A Hybrid of Darboux's Method and Singularity Analysis in Combinatorial Asymptotics

Philippe Flajolet*, Eric Fusy†, Xavier Gourdon‡,
Daniel Panario§ and Nicolas Pouyanne¶

Submitted: Jun 17, 2006; Accepted: Nov 3, 2006; Published: Nov 13, 2006
Mathematics Subject Classification: 05A15, 05A16, 30B10, 33B30, 40E10

Abstract

A "hybrid method", dedicated to asymptotic coefficient extraction in combinatorial generating functions, is presented, which combines Darboux's method and singularity analysis theory. This hybrid method applies to functions that remain of moderate growth near the unit circle and satisfy suitable smoothness assumptions—this, even in the case when the unit circle is a natural boundary. A prime application is to coefficients of several types of infinite product generating functions, for which full asymptotic expansions (involving periodic fluctuations at higher orders) can be derived. Examples relative to permutations, trees, and polynomials over finite fields are treated in this way.

Introduction

A few enumerative problems of combinatorial theory lead to generating functions that are expressed as infinite products and admit the unit circle as a natural boundary. Functions with a fast growth near the unit circle are usually amenable to the saddle point method, a famous example being the integer partition generating function. We consider here functions of moderate growth, which are outside the scope of the saddle point method. We do

*Algorithms Project, INRIA Rocquencourt, F-78153 Le Chesnay, France (Philippe.Flajolet@inria.fr).

†Algorithms Project, INRIA Rocquencourt, F-78153 Le Chesnay, France (Eric.Fusy@inria.fr).

‡Algorithms Project and Dassault Systems, France (xgourdon@yahoo.fr).

§Mathematics and Statistics, Carleton University, Ottawa, K1S 5B6, Canada (daniel@math.carleton.ca),

¶Mathématiques, Université de Versailles, 78035 Versailles, France (pouyanne@math.uvsq.fr).

so in the case where neither singularity analysis nor Darboux's method is directly applicable, but the function to be analysed can be factored into the product of an elementary function with isolated singularities and a sufficiently smooth factor on the unit circle. Such decompositions are often attached to infinite products exhibiting a regular enough structure and are easily obtained by the introduction of suitable convergence factors. Under such conditions, we prove that coefficients admit full asymptotic expansions involving powers of logarithms and descending powers of the index n, as well as periodically varying coefficients. Applications are given to the following combinatorial-probabilistic problems: the enumeration of permutations with distinct cycle lengths, the probability that two permutations have the same cycle-length profile, the number of permutations admitting an mth root, the probability that a polynomial over a finite field has factors of distinct degrees, and the number of forests composed of trees of different sizes.

Plan of the paper. We start by recalling in Section 1 the principles of two classical methods dedicated to coefficient extraction in combinatorial generating functions, namely Darboux's method and singularity analysis, which are central to our subsequent developments. The hybrid method *per se* forms the subject of Section 2, where our main result, Theorem 2, is established. Section 3 treats the asymptotic enumeration of permutations having distinct cycle sizes: this serves to illustrate in detail the hybrid method at work. Section 4 discusses more succinctly further combinatorial problems leading to generating functions with a natural boundary—these are relative to permutations, forests, and polynomials over finite fields. A brief perspective is offered in our concluding section, Section 5.

1 Darboux's method and singularity analysis

In this section, we gather some previously known facts about Darboux's method, singularity analysis, and basic properties of analytic functions that are central to our subsequent analyses.

1.1 Functions of finite order

Throughout this study, we consider analytic functions whose expansion at the origin has a finite radius of convergence, that is, functions with singularities at a finite distance from the origin. By a simple scaling of the independent variable, we may restrict attention to function that are analytic in the open unit disc D but not in the closed unit disc $\overline{D}$. What our analysis a priori excludes are thus: (i) entire functions; (ii) purely divergent series. (For such excluded cases, either the saddle point method or ad hoc manipulations of divergent series are often instrumental in gaining access to coefficients [3, 15, 30].) Furthermore we restrict attention to functions that remain of moderate growth near the unit circle in the following sense.

Definition 1 *A function $f(z)$ analytic in the open unit disc D is said to be of* global order $a \leq 0$ *if*

$$f(z) = O((1-|z|)^a) \qquad (|z| < 1),$$

that is, there exists an absolute constant M such that $|f(z)| < M(1-|z|)^a$ for all z satisfying $|z| < 1$.

This definition typically excludes the partition generating function

$$P(z) = \prod_{k=1}^{\infty} \frac{1}{1-z^k},$$

which is of infinite order and to which the saddle point method (as well as a good deal more) is applicable [1, 2, 20]. In contrast, a function like

$$\frac{e^z}{\sqrt{1+z}\sqrt[3]{1-z}}$$

is of global order $a = -\frac{1}{2}$, while

$$\exp\left(\sum_{k\geq 1} \frac{z^k}{k^2}\right) \quad \text{or} \quad (1-z)^{5/2}$$

are of global order $a = 0$.

We observe, though we do not make use of the fact, that a function $f(z)$ of global order $a \leq 0$ has coefficients that satisfy $[z^n]f(z) = O(n^{-a})$. The proof results from trivial bounds applied to Cauchy's integral form

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

upon integrating along the contour C: $|z| = 1 - n^{-1}$. (In [7], Braaksma and Stark present an interesting discussion leading to refined estimates of the $O(n^{-a})$ bound.)

1.2 Log-power functions

What we address here is the asymptotic analysis of functions whose local behaviour at designated points involves a combination of logarithms and powers (of possibly fractional exponent). For the sake of notational simplicity, we write

$$\mathrm{L}(z) := \log \frac{1}{1-z}.$$

Simplifying the theory to what is needed here, we set:

Definition 2 *A* log-power function at 1 *is a finite sum of the form*

$$\sigma(z) = \sum_{k=1}^{r} c_k \left(\mathrm{L}(z)\right)(1-z)^{\alpha_k},$$

where $\alpha_1 < \cdots < \alpha_r$ and each c_k is a polynomial. A log-power function at a finite set of points $Z = \{\zeta_1, \ldots, \zeta_m\}$, *is a finite sum*

$$\Sigma(z) = \sum_{j=1}^{m} \sigma_j\left(\frac{z}{\zeta_j}\right),$$

where each σ_j is a log-power function at 1.

In what follows, we shall only need to consider the case where the ζ_j lie on the unit disc: $|\zeta_j| = 1$.

It has been known for a long time (see, e.g., Jungen's 1931 paper, ref. [22], and [14, 15] for wide extensions) that the coefficient of index n in a log-power function admits a full asymptotic expansion in descending powers of n.

Lemma 1 (Coefficients of log-powers) *The expansion of the coefficient of a log-power function is computable by the two rules:*

$$\begin{aligned}
[z^n](1-z)^{\alpha} &\sim \frac{n^{-\alpha-1}}{\Gamma(-\alpha)} + \frac{\alpha(\alpha+1)n^{-\alpha-2}}{\Gamma(-\alpha)} + \cdots \\
[z^n](1-z)^{\alpha}\,\mathrm{L}(z)^k &= (-1)^k \frac{\partial^k}{\partial\alpha^k}\left([z^n](1-z)^{\alpha}\right) \\
&\sim (-1)^k \frac{\partial^k}{\partial\alpha^k}\left[\frac{n^{-\alpha-1}}{\Gamma(-\alpha)} + \frac{\alpha(\alpha+1)n^{-\alpha-2}}{\Gamma(-\alpha)} + \cdots\right].
\end{aligned} \tag{2}$$

The general shape of the expansion is thus

$$\begin{aligned}
[z^n](1-z)^{\alpha}L(z)^k &\underset{n\to+\infty}{\sim} \frac{1}{\Gamma(-\alpha)} n^{-\alpha-1}(\log n)^k && (\alpha \notin \mathbb{Z}_{\geq 0}) \\
[z^n](1-z)^{r}L(z)^k &\underset{n\to+\infty}{\sim} (-1)^r k(r!) n^{-r-1}(\log n)^{k-1} && (r \in \mathbb{Z}_{\geq 0}, k \in \mathbb{Z}_{\geq 1}).
\end{aligned}$$

In the last case, the term involving $(\log n)^k$ disappears as its coefficient is $1/\Gamma(-r) \equiv 0$. In essence, smaller functions at a singularity have asymptotically smaller coefficients and logarithmic factors in a function are reflected by logarithmic terms in the coefficients' expansion; for instance,

$$\begin{aligned}
[z^n]\frac{\mathrm{L}(z)}{\sqrt{1-z}} &\sim \frac{\log n + \gamma + 2\log 2}{\sqrt{\pi n}} - \frac{\log n + \gamma + 2\log 2}{8\sqrt{\pi n^3}} + \cdots \\
[z^n](1-z)\,\mathrm{L}(z)^2 &\sim -\frac{2}{n^2}(\log n + \gamma - 1) - \frac{1}{n^3}(2\log n + 2\gamma - 5) + \cdots .
\end{aligned}$$

When supplemented by the rule

$$[z^n]\sigma\left(\frac{z}{\zeta}\right) = \zeta^{-n}[z^n]\sigma(z),$$

Lemma 1 makes it effectively possible to determine the asymptotic behaviour of coefficients of all log-power functions.

1.3 Smooth functions and Darboux's method

Once the coefficients of functions in some basic scale are known, there remains to translate error terms. Precisely, we consider in this article functions of the form

$$f(z) = \Sigma(z) + R(z),$$

and need conditions that enable us to estimate the coefficients of the error term $R(z)$. Two conditions are classically available: one based on smoothness (i.e., differentiability) is summarized here, following classical authors (e.g., [31]); the other based on growth conditions *and* analytic continuation is discussed in the next subsection.

Definition 3 *Let $h(z)$ be analytic in $|z| < 1$ and s be a nonnegative integer. The function $h(z)$ is said to be $\mathcal{C}^s$–*smooth[1] on the unit disc *(or of class $\mathcal{C}^s$) if, for all $k = 0 \,..\, s$, its kth derivative $h^{(k)}(z)$ defined for $|z| < 1$ admits a continuous extension on $|z| \le 1$.*

For instance, a function of the form

$$h(z) = \sum_{n \ge 0} h_n z^n \qquad \text{with} \quad h_n = O(n^{-s-1-\delta}),$$

for some $\delta > 0$ and $s \in \mathbb{Z}_{\ge 0}$, is $\mathcal{C}^s$-smooth. Conversely, the fact that smoother functions have asymptotically smaller coefficients lies at the heart of Darboux's method.

Lemma 2 (Darboux's transfer) *If $h(z)$ is $\mathcal{C}^s$–smooth, then*

$$[z^n]h(z) = o(n^{-s}).$$

Proof. One has, by Cauchy's coefficient formula and continuity of $h(z)$:

$$[z^n]h(z) = \frac{1}{2\pi} \int_{-\pi}^{\pi} h(e^{i\theta}) e^{-ni\theta} \, d\theta.$$

When $s = 0$, the statement results directly from the Riemann-Lebesgue theorem [33, p. 109]. When $s > 0$, the estimate results from s successive integrations by parts followed by the Riemann-Lebesgue argument. See Olver's book [31, p. 309–310] for a neat discussion. □

Definition 4 *A function $Q(z)$ analytic in the open unit disc D is said to admit a* log-power expansion of class $\mathcal{C}^t$ *if there exist a finite set of points $Z = \{\zeta_1, \ldots, \zeta_m\}$ on the unit circle $|z| = 1$ and a log-power function $\Sigma(z)$ at the set of points Z such that $Q(z) - \Sigma(z)$ is $\mathcal{C}^t$–smooth on the unit circle.*

[1] A function $h(z)$ is said to be *weakly smooth* if it admits a continuous extension to the closed unit disc $|z| \le 1$ and the function $g(\theta) := h(e^{i\theta})$ is s times continuously differentiable. This seemingly weaker notion turns out to be equivalent to Definition 3, by virtue of the existence and unicity of the solution to Dirichlet's problem with continuous boundary conditions, cf [33, Ch. 11].

