating functions $f^{[k]}(z)$ where $f^{[k]}(z)$ is a "subseries" of the generating function of all functional graphs defined by

$$f^{[k]}(z) = \sum_{\varphi \in \mathcal{F}_n^{[k]}} \frac{z^{|\varphi|}}{|\varphi|\,!}, \qquad \text{with} \quad \mathcal{F}_n^{[k]} = \{\varphi \in \mathcal{F}_n \mid \xi^{\max}[\varphi] \leq k\}. \tag{33}$$

By a classical formula[7], Ξ is expressed in terms of the $f^{[k]}$ by

$$\Xi(z) = \sum_{k \geq 0} [f(z) - f^{[k]}(z)]. \tag{34}$$

However, the analytic treatment of the $f^{[k]}$ and of the associated sum in (34) becomes appreciably more difficult than in our earlier examples. Corresponding generating functions lead to two sorts of analytic problems:

Truncated series. We need to find uniform estimates for truncated Taylor series near their dominant singularity [μ, tree size, component size].

Singular iteration. We need to estimate uniformly the convergence of iteration schemes near a singularity of the fixed point [λ and ρ].

We distinguish two categories of parameters, longest paths (λ, μ, ρ) and largest components (trees and connected components).

4.1 Longest Paths

The case of the longest cycle in a random functional graph will serve to introduce the subject. The expectation was first determined by Purdom and Williams [35]. These authors use a result of Shepp and Lloyd [41] which is based on deep Tauberian methods and which describes the distribution of the longest cycle in a random permutation. Our derivation proceeds instead directly from generating functions using singularity analysis.

---

[7] The argument is a generating function version of the following well known formula for the mean value of a discrete random variable X:

$$\mathbf{E}\{X\} = \sum_{k \geq 1} k \Pr\{X = k\} = \sum_{k \geq 1} \Pr\{X \geq k\} = \sum_{k \geq 0} [1 - \Pr\{X \leq k\}].$$

Theorem 5 *The expectation of the maximum cycle length in a random mapping of $\mathcal{F}_n$ satisfies*

$$\mathbf{E}\{\mu^{\max}|\mathcal{F}_n\} \sim c_1\sqrt{n},$$

where $c_1 \approx 0.78248$ is given by

$$c_1 = \sqrt{\frac{\pi}{2}} \int_0^\infty [1 - e^{-E_1(v)}]\, dv,$$

and $E_1(v)$ denotes the exponential integral

$$E_1(v) = \int_v^\infty e^{-u} \frac{du}{u}.$$

Proof. (Sketch) Generating functions in this problem involve the *truncated logarithm*,

$$\ell_k(u) = \sum_{j=1}^{k} \frac{u^j}{j}. \tag{35}$$

Let $f^{[k]}(z)$ denote the GF of functional graphs, all of whose cycles have length at most k. Then, we have

$$f^{[k]}(z) = \exp\left(\ell_k(t(z))\right), \tag{36}$$

with $t(z)$ again the tree function.

Introduce the generating function $\Xi(z)$ associated to parameter $\mu^{\max}$ in the sense of (32). This GF is readily determined from (36):

$$\Xi(z) = \sum_{k\geq 0} [\frac{1}{1-t(z)} - f^{[k]}(z)] = \frac{1}{1-t(z)} \sum_{k\geq 1} [1 - e^{-r_k(t(z))}], \tag{37}$$

where $r_k(u)$ is the complement of the truncated logarithm,

$$r_k(u) = \log\frac{1}{1-u} - \ell_{k-1}(u) = \sum_{j\geq k} \frac{u^j}{j}.$$

The problem rests now on the determination of the asymptotic behaviour of $\Xi(z)$ as $z \to e^{-1}$. Set $t(z) = e^{-x}$. By conformal mapping properties of $t(z)$ related to its square–root singularity, when z lies in a suitable indented domain that includes the disk $|z| < e^{-1}$ (a $\mathcal{D}$ domain in the sense of Theorem 1), we have $|t(z)| < 1$ so that x lies in the half plane $\Re(x) > 0$.

The main steps for the estimation of $\Xi(z)$ are:

$$\Xi(z) = \frac{1}{1-t(z)} \sum_{k\geq 1} [1 - \exp(-\sum_{j\geq k} \frac{e^{-jx}}{j})] \tag{38}$$

$$\sim \frac{1}{1-t(z)} \sum_{k\geq 1} [1 - \exp(-\int_{kx}^\infty e^{-v} \frac{dv}{v})] \tag{39}$$

$$\sim \frac{1}{(1-t(z))^2} \int_0^\infty [1 - \exp(-\int_u^\infty e^{-v} \frac{dv}{v})]\, du. \tag{40}$$

Once Eq. (40) is established, the theorem follows immediately by singularity analysis. Now the transition from (38) to (39) results from approximating a sum by an integral, i.e. by Euler–Maclaurin summation. (It is important that we should have convergence of the integral, but this is granted since $\Re(x) > 0$, which also allows us to change the upper limit of integration from $x\infty$ to $+\infty$ using Cauchy's theorem.) The transition from (39) to (40) follows similarly by Euler summation, noting that the step x in the discrete sum (39) is $\sim 1 - t(z)$ as $z \to e^{-1}$. The only details that are omitted from this proof are the derivation of uniform error bounds. ■

In passing, observe that the same method permits one to estimate the expected length of the longest cycle in a random permutation, thereby avoiding the delicate Tauberian arguments of [41]. Related distribution results are discussed by Stepanov in [44].

The next theorem concerns the expected value of $\lambda^{\max}$. Results concerning distribution estimates were first derived by Sachkov [39] and Proskurin [34] using multivariate probabilistic methods. The derivation that follows brings a "singular iteration problem", and the corresponding methods are also useful for $\rho^{\max}$ estimates.

Theorem 6 *The expectation of the maximum tail length ($\lambda^{\max}$) in a random mapping of $\mathcal{F}_n$ satisfies*

$$\mathbf{E}\{\lambda^{\max}|\mathcal{F}_n\} \sim c_2\sqrt{n},$$

where $c_2 \approx 1.73746$ is given by

$$c_2 = \sqrt{2\pi}\log 2.$$

Proof. (Sketch) Let $t^{[h]}(z)$ denote the GF of trees with height at most h. (Height is measured by the number of edges along a longest branch, so that a one node tree has height 0.) These generating functions are given by the recurrence

$$t^{[0]}(z) = z, \qquad t^{[h+1]}(z) = z\exp(t^{[h]}(z)). \tag{41}$$

We note that, as $h \to \infty$, we have $t^{[h]}(z) \to t(z)$, at least in the sense of convergence in the ring of formal power series. The GF for mappings with $\lambda^{\max} \le h$ follows again from the techniques of Section 2, and it is

$$f^{[h]}(z) = \exp(\log\frac{1}{1-t^{[h]}(z)}) = \frac{1}{1-t^{[h]}(z)}. \tag{42}$$

The GF associated to $\xi^{\max} = \lambda^{\max}$ is then found by Eq. (34) to be

$$\Xi(z) = \sum_{h\ge 0}[\frac{1}{1-t(z)} - \frac{1}{1-t^{[h]}(z)}]. \tag{43}$$

The analytic problem now lies with determining the nature of the approximation of $t(z)$ by the $t^{[h]}(z)$ when z is in the vicinity of e^{-1}. This is a *singular iteration* problem. For instance, for z real, $0 < z < e^{-1}$, the convergence is geometric. On the opposite, for $z > e^{-1}$, we have a case of strong hyperexponential divergence. At exactly $z = e^{-1}$, convergence is extremely slow being of order $1/h$. In other terms, we approximate a function, $t(z)$ with an algebraic singularity (branch point), by a collection of entire functions $t^{[h]}(z)$, and we need to find uniform estimates in z and h in a neighbourhood of the singularity of the limit[8].

Approximations similar to those needed for the proof of Theorem 6 are provided by us in [12], where we analyze the expected height of random trees of various sorts in this manner (see also [38] for closely related results). Imitating the method of proof of [12], we define

$$\epsilon = \epsilon(z) = 2^{1/2}\sqrt{1-ez} \qquad \text{and} \qquad e_h(z) = t(z) - t^{[h]}(z).$$

We also introduce the "indented" domain

$$D = \{z \mid |z| \le e^{-1},\ |\mathrm{Arg}(e^{-1}-z)| \le \pi/2 + \delta\} \tag{44}$$

for some $\delta > 0$. The first step, whose rather involved proof we omit, is to show that in the region

$$\{z \mid |z| \le e^{-1} + \delta,\ z \notin D\}$$

[8]It turns out that the $t^{[h]}(z)$ converge to $t(z)$ for all z in $\{z \mid z = \zeta e^{-\zeta}, |\zeta| \le 1\}$. This follows from recent results in iteration of entire functions due to Devaney [9, 8]; however, these results do not seem to provide the necessary quantitative information we need.

we have $e_h(z)$ small and $t^{[h]}(z)$ bounded away from 1, so that $\Xi(z)$ is analytic there. Therefore, in order to apply Theorem 1, we only need to study $\Xi(z)$ for $z \in D$.

The main step in the proof of the theorem is to establish that for $z \in D$, the $e_h(z)$ are approximated by an explicit function of h and ϵ,

$$e_h(z) \approx 2\epsilon \frac{(1-\epsilon)^h}{1-(1-\epsilon)^h}. \tag{45}$$

This approximation shows both the slow convergence of $t^{[h]}(e^{-1})$ to $t(e^{-1})$ (in fact, it shows that $e_h(e^{-1}) \sim 2/h$), and the geometric convergence for $\epsilon \neq 0$. The proof of a precise form of (45) proceeds along lines similar to those of [12], although there are some additional technical complications.

We define

$$w(z) = \frac{1}{1-e^{-z}} - \frac{1}{z} - \frac{1}{2}, \tag{46}$$

so that $w(z)$ is analytic in $|z| < 2\pi$. The basic recurrence for the $t^{[h]}(z)$ shows that

$$e_{h+1}(z) = t(z)(1 - e^{-e_h(z)}), \tag{47}$$

and therefore, by normalizing and the trick of "taking inverses"[9],

$$\frac{t(z)^j}{e_j(z)} = \frac{t(z)^{j-1}}{e_{j-1}(z)} + \frac{1}{2}t(z)^{j-1} + t(z)^{j-1}w(e_{j-1}(z)), \tag{48}$$

from which it follows that

$$\frac{t(z)^h}{e_h(z)} = \frac{1}{2}\frac{1-t(z)^h}{1-t(z)} + \frac{1}{t(z)-z} + \sum_{j=0}^{h-1} t(z)^j w(e_j(z)). \tag{49}$$

Equation (49) is the basic tool used to estimate $e_h(z)$, with the first term in (49) corresponding to approximation (45). Another argument shows that if the δ in the definition (44) of D is taken to be small enough, then $|e_h(z)| < 5$, say for all $h \geq 0$ and all $z \in D$. This means that the expansion (49) holds for all $z \in D$, without singularities arising from the w function. Sharp bounds for the error in the approximation (45) for $e_h(z)$ are obtained by iterated use of (49): First the crude bound for $e_j(z)$, when inserted into (49), gives a more refined estimate which is then used to obtain an improved estimate for the sum on the right hand side of (49), yielding the final approximation result.

As an illustration, we develop the case where $z = e^{-1}$. The reduced form of (49), with $t(e^{-1}) = 1$ and $e_h \equiv e_h(e^{-1})$ reads

$$\frac{1}{e_h} = \frac{h}{2} + \frac{1}{1-e^{-1}} + \sum_{j=0}^{h-1} w(e_j). \tag{50}$$

We start "bootstrapping" with the information that $0 < e_h < 1$. Eq. (50) provides

$$\frac{h}{2} + O(1) \leq \frac{1}{e_h} \leq \frac{h}{2} + \frac{h}{10} + O(1),$$

which guarantees that $1/e_h$ is upper and lower bounded by terms that are of order h. Thus $e_h = \Theta(\frac{1}{h})$. Reinserting this information inside (50), and using the fact that $w(x) = x/12 + O(x^3)$ for small x, we get the improved estimate

$$\frac{h}{2} + O(1) \leq \frac{1}{e_h} \leq \frac{h}{2} + O(\log h),$$

[9]This technique amounts to comparing a non linear slowly converging iteration to a homographic recurrence, $u_{n+1} = (au_n + b)/(cu_n + d)$. A good illustration is de Bruijn's treatment of the iterates of the function $\sin(x)$ in [6, Ch. 8].

so that $e_h \sim 2/h$. Continuing in this fashion, we obtain

$$\frac{1}{e_h} \equiv \frac{1}{e_h(e^{-1})} = \frac{h}{2} + \frac{1}{12}\log h + O(1),$$

and an expansion to an arbitrary order can be generated in this way.