Lemma 3 (Darboux's method) *If $Q(z)$ admits a log-power expansion of class $\mathcal{C}^t$ with $\Sigma(z)$ an associated log-power function, its coefficients satisfy*

$$[z^n]Q(z) = [z^n]\Sigma(z) + o\left(n^{-t}\right).$$

PROOF. One has $Q = \Sigma + R$, with R being $\mathcal{C}^t$ smooth. The coefficients of R are estimated by Lemma 2. $\square$

Consider for instance

$$Q_1(z) = \frac{e^z}{\sqrt{1-z}}, \qquad Q_2(z) = \frac{\sqrt{1+z}}{\sqrt{1-z}}e^z.$$

Both are of global order $-\frac{1}{2}$ in the sense of Definition 1. By making use of the analytic expansion of e^z at 1, one finds

$$Q_1(z) = \left(\frac{e}{\sqrt{1-z}} - e\sqrt{1-z}\right) + R_1(z),$$

where $R_1(z)$, which is of the order of $(1-z)^{3/2}$ as $z \to 1^-$, is $\mathcal{C}^1$-smooth. The sum of the first two terms (in parentheses) constitutes $\Sigma(z)$, in this case with $Z = \{1\}$. Similarly, for $Q_2(z)$, by making use of expansions at the elements of $Z = \{-1, +1\}$, one finds

$$Q_2(z) = \left(\frac{e\sqrt{2}}{\sqrt{1-z}} - \frac{5e}{4}\sqrt{2}\sqrt{1-z} + \frac{1}{e\sqrt{2}}\sqrt{1+z}\right) + R_2(z),$$

where $R_2(z)$ is also $\mathcal{C}^1$–smooth. Accordingly, we find:

$$[z^n]Q_1(z) = e\frac{1}{\sqrt{\pi n}} + o\left(\frac{1}{n}\right), \qquad [z^n]Q_2(z) = \frac{e\sqrt{2}}{\sqrt{\pi n}} + o\left(\frac{1}{n}\right). \tag{3}$$

The next term in the asymptotic expansion of $[z^n]Q_2$ involves a linear combination of $n^{-3/2}$ and $(-1)^n n^{-3/2}$, where the latter term reflects the singularity at $z = -1$. Such calculations are typical of what we shall encounter later.

1.4 Singularity analysis

What we refer to as singularity analysis is a technology developed by Flajolet and Odlyzko [14, 30], with further additions to be found in [10, 11, 15]. It applies to a function with a finite number of singularities on the boundary of its disc of convergence. Our description closely follows Chapter VI of the latest edition of *Analytic Combinatorics* [15].

Singularity analysis theory adds to Lemma 1 the theorem that, under conditions of analytic continuation, O- and o-error terms can be similarly transferred to coefficients. Define a Δ-*domain* associated to two parameters $R > 1$ (the radius) and $\phi \in (0, \frac{\pi}{2})$ (the angle) by

$$\Delta(R, \phi) := \left\{z \;\middle|\; |z| < R,\ \phi < \arg(z-1) < 2\pi - \phi,\ z \neq 1\right\}$$

where $\arg(w)$ denotes the argument of w taken here in the interval $[0, 2\pi[$. By definition a Δ-domain properly contains the unit disc, since $\phi < \frac{\pi}{2}$. (Details of the values of R, ϕ are immaterial as long as $R > 1$ and $\phi < \frac{\pi}{2}$.)

The following definition is in a way the counterpart of smoothness (Definition 4) for singularity analysis of functions with isolated singularities.

Definition 5 *Let $h(z)$ be analytic in $|z| < 1$ and have isolated singularities on the unit circle at $Z = \{\zeta_1, \ldots, \zeta_m\}$. Let t be a real number. The function $h(z)$ is said to admit a* log-power expansion of type $\mathcal{O}^t$ *(relative to Z) if the following two conditions are satisfied:*

— *The function $h(z)$ is analytically continuable to an indented domain $\mathfrak{D} = \bigcap_{j=1}^m (\zeta_j \cdot \Delta)$, with Δ some Δ-domain.*

— *There exists a log-power function $\Sigma(z) := \sum_{j=1}^m \sigma_j(z/\zeta_j)$ such that, for each $\zeta_j \in Z$, one has*

$$h(z) - \sigma_j(z/\zeta_j) = O\left((z - \zeta_j)^t\right), \tag{4}$$

as $z \to \zeta_j$ in $(\zeta_j \cdot \Delta)$.

Observe that $\Sigma(z)$ is *a priori* uniquely determined only up to $O((z - \zeta_j)^t)$ terms. The minimal function (with respect to the number of monomials) satisfying (4) is called the *singular part* of $h(z)$ (up to $\mathcal{O}^t$ terms).

A basic result of singularity analysis theory enables us to extract coefficients of functions that admit of such expansions.

Lemma 4 (Singularity analysis method) *Let $Z = \{\zeta_1, \ldots, \zeta_m\}$ be a finite set of points on the unit circle, and let $P(z)$ be a function that admits a log-power expansion of type $\mathcal{O}^t$ relative to Z, with singular part $\Sigma(z)$. Then, the coefficients of h satisfy*

$$[z^n]P(z) = [z^n]\Sigma(z) + O\left(n^{-t-1}\right). \tag{5}$$

Proof. The proof of Lemma 4 starts from Cauchy's integral formula (1) and makes use of the contour C that lies at distance $\frac{1}{n}$ of the boundary of the analyticity domain, $\mathfrak{D} = \bigcap_{j=1}^m (\zeta_j \cdot \Delta)$. See [14, 15] for details. □

1.5 Polylogarithms

For future reference (see especially Section 3), we gather here facts relative to the *polylogarithm* function $\mathrm{Li}_\nu(z)$, which is defined for any $\nu \in \mathbb{C}$ by

$$\mathrm{Li}_\nu(z) := \sum_{n=1}^{\infty} \frac{z^n}{n^\nu}. \tag{6}$$

One has in particular

$$\mathrm{Li}_0(z) = \frac{z}{1-z}, \qquad \mathrm{Li}_1(z) = \log \frac{1}{1-z} \equiv \mathrm{L}(z).$$

In the most basic applications, one encounters polylogarithms of integer index, but in this paper (see the example of dissimilar forests in Section 4), the more general case of a real index ν is also needed.

Lemma 5 (Singularities of polylogarithms) *For any index $\nu \in \mathbb{C}$, the polylogarithm $\mathrm{Li}_\nu(z)$ is analytically continuable to the slit plane $\mathbb{C} \setminus \mathbb{R}_{\geq 1}$. If $\nu = m \in \mathbb{Z}_{\geq 1}$, the singular expansion of $\mathrm{Li}_m(z)$ near the singularity $z = 1$ is given by*

$$\begin{cases} \mathrm{Li}_m(z) \;=\; \dfrac{(-1)^m}{(m-1)!}\tau^{m-1}(\log \tau - H_{m-1}) + \displaystyle\sum_{j \geq 0, j \neq m-1} \frac{(-1)^j}{j!}\zeta(m-j)\tau^j \\ \tau \;:=\; -\log z \;=\; \displaystyle\sum_{\ell=1}^{\infty} \frac{(1-z)^\ell}{\ell}. \end{cases} \tag{7}$$

For ν not an integer, the singular expansion of $\mathrm{Li}_\nu(z)$ is

$$\mathrm{Li}_\nu(z) \sim \Gamma(1-\nu)\tau^{\nu-1} + \sum_{j \geq 0} \frac{(-1)^j}{j!}\zeta(\nu-j)\tau^j. \tag{8}$$

The representations are given as a *composition* of two explicit series. The expansions involve both the harmonic number H_m and the Riemann zeta function $\zeta(s)$ defined by

$$H_m = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m}, \qquad \zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

($\zeta(s)$, originally defined in the half-plane $\Re(s) > 1$, is analytically continuable to $\mathbb{C} \setminus \{1\}$ by virtue of its classical functional equation).

Proof.

First in the case of an integer index $m \in \mathbb{Z}_{\geq 2}$, since $\mathrm{Li}_m(z)$ is an iterated integral of $\mathrm{Li}_1(z)$, it is analytically continuable to the complex plane slit along the ray $[1, +\infty[$. By this device, its expansion at the singularity $z = 1$ can be determined, resulting in (7). (The representation in (7) is in fact exact and not merely asymptotic. It has been obtained by Zagier and Cohen in [27, p. 387], and is known to the symbolic manipulation system Maple.)

For ν not an integer, analytic continuation derives from a Lindelöf integral representation discussed by Ford in [16]. The singular expansion, valid in the slit plane, was established in [11] to which we refer for details. □

In the sequel, we also make use of smoothness properties of polylogarithms. Clearly, $\mathrm{Li}_k(z)$ is $\mathcal{C}^{k-2}$–smooth in the sense of Definition 3. A simple computation of coefficients shows that any sum

$$S_k(z) = \sum_{\ell \geq k} r(\ell)\left[\mathrm{Li}_\ell(z^\ell) - \mathrm{Li}_\ell(1)\right]$$

with $r(x)$ polynomially bounded in x, is $\mathcal{C}^{k-2}$–smooth. Many similar sums are encountered later, starting with those in Equations (24) and (26).

2 The hybrid method

The heart of the matter is the treatment of functions analytic in the open unit disc that can, at least partially, be "de-singularized" by means of log-power functions.

2.1 Basic technology

Our first theorem, which essentially relies on the Darboux technology, serves as a stepping stone towards the proof of our main statement, Theorem 2 below.

Theorem 1 *Let $f(z)$ be analytic in the open unit disc D, such that it admits a factorization $f = P \cdot Q$, with P, Q analytic in D. Assume the following conditions on P and Q, relative to a finite set of points $Z = \{\zeta_1, \dots, \zeta_m\}$ on the unit circle:*

- $\mathbf{C}_1$: *The "Darboux factor" $Q(z)$ is $\mathcal{C}^s$–smooth on the unit circle ($s \in \mathbb{Z}_{\geq 0}$).*
- $\mathbf{C}_2$: *The "singular factor" $P(z)$ is of global order $a \leq 0$ and admits, for some nonnegative integer t, a log-power expansion relative to Z, $P = \widetilde{P} + R$ (with $\widetilde{P}$ the log-power function and R the smooth term), that is of class $\mathcal{C}^t$.*

Assume also the inequalities (with $\lfloor x \rfloor$ the integer part function):

- $\mathbf{C_3}$: *$t \geq u_0 \geq 0$, where*

$$u_0 := \left\lfloor \frac{s + \lfloor a \rfloor}{2} \right\rfloor. \tag{9}$$

Let $c_0 = \left\lfloor \frac{s - \lfloor a \rfloor}{2} \right\rfloor$. If H denotes the Hermite interpolation polynomial[2] *such that all its derivatives of order $0, \dots, c_0 - 1$ coincide with those of Q at each of the points $\zeta_1, \dots, \zeta_m$, one has*

$$[z^n]f(z) = [z^n]\left(\widetilde{P}(z) \cdot H(z)\right) + o(n^{-u_0}). \tag{10}$$

Since $\widetilde{P}(z) \cdot H(z)$ is itself a log-power function, the asymptotic form of its coefficients is explicitly provided by Lemma 1.

Proof. Let $c \leq s$ be a nonnegative integer whose precise value will be adjusted at the end of the proof. First, we decompose Q as

$$Q = \overline{Q} + S,$$

where $\overline{Q}$ is the polynomial of minimal degree such that all its derivatives of order $0, \dots, c-1$ at each of the points $\zeta_1, \dots, \zeta_m$ coincide with those of Q:

$$\left.\frac{\partial^i}{\partial z^i}\overline{Q}(z)\right|_{z=\zeta_j} = \left.\frac{\partial^i}{\partial z^i}Q(z)\right|_{z=\zeta_j}, \qquad 0 \leq i < c, \quad 1 \leq j \leq m. \tag{11}$$

(If $c = 0$, we take $\overline{Q} = 0$.) The classical process of Hermite interpolation [21] produces such a polynomial, whose degree is at most $cm - 1$. Since $\overline{Q}$ is $\mathcal{C}^\infty$–smooth, the quantity

[2] Hermite interpolation extends the usual process of Lagrange interpolation, by allowing for higher contact between a function and its interpolating polynomial at a designated set of points. A lucid construction is found in Hildebrand's treatise [21, §8.2].

$S = Q - \overline{Q}$ is $\mathcal{C}^s$–smooth. This function S is also "flat", in the sense that it has a contact of high order with 0 at each of the points ζ_j.

We now operate with the decomposition

$$f = \widetilde{P} \cdot \overline{Q} + \widetilde{P} \cdot S + R \cdot Q, \tag{12}$$

and proceed to examine the coefficient of z^n in each term.