Returning now to $\Xi(z)$, we have

$$\begin{aligned} \Xi(z) &= \frac{1}{1-t(z)} \sum_{h\geq 0} \frac{e_h(z)}{1-t^{[h]}(z)} \\ &= \frac{1}{(1-t(z))^2} \sum_{h\geq 0} \frac{e_h(z)}{1+\frac{e_h(z)}{1-t(z)}}. \end{aligned} \tag{51}$$

Setting, like in the preceding theorem, $t(z) = e^{-x} \sim 1-\epsilon$, the computation develops as follows:

$$\Xi(z) \sim \frac{2}{\epsilon} \sum_{h\geq 0} \frac{(1-\epsilon)^h}{1+(1-\epsilon)^h} \tag{52}$$

$$\sim \frac{2}{\epsilon} \sum_{h\geq 0} \frac{e^{-hx}}{1-e^{-hx}} \tag{53}$$

$$\sim \frac{2}{\epsilon^2} \int_0^\infty \frac{e^{-y}}{1-e^{-y}}\, dy \tag{54}$$

$$\sim \frac{2\log 2}{\epsilon^2}. \tag{55}$$

A crucial step there consists of justifying the use of the approximation (45) inside the exact form (51) resulting in Eq. (52) or its equivalent form (53). Once (52) and (53) are established, (54) follows by Euler–Maclaurin summation. The final result (55), when subjected to singularity analysis yields the statement of the theorem. ■

The last result in this subsection concerns the parameter $\rho^{\max}$ also called sometimes, in accordance with graph theoretic terminology, the *diameter*. It provides an answer to an open problem of Knuth ([23], Ex. 3.1.14, p. 519). As could be expected from the nature of the parameter $\rho^{\max}$, the proof combines the tools developed for Theorems 5 ($\mu^{\max}$) and 6 ($\lambda^{\max}$), and in particular it strongly relies on the estimates of $t^{[h]}(z)$ and $e_h(z)$.

Theorem 7 *The expectation of the maximum rho length ($\rho^{\max}$) in a random mapping of $\mathcal{F}_n$ satisfies*

$$\mathbf{E}\{\rho^{\max} | \mathcal{F}_n\} \sim c_3\sqrt{n},$$

where $c_3 \approx 2.4149$ is given by

$$c_3 = \sqrt{\frac{\pi}{2}} \int_0^\infty [1 - e^{-E_1(v)-I(v)}]\, dv,$$

with $E_1(v)$ denoting the exponential integral and

$$I(v) = \int_0^v e^{-u}[1 - \exp(\frac{-2u}{e^{v-u}-1})]\, \frac{du}{u}.$$

Results from the previous sections indicate that, in a random mapping, most of the points tend to be grouped together in a single giant component. This component might therefore be expected to have very tall trees and a large cycle. Thus, the inequality

$$c_3 = 2.4149... < c_1 + c_2 = 2.5199...$$

is rather interesting as it says that, with non zero asymptotic probability, the tallest tree in a functional graph is not rooted on the longest cycle.

Proof. (Sketch) Due to the intrinsically technical proof, we shall content ourselves here with a brief description of the major points of the analysis.

The generating function of functional graphs with rho–length at most k is, in accordance with (32),

$$f^{[k]}(z) = e^{v_k(z)} \qquad \text{where} \quad v_k(z) = t^{[k-1]}(z) + \frac{1}{2}(t^{[k-2]}(z))^2 + \cdots + \frac{1}{k}(t^{[0]}(z))^k, \tag{56}$$

with $v_0(z) = 0$. This form is easily justified, since in order to build a connected component with rho–length $\leq k$, we either graft a tree of height $\leq k-1$ on a 1 node cycle, or two trees of height at most $k-2$ on a 2 node cycle etc. Thus the GF of $\rho^{\max}$ is

$$\Xi(z) = \sum_{k\geq 0} [\frac{1}{1-t(z)} - e^{v_k(z)}].$$

Let now $\Xi_0(z)$ be the GF associated with the longest cycle parameter defined in (37). Several routes are conceivable. A convenient one starts by considering the difference

$$\Delta(z) = \Xi(z) - \Xi_0(z) = \sum_{k\geq 0} [e^{\ell_k(t(z))} - e^{v_k(z)}]$$

which is associated to $\rho^{\max} - \mu^{\max}$. Factoring out the quantity $e^{\ell_k(t(z))}$ in the general term, we find:

$$\Delta(z) = \frac{1}{1-t(z)} \sum_{k\geq 0} e^{-\sum_{j>k} t(z)^j/j} [1 - e^{-w_k(z)}], \tag{57}$$

where the w's are given by

$$\begin{aligned} w_k(z) &= \sum_{l=1}^{k} \frac{1}{l}[t(z)^l - (t^{[k-l]}(z))^l] \\ &= \sum_{l=1}^{k} \frac{t(z)^l}{l}\Big[1 - (\frac{t^{[k-l]}(z)}{t(z)})^l\Big] \\ &= \sum_{l=1}^{k} \frac{t(z)^l}{l}\Big[1 - \exp\big(-l(t(z) - t^{[k-l-1]}(z))\big)\Big] \\ &= \sum_{l=1}^{k} \frac{t(z)^l}{l}\Big[1 - \exp\big(-le_{k-l-1}(z)\big)\Big]. \end{aligned} \tag{58}$$

Taken together, the last form in (58) and Eq. (57) summarize the algebraic forms of generating functions needed for asymptotic analysis.

From this exact form, the analysis proceeds, setting again $t(z) = e^{-x}$, so that $x \sim 2^{1/2}\sqrt{1-ez}$. We use the $\approx$ symbol to emphasize the fact that error terms are not made explicit (and may be dominant in some eventually unessential regions).

First it can be proved that the dominant terms in the sum (57) of $\Delta(z)$ are for those values of k such that $kx = \Theta(1)$.

A crucial step is to approximate $w_k(z)$. We have from (58)

$$w_k(z) \approx x \sum_{l=1}^{k} \frac{e^{-lx}}{lx}\Big[1 - \exp\big(-le_{k-l-1}(z)\big)\Big],$$

where, by the general approximation of (45),

$$le_{k-l-1}(z) \approx 2lx \frac{e^{-(k-l)x}}{1-e^{-(k-l)x}}. \tag{59}$$

We now appeal to a continuous model for these sums based on Euler–Maclaurin summation. Setting $kx = v$, $lx = u$, we derive for $w_k(z)$ the approximation

$$\begin{aligned} w_k(z) &\approx \int_0^v e^{-u}\left[1 - \exp\big(-2u\frac{e^{-(v-u)}}{1-e^{-(v-u)}}\big)\right]\frac{du}{u} \\ &\approx I(kx). \end{aligned} \tag{60}$$

Injecting this form inside the main formula (57) for $\Delta(z)$ leads us to

$$\Delta(z) \approx \frac{1}{1-t(z)} \sum_{k\geq 0} e^{-E_1(kx)}[1 - e^{-I(kx)}],$$

which yields to a final assault of Euler Maclaurin:

$$\Delta(z) \sim \frac{1}{x^2}\int_0^\infty e^{-E_1(v)}[1 - e^{-I(v)}]\, dv. \tag{61}$$

There are of course considerable technical difficulties in actually organizing the proper approximations with their error terms. The form (61) combined with the information gathered in (40) regarding the GF of $\mu^{\max}$ shows that

$$\Xi(z) \sim \frac{1}{x^2}\int_0^\infty [1 - e^{-E_1(v)-I(v)}]\, dv. \tag{62}$$

At this stage, the result falls as a ripe fruit by singularity analysis. ■

4.2 Largest Configurations

We consider here the analysis of the largest tree and of the largest component in a random mapping. The analysis given here will be only partial since we shall appeal to a *smoothness hypothesis* (which is intuitively clear, but harder to establish rigorously).

Generating function equations here involve series truncation operators that we have already used implicitly when dealing with longest cycle. Let $a(z) = \sum_n a_n z^n$ be a power series. We introduce two operators called *truncation* $\mathbf{T}_m$ and *remainder* $\mathbf{R}_m$ that are defined by

$$\mathbf{T}_m[a(z)] = \sum_{n\leq m} a_n z^n, \qquad \mathbf{R}_m[a(z)] = \sum_{n>m} a_n z^n. \tag{63}$$

Let ξ^{max} be one of the parameters of random mappings, largest tree size or largest component size. We shall say that the parameter is *smooth* if the following condition is satisfied:

$$\textit{There exists } \delta \textit{ such that } \quad \delta = \lim_{n\to\infty} \frac{1}{n}\mathbf{E}\{\xi^{\max}|\mathcal{F}_n\}. \tag{64}$$

If δ exits, then by standard Abelian theorems [45, Chap. 7], $\Xi(z)$ satisfies $\Xi(z) \sim \delta_1(1-ez)^{-3/2}$ when z tends to e^{-1} *along the real axis* $z < e^{-1}$, for some δ_1 directly related to δ (actually $\delta_1 = 2\sqrt{2}\delta$). Thus if we find that, limited to the real line inside its circle of convergence, $\Xi(z)$ has the proper behaviour, then we are able to deduce the value of δ:

$$\delta = \frac{1}{2\sqrt{2}} \lim_{z\to e^{-1}} \Xi(z)(1-ez)^{3/2}.$$

The smoothness assumption thus dispenses with finding local expansions in a *complex* neighbourhood of e^{-1}. The reason why we introduce it here is to bypass some intrinsic difficulty in the singular behaviour of truncated Taylor series. Indeed, Jentzsch's theorem [45, p. 238] states that, *for every power series, every point of the circle of convergence is a limit–point of zeros of partial sums.* For largest components, the generating functions $f^{[k]}$ of (33) involve truncated Taylor series and thus exhibit a very irregular behaviour on the circle $|z| = e^{-1}$. The validity of our singular expansions is then restricted to the interior of the disk of convergence $|z| < e^{-1}$. It is probable that a more refined analysis (e.g. using different integration contours for different terms in the GF $\Xi(z)$) would enable us to dispense with the smoothness condition, but this is presently not obvious.