— *The product* $\widetilde{P} \cdot \overline{Q}$. Since $\widetilde{P}$ is a log-power function and $\overline{Q}$ a polynomial, the coefficient of z^n in the product admits, by Lemma 1, a complete descending expansion with terms in the scale $\{n^{-\beta}(\log n)^k\}$, which we write concisely as

$$[z^n]\widetilde{P} \cdot \overline{Q} \in \left\{ n^{-\beta}(\log n)^k \;\middle|\; k \in \mathbb{Z}_{\geq 0},\ \beta \in \mathbb{R} \right\}. \tag{13}$$

— *The product* $\widetilde{P} \cdot S$. This is where the Hermite interpolation polynomial $\overline{Q}$ plays its part. From the construction of $\overline{Q}$, there results that $S = Q - \overline{Q}$ has all its derivatives of order $0, \ldots, c-1$ vanishing at each of the points $\zeta_1, \ldots, \zeta_m$. This guarantees the existence of a factorization

$$S(z) \equiv Q(z) - \overline{Q}(z) = \kappa(z) \prod_{j=1}^{m} (z - \zeta_j)^c,$$

where $\kappa(z)$ is now $\mathcal{C}^{s-c}$–smooth (division decreases the degree of smoothness). Then, in the factorization

$$\widetilde{P} \cdot S = \left(\widetilde{P} \cdot \prod_{j=1}^{m} (z - \zeta_j)^c \right) \cdot \kappa(z),$$

the quantity $\widetilde{P}$ is, near a ζ_j, of order at most $O(z - \zeta_j)^a$ (with a the global order of P). Thus, $\widetilde{P}S/\kappa$ is at least $\mathcal{C}^v$–smooth, with $v := \lfloor c + a \rfloor$. Since $\mathcal{C}^p \cdot \mathcal{C}^q \subset \mathcal{C}^{\min(p,q)}$, Darboux's method (Lemma 3) yields

$$[z^n]\widetilde{P} \cdot S = o\left(n^{-u(c)}\right), \qquad u(c) := \min(\lfloor c + a \rfloor, s - c). \tag{14}$$

— *The product* $R \cdot Q$. This quantity is of class $\mathcal{C}^{\min(s,t)}$ and, by Darboux's method:

$$[z^n]R \cdot Q = o\left(n^{-\min(s,t)}\right). \tag{15}$$

It now only remains to collect the effect of the various error terms of (14) and (15) in the decomposition (12):

$$[z^n]f = \left([z^n]\widetilde{P} \cdot \overline{Q} \right) + o(n^{-u(c)}) + o(n^{-\min(s,t)}).$$

Given the condition $t \geq u_0$ in $\mathbf{C_3}$, the last two terms are $o(n^{-u_0})$. A choice, which maximizes $u(c)$ (as defined in (14)) and suffices for our purposes, is

$$c_0 = \left\lfloor \frac{s - \lfloor a \rfloor}{2} \right\rfloor \qquad \text{corresponding to} \qquad u(c_0) = \left\lfloor \frac{s + \lfloor a \rfloor}{2} \right\rfloor = u_0. \tag{16}$$

The statement then results from the choice of $c = c_0$, as well as $u_0 = u(c_0)$ and $H(z) := \overline{Q}(z)$, the corresponding Hermite interpolation polynomial. $\square$

2.2 Hybridization

Theorem 1 is largely to be regarded as an existence result: due to the factorization and the presence of a Hermite interpolation polynomial, it is not well suited for effectively deriving asymptotic expansions. In this subsection, we develop the hybrid method *per se*, which makes it possible to operate directly with a small number of radial expansions of the function whose coefficients are to be estimated.

Definition 6 *Let $f(z)$ be analytic in the open unit disc. For ζ a point on the unit circle, we define the* radial expansion *of f at ζ with order $t \in \mathbb{R}$ as the smallest (in terms of the number of monomials) log-power function $\sigma(z)$ at ζ, provided it exists, such that*

$$f(z) = \sigma(z) + O\left((z-\zeta)^t\right),$$

when $z = (1-x)\zeta$ and x tends to 0^+. The quantity $\sigma(z)$ is written

$$\operatorname{asymp}(f(z), \zeta, t).$$

The interest of radial expansions is to a large extent a computational one, as these are often accessible via common methods of asymptotic analysis while various series rearrangements from within the unit circle are granted by analyticity. In contrast, the task of estimating directly a function $f(z)$ as $z \to \zeta$ *on the unit circle* may be technically more demanding. Our main theorem is accordingly expressed in terms of such radial expansions and, after the necessary conditions on the generating function have been verified, it provides an *algorithm* (Equation (17)) for the determination of the asymptotic form of coefficients.

Theorem 2 (Hybrid method) *Let $f(z)$ be analytic in the open unit disc D and such that it admits a factorization $f = P \cdot Q$, with P, Q analytic in D. Assume the following conditions on P and Q, relative to a finite set of points $Z = \{\zeta_1, \ldots, \zeta_m\}$ on the unit circle:*

- $\mathbf{D}_1$*: The "Darboux factor" $Q(z)$ is $\mathcal{C}^s$–smooth on the unit circle ($s \in \mathbb{Z}_{\geq 0}$).*
- $\mathbf{D}_2$*: The "singular factor" $P(z)$ is of global order $a \leq 0$ and is analytically continuable to an indented domain of the form $\mathfrak{D} = \bigcap_{j=1}^m (\zeta_j \cdot \Delta)$. For some non-negative real number t_0, it admits, at any $\zeta_j \in Z$, an asymptotic expansion of the form*

$$P(z) = \sigma_j(z/\zeta_j) + O\left((z-\zeta_j)^{t_0}\right) \qquad (z \to \zeta_j,\ z \in \mathfrak{D}),$$

where $\sigma_j(z)$ is a log-power function at 1.

Assume also the inequalities:

- $\mathbf{D_3}$*: $t_0 > u_0 \geq 0$, where $u_0 := \lfloor \frac{s + \lfloor a \rfloor}{2} \rfloor$.*

Then f admits a radial expansion at any $\zeta_j \in Z$ with order u_0. The coefficients of $f(z)$ satisfy:

$$\begin{aligned} [z^n]f(z) \quad &= \quad [z^n]\mathbf{A}(z) + o\left(n^{-u_0}\right), \\ \textit{where} \qquad &\mathbf{A}(z) := \sum_{j=1}^{m} \operatorname{asymp}(f(z), \zeta_j, u_0). \end{aligned} \tag{17}$$

Proof. Let us denote by

$$\Sigma(z) = \sum_{j=1}^{m} \sigma_j(z/\zeta_j),$$

the sum of the singular parts of P at the points of ζ_j. The difference $R := P - \Sigma$ is $\mathcal{C}^t$-smooth for any integer t satisfying $t < t_0$ (in particular, we can choose $t = u_0$, this by assumption $\mathbf{D_2}$. The singular factor P has thus been re-expressed as the sum of a singular part Σ and a smooth part R. The conditions of Theorem 1 are then precisely satisfied by the product PQ, the inequality $\mathbf{D_3}$ implying condition $\mathbf{C_3}$, so that one has by (10)

$$[z^n]f(z) = [z^n]\Sigma(z)H(z) + o(n^{-u_0}), \tag{18}$$

where H is the Hermite polynomial associated with Q that is described in the proof of Theorem 1 and u_0 is given by (9).

In order to complete the proof, there remains to verify that, in the coefficient extraction process of (18) above, the quantity ΣH can be replaced by $\mathbf{A}(z)$.

We have

$$[z^n]\Sigma(z)H(z) = \sum_j [z^n]\sigma_j(z/\zeta_j)H(z). \tag{19}$$

Now, near each ζ_j, we have (with $c_0 = \left\lfloor \frac{s - \lfloor a \rfloor}{2} \right\rfloor$ according to (16))

$$\begin{aligned} \sigma_j(z/\zeta_j) \quad &= \quad P(z) + O((z-\zeta_j)^{t_0}) \\ H(z) \quad &= \quad Q(z) + O((z-\zeta_j)^{c_0}) \\ P(z) \quad &= \quad O((z-\zeta_j)^{a}), \end{aligned} \tag{20}$$

respectively by assumption $\mathbf{D_2}$, by the high order contact of H with Q due to the Hermite interpolation construction, and by the global order property of $P(z)$. There results from Equation (20), condition $\mathbf{D_3}$, and the value of c_0 in (16) that

$$\sigma_j(z/\zeta_j)H(z) = \operatorname{asymp}(P(z)Q(z), \zeta_j, u_0) + O((z-\zeta_j)^{u_0}),$$

The proof, given (18) and (19), is now complete. □

Thanks to Theorem 2, in order to analyse the coefficients of a function f, the following two steps are sufficient.

(i) Establish the *existence* of a proper factorization $f = P \cdot Q$. Usually, a crude analysis is sufficient for this purpose.

(*ii*) Analyse *separately* the asymptotic character of $f(z)$ as z tends radially to a few distinguished points, those of Z.

As asserted by Theorem 2, it then becomes possible to proceed with the analysis of the coefficients $[z^n]f(z)$ *as though* the function f satisfied the conditions of singularity analysis (whereas in general $f(z)$ admits the unit circle as a natural boundary).

Manstavičius [28] develops an alternative approach that requires conditions on generating functions in the disc of convergence, but only some weak smoothness on the circumference. His results are however not clearly adapted to deriving asymptotic expansions beyond the main terms.

3 Permutations with distinct cycle sizes

The function

$$f(z) := \prod_{k=1}^{\infty}\left(1+\frac{z^k}{k}\right),$$

has been studied by Greene and Knuth [19], in relation to a problem relative to factorization of polynomials over finite fields that we treat later. As is readily recognized from first principles of combinatorial analysis [15, 17, 36, 40], the coefficient $[z^n]f(z)$ represents *the probability that, in a random permutation of size n, all cycle lengths are distinct.* One has

$$f(z) = 1 + z + \frac{z^2}{2!} + 5\frac{z^3}{3!} + 14\frac{z^4}{4!} + 74\frac{z^5}{5!} + \cdots,$$

and the coefficients constitute the sequence **EIS:A007838**[3]. In [19, §4.1.6], the authors devote some seven pages (pp. 52–58) to the derivation of the estimate (γ is Euler's constant)

$$f_n := [z^n]f(z) = e^{-\gamma} + \frac{e^{-\gamma}}{n} + O\left(\frac{\log n}{n^2}\right), \tag{21}$$

starting with a Tauberian argument and repeatedly using bootstrapping. In our treatment below, we recycle some of their calculations, though our asymptotic technology is fundamentally different.

Global order. The first task in our perspective is to determine the global order of $f(z)$. The following chain of calculations,

$$\begin{aligned} f(z) &= \prod_{k=1}^{\infty} e^{z^k/k} \prod_{k=1}^{\infty}\left(1+\frac{z^k}{k}\right)e^{-z^k/k} \\ &= \frac{1}{1-z}\exp\left(\sum_{k=1}^{\infty}\log\left(1+\frac{z^k}{k}\right)-\frac{z^k}{k}\right) \\ &= \frac{1}{1-z}\exp\left(-\frac{1}{2}\sum_{k\geq 1}\frac{z^{2k}}{k^2}+\frac{1}{3}\sum_{k\geq 1}\frac{z^{3k}}{k^3}-\cdots\right), \end{aligned} \tag{22}$$

[3]We shall use the notation **EIS:xxxxxx** to represent a sequence indexed in *The On-Line Encyclopedia of Integer Sequences* [34].

shows $f(z)$ to be of global order -1. It is based on the usual introduction of convergence factors, the exp–log transformation ($X \equiv \exp(\log X)$), and finally the logarithmic expansion.

Note that this preliminary determination of global order only gives the useless bound $f_n = O(n)$. Actually, from the infinite product expression of the Gamma function [39] (or from a direct calculation, as in [19]), there results that

$$e^{-\gamma} = \prod_{k \geq 1} \left(1 + \frac{1}{k}\right) e^{-1/k}, \tag{23}$$

hence, from the second line of (22),

$$f(z) \underset{z \to 1^-}{\sim} \frac{e^{-\gamma}}{1 - z},$$

which is compatible with (21), but far from sufficient to imply it.