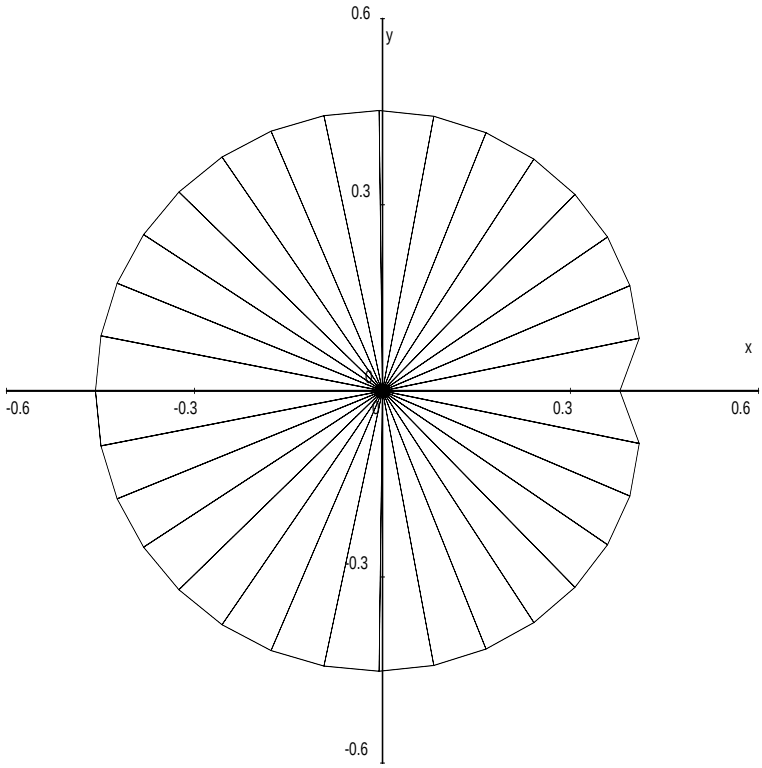

Figure 3. The star diagram of zeros of the polynomial $U_{32}(z)$, where

$$U_m(z) = 1 - \sum_{n=1}^{m} n^{n-1} \frac{z^n}{n!}.$$

This polynomial is a "truncation" of $1 - t(z)$, with $t(z)$ being the tree function, and its zeros appear in the analysis of largest tree size. In accordance with Jentzsch's theorem, the zeros tend to accumulate around the circle $|z| = e^{-1}$.

Theorem 8 *Assuming the smoothness condition, the expected value of the size of the largest tree*[10] *and the size of the largest connected component in a random mapping of $\mathcal{F}_n$ are asymptotically*

$$\begin{array}{ll} (i) & \textit{Largest tree:} \quad d_1 n \\ (ii) & \textit{Largest component:} \quad d_2 n, \end{array} \tag{65}$$

where $d_1 \approx 0.48$ and $d_2 \approx 0.75782$ are given by

$$\begin{aligned} d_1 &= 2\int_0^\infty \left[1 - \frac{1}{1 + \frac{1}{2\sqrt{\pi}} \int_x^\infty e^{-v} v^{-3/2}\, dv}\right] dx \\ d_2 &= 2\int_0^\infty \left[1 - \exp\left(\frac{1}{2}\int_x^\infty e^{-v} v^{-1}\, dv\right)\right] dx. \end{aligned}$$

Proof. (Sketch) The generating functions associated to the two cases under discussion are respectively

$$\begin{aligned} \Xi_1(z) &= \sum_{m \geq 0} \left[\frac{1}{1 - t(z)} - \frac{1}{1 - \mathbf{T}_m[t(z)]}\right] \\ \Xi_2(z) &= \sum_{m \geq 0} \left[\frac{1}{1 - t(z)} - e^{-\mathbf{T}_m[c(z)]}\right]. \end{aligned}$$

To approximate them, we set $z = e^{-1-y}$.

---

[10] Interesting distribution properties of the size of the largest tree are discussed in [24, p. 164] and [31].

Consider the case of largest tree (Ξ_1). Then, the GF can be rewritten as

$$\Xi_1(z) = \frac{1}{1-t(z)} \sum_{m\geq 0} \Big[1 - \frac{1}{1+\mathbf{R}_m[t(z)]/(1-t(z))}\Big]. \tag{66}$$

When m is large enough, and y small, using $1-t(z) \sim 2^{1/2}y^{1/2}$, we get by Stirling's approximation and Euler Maclaurin summation:

$$\begin{aligned} \frac{\mathbf{R}_m[t(z)]}{1-t(z)} &\approx 2^{-1/2}y^{-1/2} \sum_{n>m} \frac{e^{-ny}}{\sqrt{2\pi n^3}} \\ &\approx \frac{1}{2\sqrt{\pi}} \int_{my}^{\infty} e^{-v} v^{-3/2}\, dv. \end{aligned} \tag{67}$$

The final step consists in transporting approximation (67) inside Eq. (66), and using a further step of Euler–Maclaurin summation. The derivation for maximum component size is similar. ■

5 Extensions

The methodology discussed here is applicable to the analysis of a large class of combinatorial structures, roughly speaking those that can be specified using the combinatorial constructions of Section 2. It is also systematic enough that some of these analyses can be automated using computer algebra systems.

5.1 Alternative Models

Harris [19] already discusses mappings without fixed points. In the context of Section 2.1, this means that the specification of functional graphs (`FunGraph`) has to be altered by prohibiting cycles of length equal to 1 inside components:

```
type    FunGraph   = set(Component);
        Component  = cycle(Tree,card>1);
        Tree       = Node*set(Tree);
        Node       = Latom(1);
```

It is a simple exercise to derive the modified form of Eqns. (2) in this case:

$$\begin{aligned} \mathit{FunGraph}(z) &= \exp(\mathit{Component}(z)); \\ \mathit{Component} &= \log(1-\mathit{Tree}(z))^{-1} - \mathit{Tree}(z); \\ \mathit{Tree}(z) &= \mathit{Node}(z) \cdot \exp(\mathit{Tree}(z)); \\ \mathit{Node}(z) &= z, \end{aligned} \tag{68}$$

and in the equation for $\mathit{Component}(z)$, we have taken out the possibility of an isolated tree on a (size 1) cycle. In other words, the equation for modified functional graphs is

$$f_1^*(z) = \frac{e^{-t(z)}}{1-t(z)}. \tag{69}$$

Following Meir and Moon [25], Arney and Bender [1] discuss random mappings with constraints on the degrees of nodes. In fact, if we consider the functional graph attached to a quadratic transformation $\phi(x) = x^2 + c \bmod n$ for n prime, we see that, with a single exception $x = c$, all nodes have degree 0 or 2. This justifies interest in binary functional graphs, where the only (in)degrees of nodes allowed are 0 or 2. In that case, the specification only needs editing:

```
type     FunGraph   = set(Component);
         Component  = cycle(Node*BinTree);
         BinTree    = Node + Node * set(BinTree, card = 2);
         Node       = Latom(1),
```

The equation determining the GF $f_2^*(z)$ of these modified mappings becomes thus

$$f_2^*(z) = \frac{1}{1 - zb(z)}, \qquad \text{with} \quad b(z) = z + \frac{1}{2} z b^2(z). \tag{70}$$

Solving the quadratic equation for $b(z)$, we then find that

$$f_2^*(z) = \frac{1}{\sqrt{1 - 2z^2}},$$

and in particular, there are $2^{-n}(2n)!\binom{2n}{n}$ binary functional graphs of size $2n$. Algebraically, the case of general degree restrictions can be treated with comparable ease, and the corresponding analytic treatment involves the general discussion on singularity analysis of implicitly defined functions given in Section 2.2.

It is then a simple task to adjust the approach taken in earlier sections (especially Sect. 3) to such modified models. Analysis reveals that, in this case, though multiplicative constants are quite sensitive to such changes, the basic orders of growth of parameters remain essentially unaffected. An example in sharp contrast with this situation is treated in the next section as an illustration of the capabilities of an automatic analysis system.

5.2 Automatic Analysis

The methodology that we have followed in order to analyze additive parameters of random mappings is general enough, so as to make it amenable to some form of automatization. Together with B. Salvy and P. Zimmermann, the first author has developed a system named $\Lambda\Upsilon\Omega$ (Lambda–Upsilon–Omega), which takes as inputs specifications of combinatorial structures and characteristic parameters, and produces (in a number of cases) automatically the expected values of the parameters. The system makes extensive use of resources of the computer algebra system MAPLE [5].

Such an approach proves useful when analyzing complex models. A description of the current state of the system is given in [15] and it will only be illustrated by treating a *"sensitivity analysis"* problem due to Michèle Soria who discusses systematically such phenomena in her thesis [42].

The analysis below is produced automatically by the $\Lambda\Upsilon\Omega$ system. The session presents the analysis of a variant of the model of random mappings: We modify the classical definition of functional graphs by forcing all nodes on cycles to have indegree 2 exactly. In other words, we consider special functional graphs (the `Sfungraph` type) made of sets of cycles of special *planted* trees (`Stree`). The problem consists in determining to what extent essential parameters are sensitive to such a change in the model. Standard functional graphs have on average $\frac{1}{2}\log n + O(1)$ components (cycles) and $\sim \sqrt{\pi n}$ nodes on cycles. The small change in the specifications somewhat unexpectedly results in a rather drastic change of stochastic properties of these graphs.

The $\Lambda\Upsilon\Omega$ system accepts as inputs structural descriptions of "decomposable" structures in the style of Section 2 and of our earlier formal specifications. Thus, our class of special functional graphs will be specified quite naturally by:

```
type     Sfungraph  = set(Scomponent);
         Scomponent = cycle(Stree);
         Stree      = product(Node,Tree);
         Tree       = product(Node,set(Tree));
         Node       = Latom(1);
```

The $\Lambda\Upsilon\Omega$ system is primarily designed to estimate the average case complexity of algorithms. In order to analyze parameters like the number of components, we therefore write a procedure whose *complexity* is precisely equal to the parameter to be analyzed. The second part of the input thus reads:

```
procedure number_of_components(f : Sfungraph);
begin
        forall c in f do
                count;
end;

procedure number_of_cyclic_points(f : Sfungraph);
begin
        forall c in f do
                forall d in c do
                        count;
end;

measure count:1;
```

where the last line specifies that `count` is a counter with constant complexity equal to 1.

Systematic translation mechanisms allow us to compile such specifications into equations over generating functions. This task is achieved by the ALGEBRAIC ANALYZER of $\Lambda\Upsilon\Omega$ written in the Caml language [46].

```
Counting generating functions:
  Tree(z)=Node(z)*exp(Tree(z))
  Stree(z)=Node(z)*Tree(z)
  Scomponent(z)=L(Stree(z))
  Sfungraph(z)=exp(Scomponent(z))
  Node(z)=z

Complexity descriptors:
  tau_number_of_components(z)=(exp(Scomponent(z))*1*Scomponent(z))+0
  tau_number_of_cyclic_points(z)=(exp(Scomponent(z))*1*Stree(z)/(1-Stree(z)))
```

The second batch (labelled "complexity descriptors") represents generating functions of procedures' costs. These equations are then solved by a SOLVER programme written in Maple. The solution is here expressed in terms of $L(y) \equiv \log(1-y)^{-1}$ and of Maple's W–function which is defined (implicitly) by $W(z)e^{W(z)} = z$.

```
      tau_number_of_components(z) = exp(L(- z W(- z))) L(- z W(- z))

                                          exp(L(- z W(- z))) z W(- z)
     tau_number_of_cyclic_points(z) = - -----------------------------
                                                  1 + z W(- z)
```

At this stage, an ANALYTIC ANALYZER with extensive asymptotic capabilities, takes control of the asymptotic analysis [40]. It is built on a large library of Maple programmes (currently about 7000 lines), and on this problem, it selects a strategy based on singularity analysis. The number of special functional graphs (`Sfungraph`) of size n then appears in its *raw* form produced by the system as:

```
...  n! times:
                3/2  1/2         2
          exp(-1)    2    exp(1/2)  exp(-1/2) exp(n)         exp(n)
    (1/2 --------------------------------------------) + (O(--------))
                                2   1/2  3/2                    2
                  (1 - exp(-1))  Pi    n                      n
```

a formula which, after going through Maple's simplifier and LaTeX interface yields *verbatim*

$$(n\,!) \times \left[\left(\frac{\sqrt{2}e^{n-1}}{2(e^{-1}-1)^2\sqrt{\pi}n^{3/2}} \right) + \left(O\left(\frac{e^n}{n^2}\right)\right) \right].$$

The system then computes total costs (i.e., total values of parameters over all structures of size n) via their generating functions. From there, mean value estimates folllow. For instance, in the case of the *average* number of components, we get the following message

```
Floating point evaluation:
                                                  1
                          (1.458675144) + (O(------))
                                                 1/2
                                               n
```