The hybrid method. The last line of (22), is re-expressed in terms of polylogarithms as

$$f(z) = \frac{1}{1 - z} \exp\left(-\frac{1}{2} \operatorname{Li}_2(z^2) + \frac{1}{3} \operatorname{Li}_3(z^3) - \cdots\right). \tag{24}$$

It proves convenient to adjust the expansion (24), by taking out the $(1 + z)$ factor: we find

$$f(z) = e^{-z} \frac{1 + z}{1 - z} \exp\left(\sum_{m \geq 2} \frac{(-1)^{m-1}}{m} \left[\operatorname{Li}_m(z^m) - z^m\right]\right), \tag{25}$$

The right factorization of $f(z)$ is obtained transparently. Define

$$U(z) := \sum_{1 \leq \ell \leq s+1} \frac{(-1)^{\ell-1}}{\ell} \left[\operatorname{Li}_\ell(z^\ell) - z^\ell\right], \qquad V(z) := \sum_{s+2 \leq \ell} \frac{(-1)^{\ell-1}}{\ell} \left[\operatorname{Li}_\ell(z^\ell) - z^\ell\right], \tag{26}$$

so that

$$f(z) = (1 + z) e^{U(z)} \cdot e^{V(z)}. \tag{27}$$

Clearly $V(z)$ is $\mathcal{C}^s$–smooth, and so is $e^{V(z)}$ given usual rules of differentiation. Thus $Q := e^V$ is our Darboux factor. The first factor $P := (1 + z)e^U$ satisfies the condition of Theorem 2: it is the singular factor and it can be expanded to any order t of smallness. Consequently, the hybrid method is applicable and can provide an asymptotic expansion of $[z^n]f(z)$ to any predetermined degree of accuracy.

The nature of the full expansion. Given the existence of factorizations of type (27) with an arbitrary degree of smoothness (for V) and smallness (for U), it is possible to organize the calculations as follows: take the primitive roots of unity in sequence, for orders $1, 2, 3, \ldots$. Given such a root η of order ℓ, each radial restriction admits a full asymptotic expansion in descending powers of $(1 - z/\eta)$ tempered by polynomials in $\log(1 - z/\eta)$. Such an expansion can be translated formally into a full expansion in powers of n^{-1} tempered by polynomials in $\log n$ and multiplied by η^{-n}. All the terms collected in this way are bound to occur in the asymptotic expansion of $f_n = [z^n]f(z)$.

For the sequel, we start the analysis with the expansion as $z \to 1$, then consider in turn $z = -1$, $z = \omega, \omega^2$ (with $\omega = \exp(2i\pi/3)$), and finally $z = \eta$, a primitive ℓth root of unity.

The expansion at $z = 1$. Calculations simplify a bit if we set

$$z = e^{-\tau}, \qquad \tau = -\log z,$$

as in (7). By summing the singular expansions of polylogarithms (7), one arrives at an asymptotic expansion as $\tau \to 0^+$ of the form:

$$f(e^{-\tau}) = e^{-e^{-\tau}} \frac{1+e^{-\tau}}{1-e^{-\tau}} \exp\left(-\alpha(\tau)\log\tau + \beta(\tau) + \delta_1(\tau) + \delta_2(\tau) - \epsilon(\tau)\right). \tag{28}$$

There, the first two terms in the exponential correspond to summing the special terms in the singular expansions of polylogarithms (7):

$$\alpha(\tau) := \sum_{m\geq 1} \frac{(m+1)^{m-1}\tau^m}{m!}, \qquad \beta(\tau) = \sum_{m\geq 1} \frac{(m+1)^{m-1}\tau^m}{m!}(H_m - \log(m+1)).$$

The last three terms inside the exponential of (28) arise from summation over values of $m \geq 2$ of the regular parts of the polylogarithms (cf (7)), namely,

$$\sum_{m\geq 2} \frac{(-1)^{m-1}}{m} \sum_{j\geq 0,\ j\neq m-1} \frac{(-1)^j}{j!}\left[\zeta(m-j)-1\right](m\tau)^j,$$

upon distinguishing between the three cases: $j > m-1$ (giving rise to $\delta_1(\tau)$), $j = m-1$ (giving $\epsilon(\tau)$), and $j < m-1$ (giving $\delta_2(\tau)$), and exchanging the order of summations. The calculation of $\epsilon(\tau)$ and $\delta_1(\tau)$ is immediate. First

$$\delta_1(\tau) = \sum_{j\geq 2} \delta_{1,j} \frac{(-\tau)^j}{j!}, \qquad \delta_{1,j} = \sum_{m=2}^{j} (-1)^{m-1} m^{j-1}(\zeta(m-j)-1), \tag{29}$$

and since ζ values at negative integers are rational numbers, the expansion of $\delta_1(\tau)$ involves only rational coefficients. Next, one finds

$$\epsilon(\tau) = \sum_{m\geq 1} (m+1)^{m-1} \frac{\tau^m}{m!},$$

a variant of the Lambert and Cayley functions. Finally, the function $\delta_2(\tau)$ has coefficients *a priori* given by sums like in (29), but with the summation extending to $m \geq j+2$:

$$\delta_2(\tau) = \sum_{j\geq 0} \delta_{2,j} \frac{(-\tau)^j}{j!}, \qquad \delta_{2,j} = \sum_{m\geq j+2} (-1)^{m-1} m^{j-1}(\zeta(m-j)-1).$$

Each infinite sum in the expansion of δ_2 is expressible in finite form: it suffices to start from the known expansion of $\psi(1+s)$ at $s=0$, which gives ($\psi(s)$ is the logarithmic derivative of the Gamma function)

$$\psi(1+s)+\gamma-\frac{s}{1+s}=(\zeta(2)-1)s-(\zeta(3)-1)s^2+\cdots, \tag{30}$$

and differentiate an arbitrary number of times with respect to s, then finally set $s=1$. One finds for instance, in this way,

$$\delta_{2,0}=-\gamma-\log 2+1, \quad \delta_{2,1}=\frac{1}{2}, \quad \delta_{2,2}=-\frac{1}{6}\pi^2-\frac{1}{4}.$$

Equation (28) provides a complete algorithm for expanding $f(z)$ as $z\to 1^-$. The first few terms found are

$$\begin{aligned} f(z) &= e^{-\gamma}\Bigg(\frac{1}{1-z}-\log(1-z)-\log 2+\frac{1}{2}(1-z)\log^2(1-z) \\ &\qquad +(\log 2-2)(1-z)\log(1-z)+O(1-z)\Bigg). \end{aligned}$$

Then, an application of Theorem 2 yields the terms in the asymptotic expansion of f_n arising from the singularity $z=1$:

$$\widehat{f}_n^{[1]}=e^{-\gamma}+\frac{e^{-\gamma}}{n}+\frac{e^{-\gamma}}{n^2}(-\log n+c_{2,0})+\frac{e^{-\gamma}}{n^3}(\log^2 n+c_{3,1}\log n+c_{3,0})+\cdots \tag{31}$$

where

$$\begin{aligned} &c_{2,0}=-1-\gamma+\log 2, \qquad c_{3,1}=4+2\gamma-2\log 2, \\ &c_{3,0}=1+4\gamma-\log 2-3\log 3+\log^2 2-\tfrac{\pi^2}{3}+\gamma^2-2\gamma\log 2. \end{aligned} \tag{32}$$

From preceding considerations, the coefficients all lie in the ring generated by $\log 2$, $\log 3,\ldots$, γ, π, and $\zeta(3),\zeta(5),\ldots$.

The terms given in (31) provide quite a good approximation. Figure 1 displays a comparison between f_n and its asymptotic approximation $\widehat{f}_n^{[1]}$, up to terms of order n^{-3}. We find

$$f_n=\widehat{f}_n^{[1]}\left(1+\frac{R_n}{n^3}\right), \qquad |R_n|\le 22,$$

for all $1\le n\le 1000$, and expect the bound to remain valid for all $n\ge 1$.

Expansions at $z=-1$ and at $z=\omega,\omega^2$. We shall content ourselves with brief indications on the shape of the corresponding singular expansions. Note that Figure 1 clearly indicates the presence of a term of the form

$$\frac{\Omega(n)}{n^3}$$

in the full asymptotic expansion of f_n, where $\Omega(n)$ is a function with period 6. This motivates an investigation of the behaviour of $f(z)$ near primitive square and cube roots of unity.

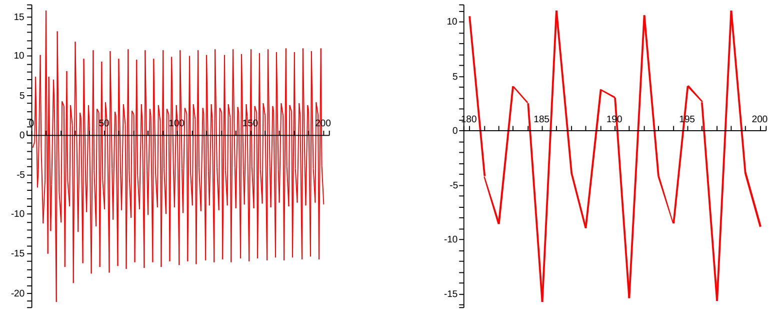

Figure 1: Permutations with distinct cycle lengths: the approximation error as measured by $n^3(f_n/\widehat{f}_n^{[1]} - 1)$, with $\widehat{f}_n^{[1]}$ truncated after n^{-3} terms, for $n = 1\,..\,200$ (left) and for $n = 180\,..\,200$ (right).

Start with $z \to -1^+$. The definition of $f(z)$ implies that

$$f(z) \underset{z\to -1^+}{\sim} (1+z)\prod_{k=2}^{\infty}\left(1+\frac{(-1)^k}{k}\right) = (1+z)$$

(the infinite product telescopes). Set $\mathcal{Z} = 1+z$ and restrict attention to the type of the expansions at $z=-1$. Only half of the polylogarithms in (25) are singular, so that the expansion at $z=-1$ is of the *type*

$$\mathcal{Z}\exp\left(\mathcal{Z}\log\mathcal{Z} + \mathcal{Z} + \mathcal{Z}^2 + \mathcal{Z}^3\log\mathcal{Z} + \cdots\right) = \mathcal{Z} + \mathcal{Z}^2\log\mathcal{Z} + \mathcal{Z}^2 + \mathcal{Z}^3\log^2\mathcal{Z} + \cdots.$$

There, we have replaced all unspecified coefficients by the constant 1 for readability. This singular form results in a contribution to the asymptotic form of f_n:

$$\widehat{f}_n^{[-1]} = (-1)^n\left(\frac{d_3}{n^3} + \frac{d_{4,1}\log n + d_{4,0}}{n^4} + \cdots\right).$$

(Compared to roots of unity of higher order, the case $z=-1$ is special, because of the factor $(1+z)$ explicitly present in the definition of $f(z)$.) A simple calculation shows that $d_3 = 2$, so that

$$\widehat{f}_n^{[-1]} \sim 2\frac{(-1)^n}{n^3}.$$

Next, let $\omega = e^{2i\pi/3}$ and set $\mathcal{Z} := (1 - z/\omega)$. The type of the expansion at $z=\omega$ is

$$\begin{aligned} f(z) &\sim f(\omega)\exp\left(\mathcal{Z} + \mathcal{Z}^2\log\mathcal{Z} + \mathcal{Z}^3 + \cdots\right) \\ &\sim f(\omega)\left(1 + \mathcal{Z} + \mathcal{Z}^2\log\mathcal{Z} + \mathcal{Z}^2 + \mathcal{Z}^3\log\mathcal{Z} + \mathcal{Z}^4\log^2\mathcal{Z} + \cdots\right), \end{aligned}$$

since now every third polylogarithm is singular at $z=\omega$. This induces a contribution of the form

$$\widehat{f}_n^{[\omega]} = \omega^{-n}\left(\frac{e_3}{n^3} + \frac{e_{4,1}\log n + e_{4,0}}{n^4} + \cdots\right),$$

arising from $z = \omega$, and similarly, for a conjugate contribution arising from ω^2. Another simple calculation shows that

$$e_3 = 3f(\omega),$$

and leaves us with the task of estimating $f(\omega)$. The use of the formula,

$$\prod_{k\geq 1}\left(1+\frac{s}{n+a}\right)e^{-s/n} = \frac{\Gamma(1+a)e^{-s\gamma}}{\Gamma(1+s+a)},$$

a mere avatar of the product formula for the Gamma function, yields then easily

$$f(\omega) = \frac{3\Gamma(\frac{2}{3})}{\Gamma(\frac{1}{3}+\frac{\omega}{3})\Gamma(\frac{2}{3}+\frac{\omega^2}{3})}.$$

The fluctuations of period 6 evidenced by Figure 1 are thus fully explained: one has

$$\widehat{f}_n^{[-1]} + \widehat{f}_n^{[\omega]} + \widehat{f}_n^{[\omega^2]} = \frac{\Omega(n)}{n^3} + O\left(\frac{\log n}{n^4}\right),$$

where the periodic function Ω is ($\Re$ designates a real part)

$$\Omega(n) = 2(-1)^n + 2\Re\left(\omega^{-n}\frac{9\Gamma(\frac{2}{3})}{\Gamma(\frac{1}{6}+\frac{i\sqrt{3}}{6})\Gamma(\frac{1}{2}-\frac{i\sqrt{3}}{6})}\right).$$

Expansions at $z = \eta$, a primitive ℓth root of unity. Let $\eta = \exp(2i\pi/\ell)$ and $\mathcal{Z} = (1 - z/\eta)$. The expansion of $f(z)$ is now of the type

$$f(z) \sim f(\eta)\exp\left(\mathcal{Z} + \cdots + \mathcal{Z}^{\ell-1}\log\mathcal{Z} + \mathcal{Z}^{\ell-1} + \cdots\right),$$

where $\mathcal{Z}^{\ell-1}\log\mathcal{Z}$ corresponds to the singular term in $\mathrm{Li}_\ell(z^\ell)$. Consequently, fluctuations start appearing at the level of terms of order $n^{-\ell}$ in the asymptotic expansion of f_n as $n \to +\infty$. The value of $f(\eta)$ is expressible in terms of Gamma values at algebraic points, as we have seen when determining $f(\omega)$. The coefficients in the expansion also involve values of the ψ-function ($\psi(s) = \frac{d}{ds}\log\Gamma(s)$) and its derivatives at rational points, which include ζ values as particular cases.