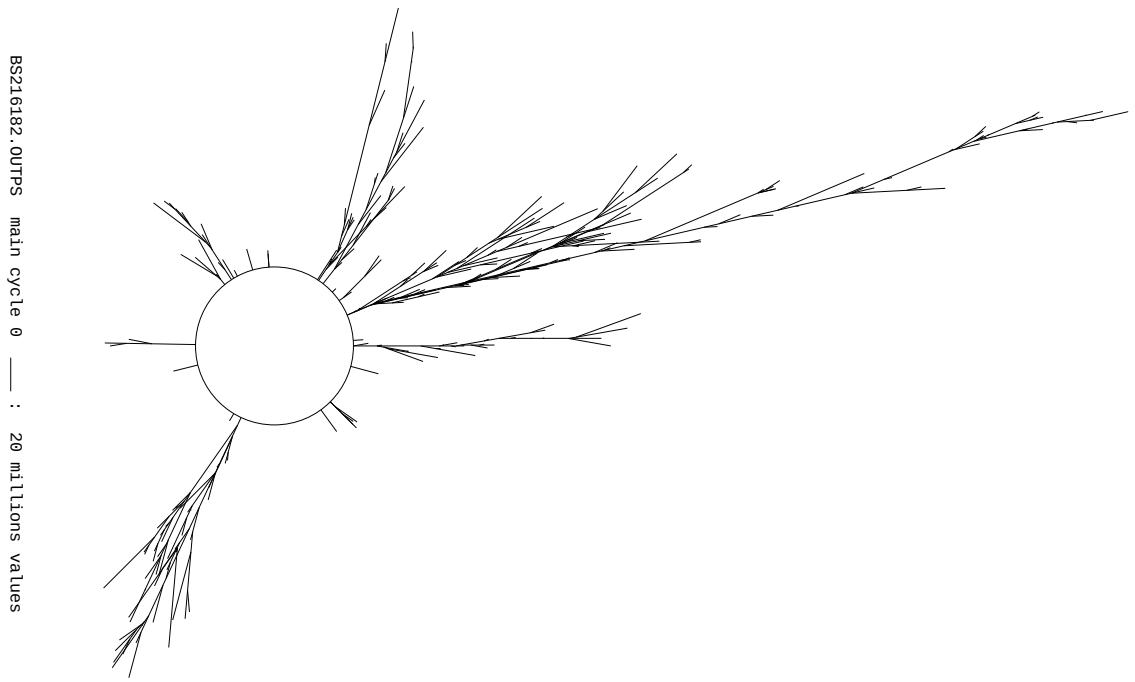

Figure 4. A rendering due to Quisquater and Delescaille of the "giant component" in a functional graph representing an iteration structure of the DES cryptosystem. The DES is used here as an iterator on a set of cardinality 2^{56} by letting its "output" loop on its "key" entry (keeping the "message"fixed). The drawing represents a skeleton graph where approximately 1 in every 10^6 points is sampled. Such graphs are discussed in [36, 37].

where the symbolic form of the constant 1.4586 was also determined in passing by the system:

$$1 - \log(1 - e^{-1}).$$

Similarly, for the number of cyclic points, we obtain

```
Floating point evaluation:
                                                  1
                          (2.163953412) + (O(------))
                                                 1/2
                                                n
```

with the symbolic form of the constant being

$$-\frac{e^{-1}+1}{e^{-1}-1}.$$

In total, within a few minutes of symbolic computations, the system, starting from formal specifications, has determined first symbolically, then numerically, that: (i) the expected number of components is ~ 1.45; (ii) the expected number of points lying on cycles is ~ 2.16. This example demonstrates an unusual case of model sensitivity (compare with the corresponding values of $O(\log n)$ and $O(\sqrt{n})$ for unconstrained random mappings). The precise capabilities of the system are described in [14, 15, 40, 46].

6 Conclusions

We have seen a systematic approach to the analysis of a large number of parameters of random mappings (or functional graphs) using a coherent generating function framework.

In a random mapping of size n, cycles presents themselves after about $\sqrt{n}$ iteration steps (Section 2), and this phenomenon is fairly unavoidable since the expected diameter is also $O(\sqrt{n})$ (Section 3). Also, random functional graphs tend to have one giant component and a few large trees.

These facts are well illustrated by extensive computations performed by J-J. Quisquater with the DES cryptographic system (see Fig. 4 and [36, 37]). Simulations with shift register sequences [1] or with Pollard's algorithm [33] (i.e., quadratic functions), as well as Bach's theoretical results [2] also confirm the frequent validity of predictions based on the heuristic random mapping model for various applications in cryptography, random number generation, computational number theory, or the analysis of algorithms.

Acknowledgements. This research was supported in part by the ESPRIT II Basic Research Actions Program of the EC under contract No. 3075 (project ALCOM).

References

[1] J. Arney and E. D. Bender. Random mappings with constraints on coalescence and number of origins. *Pacific J. Math.*, 103:269–294, 1982.

[2] E. Bach. Toward a theory of Pollard's rho–method. *Information and Computation*, to appear, 1989.

[3] R. P. Brent and J. M. Pollard. Factorization of the eighth Fermat number. *Mathematics of Computation*, 36:627–630, 1981.

[4] A. Z. Broder. Weighted random mappings; properties and applications. Technical Report STAN-CS-85-1054, Computer Science Dept., Stanford University, 1985. (Author's PhD Thesis).

[5] B.W. Char, K.O. Geddes, G.H. Gonnet, M.B. Monagan, and S.M. Watt. *MAPLE: Reference Manual*. University of Waterloo, 1988. 5th edition.

[6] N. G. de Bruijn. *Asymptotic Methods in Analysis*. North Holland, third edition, 1958. Reprinted by Dover, 1981.

[7] J. M. Delaurentis. Components and cycles of a random function. In C. Pomerance, editor, *Advances in Cryptology*, volume 293 of *Lecture Notes in Computer Science*, pages 231–242, 1988. (Proceedings of CRYPTO'87, Santa–Barbara.).

[8] R. L. Devaney. Dynamics of entire maps. in *Proc. International Conference on Dynamics*, Stefan Banach Center, Warsaw (to appear).

[9] R. L. Devaney. Julia sets and bifurcation diagrams for exponential maps. *Bulletin of the American Mathematical Society*, 11:167–171, 1984.

[10] M. A. Evgrafov. *Analytic Functions*. Dover, New York, 1966.

[11] P. Flajolet, D. E. Knuth, and B. Pittel. The first cycles in an evolving graph. *Discrete Mathematics*, 75:167–215, 1989.