Proposition 1 *The probability that a permutation is made of cycles of distinct lengths admits a full asymptotic expansion of the form*

$$\begin{aligned} f_n \quad \sim \quad & e^{-\gamma} + \frac{e^{-\gamma}}{n} + \frac{e^{-\gamma}}{n^2}\left(-\log n - 1 - \gamma + \log 2\right) \\ & + \frac{1}{n^3}\left[e^{-\gamma}\left(\log^2 n + c_{3,1}\log n + c_{3,0}\right) + 2(-1)^n + 2\Re\left(\frac{9\Gamma(\frac{2}{3})\omega^{-n}}{\Gamma(\frac{1}{6}+\frac{i\sqrt{3}}{6})\Gamma(\frac{1}{2}-\frac{i\sqrt{3}}{6})}\right)\right] \\ & + \sum_{r\geq 4}\frac{P_r(n)}{n^r}, \end{aligned}$$

with $c_{3,1}$ and $c_{3,0}$ as given by (32)*. There, $P_r(n)$ is a polynomial of exact degree $r-1$ in $\log n$ with coefficients that are periodic functions of n with period $D(r) = \mathrm{lcm}(2,3,\ldots,r)$.*

Figure 2 displays the error of the approximation obtained by incorporating all terms till order n^{-3} included in the asymptotic expansion of f_n. Fluctuations of period 12 (due to the additional presence of $i = \sqrt{-1}$) start making an appearance.

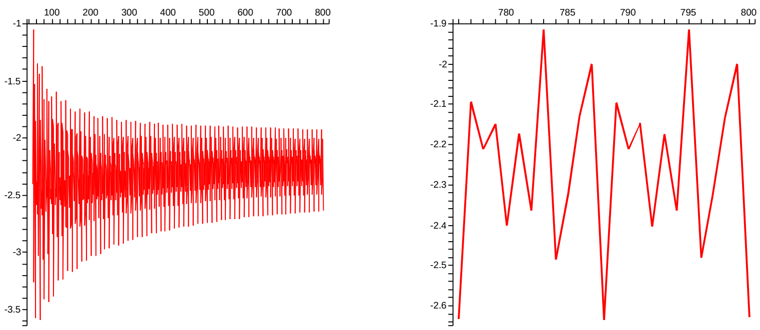

Figure 2: Permutations with distinct cycle lengths: the approximation error as measured by $n^4 \log^3 n(f_n/(\widehat{f}_n^{[1]} + \widehat{f}_n^{[-1]} + \widehat{f}_n^{[\omega]} + \widehat{f}_n^{[\omega^2]}) - 1)$, with the $\widehat{f}_n$ truncated after n^{-3} terms, for $n = 50\,..\,800$ (left) and for $n = 776\,..\,800$ (right).

4 Permutations, polynomials, and trees

We now examine several combinatorial problems related to permutations, polynomials over finite fields, and trees that are amenable to the hybrid method. The detailed treatment of permutations with distinct cycle lengths can serve as a beacon for the analysis of similar infinite product generating functions, and accordingly our presentation of each example will be quite succinct.

In the examples that follow, the function f whose coefficients are to be analysed is such that there is an increasing family of sets $Z^{(1)}, Z^{(2)}, \ldots$ (ordered by inclusion, and with elements being roots of unity), attached to a collection of asymptotic expansions having smaller and smaller error terms. In that case, a full asymptotic expansion is available for the coefficients of f. The general asymptotic shape of $[z^n]f$ involves standard terms of the form $n^{-p}\log^q n$ modulated by complex exponentials, since $[z^n]\sigma(z/\zeta) = \zeta^{-n}\sigma_n$. We formalize this notion by a definition.

Definition 7 *A sequence (f_n) is said to admit a* full asymptotic expansion with oscillating coefficients *if it is of the form*

$$f_n \sim \sum_{r\geq 0} \frac{P_r(n)}{n^{\alpha_r}} \qquad (n \to \infty),$$

where the exponents α_r increase to $+\infty$ and each $P_r(n)$ is a polynomial in $\log n$ whose coefficients are periodic functions of n.

In a small way, Proposition 1 and the forthcoming statements, Propositions 2–6, can be regarded as analogues, in the realm of functions of slow growth near the unit circle, of the Hardy-Ramanujan-Rademacher analysis [1, 2, 20] of partition generating functions, the latter exhibiting a very fast growth (being of infinite order) as $|z| \to 1$.

4.1 Permutations admitting an m-th root

The problem of determining the number of permutations that are squares or equivalently "have a square root" is a classical one of combinatorial analysis: see Wilf's vivid account in [40, §4.8]. The problem admits an obvious generalization. We shall let $\Pi_m(z)$ be the exponential generating function of permutations that are mth powers or, if one prefers, admit an mth root.

How many permutations have square roots? For the generating function Π_2, we follow Wilf's account. Upon squaring a permutation τ, each cycle of even length of τ falls apart into two cycles of half the length, while an odd cycle gives rise to a cycle of the same length. Hence, if σ has a square root, then the number of cycles it has of each even length must be even. By general principles of combinatorial analysis, the exponential generating function of the number $\Pi_{2,n}$ of permutations of n elements that have square roots satisfies

$$\begin{aligned}
\Pi_2(z) := \sum_{n\geq 0} \Pi_{2,n} \frac{z^n}{n!} &= e^z \cosh(z^2/2) e^{z^3/3} \cosh(z^4/4) e^{z^5/5} \cdots \\
&= \exp\left(\frac{1}{2}\log\frac{1+z}{1-z}\right) \prod_{m\geq 1} \cosh\left(\frac{z^{2m}}{2m}\right) \\
&= \sqrt{\frac{1+z}{1-z}} \prod_{m\geq 1} \cosh\left(\frac{z^{2m}}{2m}\right).
\end{aligned} \tag{33}$$

The series starts as

$$\Pi_2(z) = 1 + z + \frac{z^2}{2!} + 3\frac{z^3}{3!} + 12\frac{z^4}{4!} + 60\frac{z^5}{5!} + 270\frac{z^6}{6!} + \cdots,$$

its coefficients being **EIS:A003483**, with the quantity $[z^n]\Pi_2(z)$ representing the probability that a permutation is a square. The GF of (33) is given by Bender [3, p. 510] who attributes it to Blum [5]. It is interesting to note that Bender mentions the following estimate from [5],

$$[z^n]\Pi_2(z) \sim \frac{2}{\sqrt{\pi n}} e^G, \tag{34}$$

and derives it by an application of the Tauberian theorem[4] of Hardy, Littlewood, and Karamata. Accordingly, no error terms are available, given the nonconstructive character of classical Tauberian theory. We state:

Proposition 2 *The probability that a random permutation of size n has a square-root admits a full asymptotic expansion with oscillating coefficients. In particular, it satisfies*

$$[z^n]\Pi_2(z) \sim \sqrt{\frac{2}{\pi n}} e^G \left[1 - \frac{\log n}{n} + \frac{c_3 + (-1)^n}{4n}\right] - \frac{2e^G(-1)^{\lfloor n/2 \rfloor}}{n^2} + O\left(\frac{\log n}{n^{5/2}}\right), \tag{35}$$

[4] Regarding Tauberian side conditions, Bóna, McLennan, and White [6] prove by elementary combinatorial arguments that the sequence $\Pi_{2,n}$ is monotonically nonincreasing in n.

where

$$\begin{cases} e^G & = \displaystyle\prod_{k\geq 1} \cosh\left(\frac{1}{2k}\right) & \doteq \quad 1.22177\,95151\,92536 \\ c_2 & = \displaystyle\sum_{k\geq 1}\left(\frac{1}{2k} - \tanh\left(\frac{1}{2k}\right)\right), & c_3 = -12 + 16\log 2 + 4\gamma + 2c_2. \end{cases} \tag{36}$$

PROOF. First a rough analysis suffices to see that

$$\Pi_2(z) \underset{z\to 1}{\sim} \sqrt{\frac{2}{1-z}}e^G \qquad \text{and} \qquad \Pi_2(z) \underset{z\to -1}{\sim} \sqrt{\frac{1+z}{2}}e^G.$$

In order to refine these expansions, introduce the normalized tangent numbers by

$$\tan z = \sum_{m\geq 0} \tau_m z^{2m+1}, \qquad \text{so that} \quad \log\cos(z) = \sum_{m\geq 1} \tau_{m-1}\frac{z^{2m}}{2m}.$$

The usual exp-log reorganization of the Π_2 series yields

$$\Pi_2(z) = \sqrt{\frac{1+z}{1-z}}\exp\left(\sum_{m\geq 1}\frac{(-1)^{m-1}}{m2^{2m+1}}\tau_{m-1}\operatorname{Li}_{2m}\left(z^{4m}\right)\right).$$

In passing, this provides for G, the fast convergent series

$$G = \sum_{m\geq 1}\frac{(-1)^{m-1}}{m2^{2m+1}}\tau_{m-1}\zeta(2m),$$

on which the numerical estimate of (36) is based.

Next, take out the e^G factor, leading to

$$\Pi_2(z) = e^G\sqrt{\frac{1+z}{1-z}}\exp\left(\sum_{m\geq 1}\frac{(-1)^{m-1}}{m2^{2m+1}}\tau_{m-1}\left[\operatorname{Li}_{2m}\left(z^{4m}\right) - \zeta(2m)\right]\right). \tag{37}$$

At $z = 1$, the largest singular term in the exponential arises from $\operatorname{Li}_2(z^4)$, the contributions from the other polylogarithms being of smaller order

$$\Pi_2(z) \underset{z\to 1}{\sim} e^G\sqrt{\frac{2}{1-z}}\left(1 + 2(1-z)\log(1-z) + c^\star(1-z) + O\left((1-z)^2\log^2(1-z)\right)\right),$$

where, here and later, $c^\star$ designates a computable constant that we leave unspecified for the purpose of readability. Similarly, at $z = -1$, we find

$$\Pi_2(z) \underset{z\to -1}{\sim} e^G\sqrt{\frac{1+z}{2}}\left(1 + O\left((1+z)\log(1+z)\right)\right).$$

At $z = i = \sqrt{-1}$ (hence at $z = -i$, by conjugacy), we have

$$\Pi_2(z) \underset{z\to i}{\sim} \frac{1+i}{2} \left(P^\star(1-z/i) + 2(1-z/i)\log(1-z/i) + O((1-z/i)^{3/2})\right),$$

with $P^\star$ an unspecified polynomial that does not leave a trace in the coefficients' expansion.

The singular contribution to Π_2 arising from any root of unity ζ of order ≥ 8 is at most $O\left((1-z/\zeta)^3 \log(1-z/\zeta)\right)$, which translates to an $O(n^{-4})$ term. The proof of (35) is then completed upon making $c^\star$ in the expansion at 1 explicit, which introduces the new constants c_2, c_3. Existence of the full expansions finally follows from the usual analysis of polylogarithms of powers, taken at roots of unity. $\square$

How many permutations have an mth root? Like the previous one, this problem is briefly mentioned in Bender's survey [3]. We follow again Wilf's exposition [40, §4.8]. For a pair ℓ, m of positive integers, we define $(\!(\ell, m)\!)$ to be

$$(\!(\ell, m)\!) := \lim_{j\to\infty} \gcd(\ell^j, m).$$

(Thus, $(\!(\ell, m)\!)$ gathers from the prime decomposition of m all the factors that involve a prime divisor of ℓ.) The characterization of permutations that are mth powers then generalizes [3, 32, 37, 40]: a permutation has an mth root if and only if, for each $\ell = 1, 2, \ldots$, it is true that the number of cycles of length ℓ is a multiple of $(\!(\ell, m)\!)$. This observation leads to an expression for the corresponding generating function. Indeed, define the "sectioned exponential",

$$\exp_d(z) := \sum_{n\geq 0} \frac{x^{dn}}{(dn)!} = \frac{1}{d}\sum_{j=0}^{d-1} \exp\left(e^{2ij\pi/d} z\right),$$

so that $\exp_1(z) = e^z$ and $\exp_2(z) = \cosh(z)$. The exponential generating function of permutations that are mth powers is then

$$\Pi_m(z) = \prod_{\ell=1}^{\infty} \exp_{(\!(\ell,m)\!)}\left(\frac{z^\ell}{\ell}\right). \tag{38}$$

The generating function of (38) has been investigated by Pouyanne [32], whose paper provides the first order asymptotic estimate of $[z^n]\Pi_m$. There is a fundamental factorization,

$$\Pi_m(z) = A_m(z) \cdot B_m(z), \tag{39}$$

where A_m gathers from the product (38) the numbers ℓ that are relatively prime to m and $B(z)$ gathers the rest.

The factor A_m is found by series rearrangements to be an algebraic function expressible by radicals,

$$A_m(z) = \prod_{k \mid m} (1-z^k)^{-\mu(k)/k},$$

with $\mu(k)$ the Möbius function. For $m=2$ (square permutations), this is the ubiquitous prefactor $A_2(z)=\sqrt{(1+z)/(1-z)}$. For $m=6$, for instance, the prefactor becomes

$$A_6(z)=\left(\frac{1+z}{1-z}\right)^{1/3}\left(\frac{1+z+z^2}{1-z+z^2}\right)^{1/6}.$$

The factor B_m is a transcendental function that admits the unit circle as a natural boundary [32]. It is expressible as an infinite product of sectioned exponentials:

$$B_m(z)=\prod_{\substack{\ell=1\\ \gcd(\ell,m)>1}}^{\infty}\exp_{(\!(\ell,m)\!)}\left(\frac{z^\ell}{\ell}\right). \tag{40}$$

For $m=2$, this is the infinite product of hyperbolic cosines. For $m=6$, one has

$$B_6(z)=\prod_{\ell\equiv 0\bmod 6}\exp_6\left(\frac{z^\ell}{\ell}\right)\prod_{\ell\equiv 2,4\bmod 6}\exp_2\left(\frac{z^\ell}{\ell}\right)\prod_{\ell\equiv 3\bmod 6}\exp_3\left(\frac{z^\ell}{\ell}\right).$$

These singular factors can be analysed just like in the case of Π_2 by an exp-log transformation. One first observes that the limit value $B_m(1)$ is well defined, since the infinite product converges at least as fast as $\prod(1+\ell^{-2})$. It is seen next that singularities are at roots of unity, and the radial expansions can be computed in the usual way from the polylogarithmic expansion. We can now state a (somewhat minor) improvement over [32]:

Proposition 3 *The probability that a random permutation of size n has an mth root admits a full asymptotic expansion with oscillating coefficients. To first asymptotic order, it satisfies*

$$[z^n]\Pi_m(z)\sim\frac{\varpi_m}{n^{1-\varphi(m)/m}},\qquad \varpi_m:=\frac{B_m(1)}{\Gamma(\varphi(m)/m)}\prod_{k\,\mid\,m}k^{-\mu(k)/k},$$

where $\varphi(m)$ is the Euler totient function and

$$B_m(1)=\prod_{\substack{\ell=1\\ \gcd(\ell,m)>1}}^{\infty}\exp_{(\!(\ell,m)\!)}\left(\frac{1}{\ell}\right). \tag{41}$$

In particular, when $m=p$ is a prime number, one has

$$[z^n]\Pi_p(z)\sim\frac{\varpi_p}{n^{1/p}},\qquad \varpi_p:=\frac{p^{1/p}}{\Gamma(1-1/p)}\prod_{\ell=1}^{\infty}\exp_p\left(\frac{1}{\ell p}\right). \tag{42}$$

For instance, we find:

$$[z^n]\Pi_6(z)=B_6(1)\left[\frac{\sqrt[6]{12}}{\Gamma(\frac13)}n^{-2/3}+\frac{2\sqrt[12]{12}}{\Gamma(\frac16)}\Re\left(e^{-i\frac{\pi}{3}(n+\frac14)}\right)n^{-5/6}+O\left(\frac1n\right)\right],$$

and (42) improves upon an early estimate of Turán [37, Th. IV].

4.2 Pairs of permutations having the same cycle type

Given a permutation σ, its *cycle type* is the (unordered) multiset formed with the lengths of the cycles entering its decomposition into cycles. For a permutation of size n, this type can be equivalently represented by a partition of the integer n: for instance $(2^3, 5, 7^2)$ represents the profile of any permutation of size 25 that has three cycles of length 2, one cycle of length 5, and two cycles of length 7. The probability a_π that a random permutation of size n has profile

$$\pi = (1^{n_1}, 2^{n_2}, \ldots), \qquad \text{with} \quad 1n_1 + 2n_2 + \cdots = n$$

is, by virtue of a well-known formula [8, p. 233],

$$a_\pi = \prod_{i\geq 1} \frac{1}{i^{n_i} n_i!},$$

corresponding to the generating function in infinitely many variables

$$\Phi(z; x_1, x_2, \ldots) = \exp\left(x_1 z + x_2 \frac{z^2}{2} + x_3 \frac{z^3}{3} + \cdots\right), \tag{43}$$

which is such that $a_\pi = [z^n x_1^{n_1} x_2^{n_2} \cdots]\Phi$.

In this subsection, we estimate *the probability that two permutations of size n taken uniformly and independently at random have the same cycle type.* (Each pair of permutations is taken with probability $1/n!^2$.) The quantity to be estimated is thus

$$W_n = \sum_{\pi \vdash n} \left(a_\pi\right)^2,$$

where the summation ranges over all partitions $\pi = (1^{n_1}, 2^{n_2}, \ldots)$ of n. This problem was suggested to the authors by the reading of a short note of Wilf [41], who estimated the probability that two permutations have the same number of cycles (the answer to the latter question turns out to be asymptotic to $1/(2\sqrt{\pi \log n})$).

Given (43), it is not hard to find the generating function of the sequence (W_n):

$$W(z) := \sum_{n\geq 0} W_n z^n = \prod_{k=1}^{\infty} I\left(\frac{z^k}{k^2}\right) \qquad \text{where} \quad I(z) = \sum_{n\geq 0} \frac{z^n}{n!^2}, \tag{44}$$

the reason being that

$$W(z) = \sum_{n\geq 0} \sum_{\pi \vdash n} \frac{z^{n_1+2n_2+\cdots}}{\prod_i i^{2n_i} n_i!^2} = \prod_{i\geq 1} \left(\sum_{n_i\geq 0} \frac{z^{in_i}}{i^{2n_i} n_i!^2} \right).$$

The function written $I(z)$, which is obviously entire, is a variant of the Bessel function I_0 (see, e.g., [39]): $I(z) = I_0(2\sqrt{z})$. Also, from (44), the expansion of $W(z)$ is readily computed: one has

$$W(z) = 1 + z + 2\frac{z^2}{2!^2} + 14\frac{z^3}{3!^2} + 146\frac{z^4}{4!^2} + 2602\frac{z^5}{5!^2} + \cdots,$$

where the coefficients are **EIS:A087132** ("sum of the squares of the sizes of conjugacy classes in the symmetric group $\mathfrak{S}_n$").

Proposition 4 *The probability W_n that two permutations of size n have the same cycle type satisfies*

$$W_n = \frac{W(1)}{n^2} + O\left(\frac{\log n}{n^3}\right), \qquad W(1) = \prod_{k\geq 1} I\left(\frac{1}{k^2}\right) \doteq 4.26340\,35141\,52669. \tag{45}$$

Furthermore, this probability admits a full asymptotic expansion with oscillating coefficients.

Proof. We shall only sketch the analysis of the dominant asymptotic term, the rest being by now routine. From the expression of $W(z)$, the exp-log transformation yields

$$W(z) = \exp\left(\sum_{k\geq 1} H\left(\frac{z^k}{k^2}\right)\right) \qquad \text{where} \quad H(z) := \log\left(I(z)\right).$$

Let $h_\ell = [z^\ell]H(z)$, that is, $H(z) = \sum_\ell h_\ell z^\ell = z - \frac{1}{4}z^2 + \cdots$ (the sequence $(h_\ell \ell!^2)$ is **EIS:A002190**, which occurs in the enumeration of certain pairs of permutations by Carlitz). Then

$$W(z) = \exp\left(\sum_{k\geq 1}\sum_{\ell\geq 1} h_\ell \frac{z^{k\ell}}{k^{2\ell}}\right) = \exp\left(\sum_{\ell\geq 1} h_\ell \mathrm{Li}_{2\ell}(z^\ell)\right).$$

This expression ensures that the hybrid method can be applied at any order, with $W(z)$ being of global order $a = 0$. The first term of the asymptotic estimate is provided by the factorization relative to $Z = \{1, -1\}$, namely $W(z) = P(z)Q(z)$, with

$$P(z) = \exp\left(\mathrm{Li}_2(z) - \frac{1}{4}\mathrm{Li}_4(z^2)\right), \qquad Q(z) = \exp\left(\sum_{\ell\geq 3} h_\ell \mathrm{Li}_{2\ell}(z^\ell)\right).$$

Since $Q(z)$ is clearly $\mathcal{C}^4$ on the closed unit disk, the hybrid method applies: with the notations of Theorem 2, one can take $s = 4$, to the effect that $u_0 = 2$. Using the algorithmic scheme of Section 3, we find

$$\begin{aligned} W(z) &\underset{z\to 1^-}{=} W(1)\left[1 - (1-z)L + \frac{1}{2}(1-z)^2 L + \frac{1}{2}(1-z)^2 L^2 + O((1-z)^2)\right] \\ W(z) &\underset{z\to -1^+}{=} W(-1)\left[1 + O((1+z)^2)\right], \end{aligned}$$

with $L \equiv L(z) = \log(1-z)^{-1}$. Theorem 2 then directly yields $W_n \sim W(1)/n^2$, and further asymptotic terms can easily be extracted. $\square$

Regarding other statistics on *pairs* of permutations, it is well worth mentioning Dixon's recent study of the probability that two randomly chosen permutations generate a transitive group [9]. For the symmetric group $\mathfrak{S}_n$, this probability is found to be asymptotic to

$$1 - \frac{1}{n} - \frac{1}{n^2} - \frac{4}{n^3} - \frac{23}{n^4} - \cdots$$

and, up to exponentially smaller order terms, this expansion also gives the probability that two random permutations generate the whole symmetric group. In that case, the analytic engine is Bender's theory of coefficient extraction in divergent series [3].

4.3 Factorizations of polynomials over finite fields

Factoring polynomials in $\mathbb{Q}[X]$ is a problem of interest in symbolic computation, as it has implications in the determination of partial fraction expansions and symbolic integration, for instance. Most of the existing algorithms proceed by a reduction to a few factorizations of polynomials with coefficients in some finite field $\mathbb{F}_q$ (with q a prime power): see the books by Berlekamp, Knuth, or von zur Gathen and Gerhard [4, 38, 26]. Several of the algorithms for factoring polynomials over finite fields involve what is known as the *distinct degree factorization*. To wit, let $\phi \in \mathbb{F}_q[X]$ be completely factored as

$$\phi = \prod_j \iota_j^{n_j},$$

where the ι_j are distinct irreducible polynomials. The distinct degree factorization produces the decomposition of the square-free part of ϕ under the form

$$\text{squarefree}(\phi) = \beta_1 \beta_2 \cdots \beta_n, \qquad \text{where} \quad \beta_k = \prod_{\deg(\iota_j)=k} \iota_j \, .$$

We refer to the paper [13] by three of us for details.