[12] P. Flajolet and A. Odlyzko. The average height of binary trees and other simple trees. *Journal of Computer and System Sciences*, 25:171–213, 1982.

[13] P. Flajolet and A. M. Odlyzko. Singularity analysis of generating functions. *SIAM Journal on Discrete Mathematics*, 3(1), February 1990. To appear. Also available as INRIA Research Report 826, 1987, 25p.

[14] P. Flajolet, B. Salvy, and P. Zimmermann. Lambda–Upsilon–Omega: An assistant algorithms analyzer. In T. Mora, editor, *Applied Algebra, Algebraic Algorithms and Error–Correcting Codes*, volume 357 of *Lecture Notes in Computer Science*, pages 201–212, 1989. (Proceedings AAECC'6, Rome, July 1988).

[15] P. Flajolet, B. Salvy, and P. Zimmermann. Lambda–Upsilon–Omega: The 1989 Cookbook. Research Report 1073, Institut National de Recherche en Informatique et en Automatique, August 1989.

[16] P. Flajolet and M. Soria. Gaussian limiting distributions for the number of components in combinatorial structures. *J. Combinatorial Theory*, 1989. To appear. Available as INRIA Research Report 809, March 1988.

[17] D. Foata. *La série génératrice exponentielle dans les problèmes d'énumération*. S.M.S. Montreal University Press, 1974.

[18] I. P. Goulden and D. M. Jackson. *Combinatorial Enumeration*. John Wiley, New York, 1983.

[19] B. Harris. Probability distributions related to random mappings. *Annals of Mathematical Statistics*, 31(2):1045–1062, 1960.

[20] J. Jaworski. *Random Mappings*. PhD thesis, A. Mickiewicz University, 1985. (In Polish).

[21] I. B. Kalugin. A class of random mappings. *Proceedings of the Steklov Institute of Mathematics*, 177(4):79–110, 1988. (Issue on *Probabilistic Problems of Discrete Mathematics*).

[22] D. E. Knuth. *The Art of Computer Programming*, volume 3: Sorting and Searching. Addison-Wesley, 1973.

[23] D. E. Knuth. *The Art of Computer Programming*, volume 2: Seminumerical Algorithms. Addison-Wesley, 2nd edition, 1981.

[24] V. F. Kolchin. *Random Mappings*. Optimization Software Inc., New York, 1986. Translated from *Slučajnye Otobraženija*, Nauka, Moscow, 1984.

[25] A. Meir and J. W. Moon. On the altitude of nodes in random trees. *Canadian Journal of Mathematics*, 30:997–1015, 1978.

[26] L. R. Mutafčiev. On some stochastic problems of discrete mathematics. In *Mathematics and Education in Mathematics* (Sunny Beach), pages 57–80, Bulgarian Academy of Sciences, Sophia, Bulgaria, 1984.

[27] L. R. Mutafčiev. Limit theorems concerning random mapping patterns. *Combinatorica*, 8:345–356, 1988.

[28] A. M. Odlyzko. Periodic oscillations of coefficients of power series that satisfy functional equations. *Advances in Mathematics*, 44:180–205, 1982.

[29] F. W. J. Olver. *Asymptotics and Special Functions*. Academic Press, 1974.

[30] A. I. Pavlov. On an equation in a symmetric semigroup. *Proceedings of the Steklov Institute of Mathematics*, 177(4):121–128, 1988. (Issue on *Probabilistic Problems of Discrete Mathematics*).

[31] Yu. L. Pavlov. The asymptotic distribution of maximum tree size in a random forest. *Theory of Probability and Applications*, 22:509–520, 1977.

[32] Yu. L. Pavlov. On random mappings with constraints on the number of cycles. *Proceedings of the Steklov Institute of Mathematics*, 177(4):131–143, 1988. (Issue on *Probabilistic Problems of Discrete Mathematics*).

[33] J. M. Pollard. A Monte Carlo method for factorization. *BIT*, 15(3):331–334, 1975.

[34] G. V. Proskurin. On the distribution of the number of vertices in strata of a random mapping. *Theory of Probability and Applications*, 18:803–808, 1973.

[35] P. Purdom and J. Williams. Cycle length in a random function. *Transactions of the American Mathematical Society*, 133:547–551, 1968.

[36] J.-J. Quisquater and J.-P. Delescaille. Other cycling tests for DES. In C. Pomerance, editor, *Advances in Cryptology*, volume 293 of *Lecture Notes in Computer Science*, pages 255–256. Springer-Verlag, 1988. (Proceedings of CRYPTO'87, Santa–Barbara.).

[37] J.-J. Quisquater and J.-P. Delescaille. How easy is collision search? New results and applications to DES. In *Proceedings of CRYPTO'89*, Lecture Notes in Computer Science. Springer-Verlag, 1989. To appear.

[38] A. Rényi and G. Szekeres. On the height of trees. *Australian Journal of Mathematics*, 7:497–507, 1967.

[39] V. N. Sachkov. Random mappings with bounded height. *Theory of Probability and Applications*, 18:120–130, 1973.

[40] B. Salvy. Fonctions génératrices et asymptotique automatique. Research Report 967, Institut National de Recherche en Informatique et en Automatique, 1989.

[41] L. A. Shepp and S. P. Lloyd. Ordered cycle lengths in a random permutation. *Transactions of the American Mathematical Society*, 121:340–357, 1966.

[42] M. Soria. *Méthodes d'analyse pour les constructions combinatoires et les algorithmes*. Doctorat ès sciences, Université de Paris–Sud, Orsay, 1989.

[43] R. P. Stanley. *Enumerative Combinatorics*, volume I. Wadsworth & Brooks/Cole, 1986.

[44] V. E. Stepanov. Limit distributions of certain characteristics of random mappings. *Theory of Probability and Applications*, 14:612–626, 1969.

[45] E. C. Titchmarsh. *The Theory of Functions*. Oxford University Press, 2nd edition, 1939.

[46] P. Zimmermann. Alas: un système d'analyse algébrique. Research Report 968, Institut National de Recherche en Informatique et en Automatique, 1989.