The distinct degree factorization of ϕ as defined above coincides with the complete factorization of ϕ if and only if ϕ has all its irreducible factors of different degrees. For the purpose of analysis of algorithms, it is then of interest to quantify the probability of that event. This problem has been considered independently by the authors of [12, 13] and by Knopfmacher & Warlimont in [24].

First, without loss of generality, we restrict attention to monic polynomials. If q is the cardinality of the base field $\mathbb{F}_q$, the number of monic polynomials of degree n is $P_n = q^n$, with ordinary generating function

$$P(z) = \sum_{n \geq 0} q^n z^n = \frac{1}{1 - qz}.$$

The unique factorization property implies that the class $\mathcal{P}$ of all (monic) polynomials is isomorphic to the class obtained by applying the Multiset construction to the class $\mathcal{I}$ of (monic) irreducible polynomials. This, by well known principles of combinatorial analysis [4, 15] translates to an equation binding the generating function $I(z)$ of irreducible polynomials, namely,

$$P(z) = \prod_{n=1}^{\infty} (1 - z^n)^{-I_n} = \exp\left(I(z) + \frac{1}{2} I(z^2) + \frac{1}{3} I(z^3) + \cdots \right), \tag{46}$$

where I_n is the number of monic irreducible polynomials of degree n. The solution is obtained by taking a logarithm of the second form and applying Möbius inversion:

$$I(z) = \sum_{k \geq 1} \frac{\mu(k)}{k} \log \frac{1}{1 - qz^k}, \tag{47}$$

and, as a consequence, the number I_n admits the explicit formula (already known to Gauß, see references in [13, p. 46]):

$$I_n = \frac{1}{n} \sum_{k \ | \ n} \mu(k) q^{n/k} = \frac{q^n}{n} + R_n \quad \text{where} \quad |R_n| \le q^{n/2}. \tag{48}$$

In passing this approach also shows that

$$I(z) = \log \frac{1}{1 - qz} + R(z),$$

where $R(z)$ is analytic in $|z| < q^{-1/2}$, so that $I(z)$ has a logarithmic singularity at $z = q^{-1}$.

Let D_n be the number of (monic) polynomials composed of irreducible factors of distinct degrees. The corresponding generating function, $D(z)$ satisfies

$$D(z) = \prod_{n=1}^{\infty} \left(1 + I_n z^n\right), \tag{49}$$

and the probability of the event over polynomials of degree n is

$$\frac{D_n}{q^n} = [z^n]\, D\left(zq^{-1}\right).$$

It is in fact the simplification of this problem for fields of large cardinalities that originally led Greene and Knuth to consider the problem of enumerating permutations with distinct cycle lengths (see [13] for context). We have:

Proposition 5 *The probability that a random polynomial of degree n over $\mathbb{F}_q$ has all its irreducible factors of distinct degrees satisfies the asymptotic estimate*

$$\frac{D_n}{q^n} = \delta(q) + O\left(\frac{1}{n}\right), \tag{50}$$

where the constant $\delta(q)$ is given by

$$\delta(q) = \prod_{k \ge 1} \left(1 + \frac{I_k}{q^k}\right) (1 - q^{-k})^{I_k}. \tag{51}$$

In addition, this probability admits a full asymptotic expansion with oscillating coefficients.

Proof. We start with a rough analysis based on comparing $D(z)$ and $P(z)$. The second form of (46) implies

$$\frac{D(z/q)}{P(z/q)} = \prod_{n \ge 1} \left(1 + I_n q^{-n} z^n\right) (1 - z^n q^{-n})^{I_n}. \tag{52}$$

At $z=1$, the general factor in the product satisfies, for large n,

$$\begin{aligned}(1+I_nq^{-n})(1-q^{-n})^{I_n} &= \left(1+\frac{1}{n}+O(q^{-n/2})\right)\exp\left(-\frac{1}{n}+O(q^{-n/2})\right) \\ &= 1+\frac{1}{2n^2}+O(n^{-3}),\end{aligned} \tag{53}$$

given the known form (48) of I_n. This is enough to ensure the convergence of the infinite product defining $\delta(q)$ and proves that

$$D\left(\frac{z}{q}\right) \sim \frac{\delta(q)}{1-z} \qquad (z \to 1^-),$$

which is evidently compatible with the asserted estimate (50). Also, the estimate (53) points to the fact that convergence of the infinite product giving $\delta(q)$ is very slow, but also suggests the modified scheme (compare with (23)),

$$\delta(q) = e^{-\gamma}\prod_{k\geq 1}\left(\frac{1+I_kq^{-k}}{1+1/k}(1-q^{-k})^{I_k}e^{1/k}\right). \tag{54}$$

which now exhibits geometric convergence.

In order to complete the derivation of (50), we apply the exp-log transformation to (49):

$$D\left(\frac{z}{q}\right) = \exp\left(\sum_{m\geq 1}\frac{(-1)^{m-1}}{m}\Lambda_m(z)\right), \qquad \Lambda_m(z) := \sum_{n\geq 1}\left(I_nq^{-n}z^n\right)^m. \tag{55}$$

Also, we have $\Lambda_1(z) = I(z/q)$. Taking out the factor $e^{\Lambda_1(z)} = e^{I(z/q)}$ gives

$$\begin{aligned}D(\frac{z}{q}) &= e^{I(z/q)}\cdot\exp\left(\sum_{m\geq 2}\frac{(-1)^{m-1}}{m}\Lambda_m(z)\right) \\ &= \frac{1}{1-z}\exp\left(\sum_{k\geq 2}\frac{\mu(k)}{k}\log\frac{1}{1-q^{1-k}z^k}\right)\exp\left(\sum_{m\geq 2}\frac{(-1)^{m-1}}{m}\Lambda_m(z)\right) \\ &= \frac{e^{A(z)}}{1-z}\exp\left(\sum_{m\geq 2}\frac{(-1)^{m-1}}{m}\Lambda_m(z)\right),\end{aligned} \tag{56}$$

where $A(z)$ is analytic in $|z| < q^{1/2}$.

Next, we observe from (48) that

$$\Lambda_m(z) = \mathrm{Li}_m(z^m) + S_m(z),$$

where $S_m(z)$ is analytic in $|z| < q^{1/2}$. The existence of a factorization fulfilling the conditions of Theorem 2 now follows from the usual split of the sum in the exponential of (56), last line:

$$\sum_{m\geq 2}\frac{(-1)^{m-1}}{m}\Lambda_m(z) = \sum_{m=2}^{M}\frac{(-1)^{m-1}}{m}\Lambda_m(z) + \sum_{m\geq M}\frac{(-1)^{m-1}}{m}\Lambda_m(z).$$

The first split sum is singular at roots of unity of order $\leq M$ and admits a log-power expansion of type $\mathcal{O}^t$ for any t; the second split sum has its nth coefficient that is of order $O(n^{-M-1})$, and is accordingly $\mathcal{C}^{M-1}$. By Theorem 2, these considerations imply that $[z^n]D(z/q)$ admits a full asymptotic expansion with oscillating coefficients.

It is not hard then to track the order of the term that corrects the dominant asymptotic regime: in essence, it arises from the factor

$$\frac{1}{1-z}e^{-\frac{1}{2}\operatorname{Li}_2(z^2)},$$

whose coefficients are $O(n^{-1})$. $\square$

A variant of this problem is also considered in [13, 24]: *determine the probability that a random polynomial of degree n is such that its square-free factorization consists of polynomials of distinct degrees.* The generating function is then

$$\widehat{D}(z) = \prod_{n\geq 1}\left(1+\frac{I_n z^n}{1-z^n}\right).$$

By devices entirely similar to those employed in the proof of Proposition 5, one finds that the corresponding probability satisfies

$$\frac{\widehat{D}_n}{q^n} = \widehat{\delta}(q) + O\left(\frac{1}{n}\right),$$

where the constant $\widehat{\delta}(q)$ is

$$\widehat{\delta}(q) = \prod_{k\geq 1}\left(1+\frac{I_k}{q^k-1}\right)(1-q^{-k})^{I_k} = e^{-\gamma}\prod_{k\geq 1}\left(\frac{1+I_k/(q^k-1)}{1+1/k}(1-q^{-k})^{I_k}e^{1/k}\right).$$

The treatment of [13] is based on a crude application of the hybrid method, that of [24] relies on elementary bounds and coefficient manipulations, but it is not clearly applicable to derive asymptotic expansions beyond the first term.

4.4 Dissimilar forests

Fix a class $\mathcal{T}$ of rooted trees. An unordered forest is a multiset of trees in $\mathcal{T}$, and we let $\mathcal{F}$ be the class of all forests. A forest is said to be *dissimilar* if all the trees that it contains are of different sizes. We let $\mathcal{E}$ denote the class of dissimilar forests.

For instance, the collection $\mathcal{T}$ of all plane trees has generating function

$$T(z) = \frac{1-\sqrt{1-4z}}{2}; \tag{57}$$

a well-known fact [15, 17, 25, 35, 40]. The generating function of unordered forests is given by a construction analogous to (46):

$$\begin{aligned} F(z) &= \prod_{n\geq 1}(1-z^n)^{-T_n} \quad = \quad \exp\left(\sum_{k=1}^{\infty}\frac{1}{k}T(z^k)\right) \\ &= 1+z+2z^2+4z^3+10z^4+26z^5+77z^6+235z^7+\cdots \end{aligned}$$

(the coefficients constitute **EIS:A052854**). The generating function of dissimilar forests, which is our actual object of study, is

$$\begin{aligned} E(z) &= \prod_{n=1}^{\infty}(1+T_nz^n) \\ &= 1+z+z^2+3z^3+7z^4+21z^5+63z^6+203z^7+\cdots \end{aligned}$$

(currently unlisted in [34]).

The coefficients $[z^n]T(z)$ are the famous Catalan numbers of combinatorial theory,

$$T_n = \frac{1}{n}\binom{2n-2}{n-1} \sim \frac{4^{n-1}}{\sqrt{\pi n^3}}.$$

the asymptotic estimate being in agreement with the square-root singularity that is visible in $T(z)$. An easy analysis of $F(z)$ then shows that, as $z \to \frac{1}{4}$,

$$\begin{aligned} F(z) &= K - \frac{1}{2}K\sqrt{1-4z}+\cdots \\ K &:= \exp\left(\sum_{k=1}^{\infty}\frac{1}{2k}\left(1-\sqrt{1-4^{1-k}}\right)\right) \doteq 1.71603\,05349\,22281, \end{aligned} \tag{58}$$

resulting in the estimate

$$F_n \sim K\frac{4^{n-1}}{\sqrt{\pi n^3}}.$$

Proposition 6 *The probability that a random forest of rooted plane trees having total size n is dissimilar is asymptotic to the constant*

$$\kappa = \frac{e^{L+1/2}}{K} \qquad \textit{with} \quad L := \sum_{m=2}^{\infty}\frac{(-1)^{m-1}}{m}\sum_{n\geq 1}\left(\frac{1}{n}\binom{2n-2}{n-1}4^{-n}\right)^m. \tag{59}$$

This probability admits a complete asymptotic expansion with oscillating coefficients.

PROOF. We limit the calculation to first order asymptotics. As usual, start from the exp-log trick, which yields

$$E(z) = e^{T(z)}\exp\left(\sum_{m=2}^{\infty}\frac{(-1)^{m-1}}{m}\Lambda_m(z)\right), \tag{60}$$

where the functions Λ_m that play the rôle of special polylogarithms are defined by

$$\Lambda_m(z) := \sum_{n\geq 1} \left(\frac{1}{n} \binom{2n-2}{n-1} z^n \right)^m . \tag{61}$$

Observe that the functions $\Lambda_m(z)$ are Δ-analytic, by virtue of a theorem asserting the closure of functions of singularity analysis class under Hadamard products [10, 15]. (The function $\Lambda_m(z)$ is roughly comparable to $\mathrm{Li}_{3m/2}(4^m z^m)$.) Splitting the sum in (60) according to $m \leq M$ and $m > M$, for an arbitrarily large M, yields a factorization of $E(z)$ that fulfills the conditions of Theorem 2. Hence the existence of a full expansion for coefficients is granted.

For first order asymptotics, it suffices to analyse what happens as $z \to (\frac{1}{4})^-$. We find, from (60) and with the notations of (59)

$$E(z) = e^{L+1/2} \left(1 - \frac{1}{2}\sqrt{1-4z} + O(1-4z) \right),$$

which implies the stated estimate. □

The analysis obviously extends to any simple family of trees, in the sense of Meir and Moon [15, 29], including the case of Cayley trees that are enumerated by n^{n-1}.

5 Conclusion

As demonstrated by our foregoing examples, several infinite-product generating functions occurring in combinatorics are amenable to the hybrid method, despite the fact that they admit the unit circle as a natural boundary. For comparison purposes, Figure 3 displays a few typical infinite-product generating functions and the general asymptotic shapes[5] of their coefficients.

Perhaps the most well-known generating function in this range is

$$Q_0(z) := \prod_{n\geq 1} (1 + z^n),$$

whose coefficients enumerate partitions into distinct summands. In such a case, the analysis of coefficients, first performed by Hardy and Ramanujan, is carried out by mean of the saddle point method, in accordance with the fact that the function $Q_0(z)$ gets exponentially large at its "main" singularity $z = 1$. This and similar cases are best treated by means of Meinardus' method [1].

The function

$$Q_{-1/2}(z) := \prod_{n\geq 1} \left(1 + \frac{z^n}{\sqrt{n}} \right),$$

[5] We use '$\propto$' to represents asymptotic proportionality, that is, asymptotic equivalence up to an unspecified multiplicative constant.

Generating function	*Type*	*Coefficients*
$Q_0 = \prod_{n\geq 1}(1+z^n)$	Partitions dist. summ.	$\propto n^{-3/4}e^{\pi\sqrt{n/3}}$
$Q_{-1/2} = \prod_{n\geq 1}\left(1+\frac{z^n}{\sqrt{n}}\right)$		$\propto n^{-1/2}e^{\frac{3}{2}\sqrt[3]{2\pi n}}$
$Q_{-1} = \prod_{n\geq 1}\left(1+\frac{z^n}{n}\right)$	Perm. dist. cycle lengths	$\propto 1$
$Q_{-3/2} = \prod_{n\geq 1}\left(1+\frac{z^n}{n^{3/2}}\right)$	Forest dist. comp. sizes	$\propto n^{-3/2}$
$Q_{-2} = \prod_{n\geq 1}\left(1+\frac{z^n}{n^2}\right)$	Perm. same cycle type	$\propto n^{-2}$
$Q_{-\infty} = \prod_{n\geq 1}\left(1+\frac{z^n}{n!}\right)$	Set part. dist. block lengths	Mixed regimes [23].

Figure 3: Some typical infinite-product generating functions, their "types", and the asymptotic shape of the corresponding coefficients.

is also fast growing near $z = 1$ and is best transformed by means of convergence factors:

$$Q_{-1/2}(z) = \frac{e^{\mathrm{Li}_{1/2}(z)}}{\sqrt{1-z}}\prod_{n\geq 1}\left(1+\frac{z^n}{\sqrt{n}}\right)e^{-z/\sqrt{n}+z^2/2n}.$$

This expression shows a growth similar to that of the function $\exp((1-z)^{-1/2})$, to which the saddle point method is applicable. All computations done, we find

$$Q_{-1/2,n} \sim G\frac{e^{\zeta(1/2)}}{\sqrt{3\pi n}}\exp\left(\frac{3}{2}\sqrt[3]{2\pi n}\right) \qquad \text{with} \quad G = \prod_{n\geq 1}\left(1+\frac{1}{\sqrt{n}}\right)e^{-1/\sqrt{n}+1/(2n)}.$$

The next three examples of Figure 3 are relative to functions of the form

$$Q_\alpha := \prod_{n\geq 1}(1+z^n n^\alpha),$$

with $\alpha \leq -1$. These are typical cases where the hybrid method is applicable. The function Q_{-1} is exactly the one encountered when enumerating permutations with distinct cycle lengths. The function $Q_{-3/2}$ provides a simplified analytic model of dissimilar forests, while Q_{-2} behaves like the generating function of permutations having the same cycle type. The general pattern is, for $\alpha < -1$:

$$Q_{\alpha,n} \propto n^\alpha.$$

At the other end of the spectrum, we find the function

$$Q_\infty(z) := \prod_{n\geq 1}\left(1+\frac{z^n}{n!}\right),$$

which is the exponential generating function of set partitions, all of whose blocks are of distinct sizes. Clearly, this is an entire function to which the hybrid method is not applicable. Coefficients have been precisely studied by the seven authors of [23], with some (but not all) of the regimes being accessible to the saddle point method.

Finally, Gourdon has developed in [18] methods leading to asymptotic expansions of a shape similar to the ones of the present paper in relation to a refinement of Golomb's problem posed by Knuth in [25, Ex. 1.3.3.23]. He showed that the expected length of the longest cycle in a permutation of size n admits an asymptotic representation which starts as ($\omega = e^{2i\pi/3}$)

$$\lambda n + \tfrac{1}{2}\lambda - \tfrac{e^{\gamma}}{24n} + \left(\tfrac{e^{\gamma}}{48} - \tfrac{1}{8}(-1)^n\right)\tfrac{1}{n^2} + \left(\tfrac{17e^{\gamma}}{3840} + \tfrac{1}{8}(-1)^n + \tfrac{1}{6}\omega^{1-n} + \tfrac{1}{6}\omega^{n-1}\right)\tfrac{1}{n^3},$$

with higher order roots of unity appearing at higher asymptotic orders. The proof has analogies to the techniques of the present paper, with the additional need of precise expansions that describe the behaviour of the truncated logarithmic series on the unit disc.

Acknowledgements. Bruno Salvy's `equivalent` program has proved invaluable in permitting us to make several of our asymptotic expansions explicit. We are grateful to Svante Janson for penetrating remarks that allowed us to correct several errors and inaccuracies.

References

[1] George E. Andrews, *The theory of partitions*, Encyclopedia of Mathematics and its Applications, vol. 2, Addison–Wesley, 1976.

[2] Raymond Ayoub, *An introduction to the analytic theory of numbers*, Mathematical Surveys, No. 10, American Mathematical Society, Providence, R.I., 1963.

[3] Edward A. Bender, *Asymptotic methods in enumeration*, SIAM Review **16** (1974), no. 4, 485–515.

[4] Elwyn R. Berlekamp, *Algebraic coding theory*, Mc Graw-Hill, 1968, Revised edition, 1984.

[5] J Blum, *Enumeration of the square permutations in* $\mathfrak{S}_n$, Journal of Combinatorial Theory, Series A **17** (1974), 156–161.

[6] Miklós Bóna, Andrew McLennan, and Dennis White, *Permutations with roots*, Random Structures & Algorithms **17** (2000), no. 2, 157–167.

[7] B. L. J. Braaksma and D. Stark, *A Darboux-type theorem for slowly varying functions*, Journal of Combinatorial Theory, Series A **77** (1997), no. 1, 51–66.

[8] Louis Comtet, *Advanced combinatorics*, Reidel, Dordrecht, 1974.

[9] J. D. Dixon, *Asymptotics of generating the symmetric and alternating groups*, Electronic Journal of Combinatorics **12** (2005), no. R56, 1–5.

[10] James A. Fill, Philippe Flajolet, and Nevin Kapur, *Singularity analysis, Hadamard products, and tree recurrences*, Journal of Computational and Applied Mathematics **174** (2005), 271–313.

[11] Philippe Flajolet, *Singularity analysis and asymptotics of Bernoulli sums*, Theoretical Computer Science **215** (1999), no. 1-2, 371–381.

[12] Philippe Flajolet, Xavier Gourdon, and Daniel Panario, *Random polynomials and polynomial factorization*, Automata, Languages, and Programming (F. Meyer auf der Heide and B. Monien, eds.), Lecture Notes in Computer Science, no. 1099, 1996, Proceedings of the 23rd ICALP Conference, Paderborn, July 1996., pp. 232–243.

[13] ______, *The complete analysis of a polynomial factorization algorithm over finite fields*, Journal of Algorithms **40** (2001), no. 1, 37–81.

[14] Philippe Flajolet and Andrew M. Odlyzko, *Singularity analysis of generating functions*, SIAM Journal on Algebraic and Discrete Methods **3** (1990), no. 2, 216–240.

[15] Philippe Flajolet and Robert Sedgewick, *Analytic combinatorics*, April 2006, Chapters I–IX of a book to be published by Cambridge University Press, 717p.+x, available electronically from P. Flajolet's home page.

[16] W. B. Ford, *Studies on divergent series and summability and the asymptotic developments of functions defined by Maclaurin series*, 3rd ed., Chelsea Publishing Company, New York, 1960, (From two books originally published in 1916 and 1936.).

[17] Ian P. Goulden and David M. Jackson, *Combinatorial enumeration*, John Wiley, New York, 1983.

[18] Xavier Gourdon, *Combinatoire, algorithmique et géométrie des polynômes*, Ph.D. thesis, École Polytechnique, June 1996.

[19] D. H. Greene and D. E. Knuth, *Mathematics for the analysis of algorithms*, Birkhäuser, Boston, 1981.

[20] G. H. Hardy, *Ramanujan: Twelve lectures on subjects suggested by his life and work*, third ed., Chelsea Publishing Company, New-York, 1978, Reprinted and Corrected from the First Edition, Cambridge, 1940.

[21] F. B. Hildebrand, *Introduction to numerical analysis*, second ed., McGraw-Hill Book Co., New York, 1974, International Series in Pure and Applied Mathematics.

[22] R. Jungen, *Sur les séries de Taylor n'ayant que des singularités algébrico-logarithmiques sur leur cercle de convergence*, Commentarii Mathematici Helvetici **3** (1931), 266–306.

[23] A. Knopfmacher, A. M. Odlyzko, B. Pittel, L. B. Richmond, D. Stark, G. Szekeres, and N. C. Wormald, *The asymptotic number of set partitions with unequal block sizes*, Electronic Journal of Combinatorics **6** (1999), no. 1, R2:1–37.

[24] Arnold Knopfmacher and Richard Warlimont, *Distinct degree factorizations for polynomials over a finite field*, Transactions of the American Mathematical Society **347** (1995), no. 6, 2235–2243.

[25] Donald E. Knuth, *The art of computer programming*, 3rd ed., vol. 1: Fundamental Algorithms, Addison-Wesley, 1997.

[26] ———, *The art of computer programming*, 3rd ed., vol. 2: Seminumerical Algorithms, Addison-Wesley, 1998.

[27] L. Lewin (ed.), *Structural properties of polylogarithms*, American Mathematical Society, 1991.

[28] E. Manstavičius, *Mappings on decomposable combinatorial structures: analytic approach*, Combinatorics, Probability and Computing **11** (2002), no. 1, 61–78.

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

[30] A. M. Odlyzko, *Asymptotic enumeration methods*, Handbook of Combinatorics (R. Graham, M. Grötschel, and L. Lovász, eds.), vol. II, Elsevier, Amsterdam, 1995, pp. 1063–1229.

[31] F. W. J. Olver, *Asymptotics and special functions*, Academic Press, 1974.

[32] Nicolas Pouyanne, *On the number of permutations admitting an mth root*, Electronic Journal of Combinatorics **9** (2002), no. 1:R3, 1–12.

[33] Walter Rudin, *Real and complex analysis*, third ed., McGraw-Hill Book Co., New York, 1987.

[34] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, 2006, Published electronically at `www.research.att.com/~njas/sequences/`.

[35] Richard P. Stanley, *Enumerative combinatorics*, vol. I, Wadsworth & Brooks/Cole, 1986.

[36] ———, *Enumerative combinatorics*, vol. II, Cambridge University Press, 1999.

[37] P. Turán, *On some connections between combinatorics and group theory*, Combinatorial theory and its applications, III (Proc. Colloq., Balatonfüred, 1969), North-Holland, Amsterdam, 1970, pp. 1055–1082.

[38] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, Cambridge University Press, New York, 1999.

[39] E. T. Whittaker and G. N. Watson, *A course of modern analysis*, fourth ed., Cambridge University Press, 1927, Reprinted 1973.

[40] Herbert S. Wilf, *Generatingfunctionology*, Academic Press, 1994, Second edition, available on the internet from Herbert Wilf's home page.

[41] ———, *The variance of the Stirling cycle numbers*, ArXiv: math.CO/0511428, November 2005, 3 pages.