# Analytic Combinatorics of Unlabeled Objects

Pablo Rotondo

October 4, 2025

## Preamble

Welcome. This is the first part of the course "Analysis of Algorithms", code 2.15. You might also be interested in the course "Algorithmic aspects of combinatorics", code 2.10, which is thematically linked.

The evaluation is divided into two exams, a mid-term and a final exam, both with equal weight.

These notes correspond (more or less, they are likely to evolve) to the first 4 classes. I have tried for each section to contain at least one related algorithmic application, showing the use of the methods introduced therein. Of course, this is only an introduction and much more could be said about everything. The reader is encouraged to do the accompanying exercises and read the bibliography, in particular the book Analytic Combinatorics [3].

## Contents

## 1.  Introduction

This is a course about **Analysis of Algorithms**. The purpose is to study, very precisely, the behavior of algorithms. To do this in spite of the hardware we **count**: basic operations, memory used, etc.

You have most likely already worked with simple analysis. For example, you might remember that QuickSort performs $O(n \log n)$ comparisons on average but $\Theta(n^2)$ on the worst case.

In this course we are interested in the *precise* asymptotics and *random behavior* of algorithms and data structures. We are not alone; there is a body of techniques that can come in handy!

In this part of the course we will deal with the tools from Analytic Combinatorics. Later on you will also learn about probabilistic tools.

> **Analytic Combinatorics** aims at predicting precisely the properties of large structured combinatorial configurations, through an approach based extensively on analytic methods. Generating functions are the central objects of study of the theory.
> – Philippe Flajolet (1948–2011), Robert Sedgewick (1946–)



Philippe Flajolet, © Inria / Foto C. Tourniaire
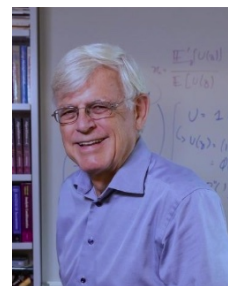


Robert Sedgewick, Wikipedia, **CC BY-SA 4.0**

The origins of Analytic Combinatorics can be traced back to Euler and Analytic Number Theory. The theory was developed, in great measure, by **Philippe Flajolet** during the 80s and 90s. This included the study of several key algorithms and data structures, such as Probabilistic counting and Tries.

The field is summarized in the Magnum Opus of P. Flajolet y R. Sedgewick [3] :

> **Analytic Combinatorics**, `https://algo.inria.fr/flajolet/Publications/books.html`.
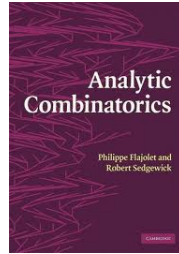
Analytic Combinatorics provides us with a large set of tools to analyze algorithms and data structures, specially when the size of the objects is very large.

The process of Analytic Combinatorics can be divided into two main steps:

1. **Symbolic step**: from an specification [recursive, iterative,...] of the problem, we find an equation for the *generating function* associated.

2. **Analytic step**: using appropriate *Transfer Theorems*, the analytic properties of the generating function turn into asymptotics for the coefficients.

This is well encapsulated in the motto:

*If you can specify it, you can analyze it !* – P. Flajolet, R. Sedgewick

## 2. Ordinary Generating Functions and Combinatorial Classes

Generating functions are the central objects of Analytic Combinatorics. They are a useful representation in order to count or obtain asymptotics. In this section we develop the basic workings of the *symbolic step*, which allows us to derive the generating function or, at least, characteristics of it.

There is a convenient dictionary for counting generating functions, which translates basic operations between the combinatorial classes to operations between the respective generating functions. This is dictionary is described in Sections 2.2 and 2.4

We begin from generating functions of a single variable. In Section 2.5 we introduce more variables, which serve to "mark" different parameters of the objects counted.

### 2.1. Formal power series

*A generating function is a clothesline on which we hang up a sequence of numbers for display.*
– Herbert S. Wilf (1931–2012)



Wikipedia, **CC BY-SA 3.0**.

**Definition 2.1.** Given a sequence of complex numbers $\{a_n\}_{n=0}^{\infty}$, we define its *Ordinary Generating*
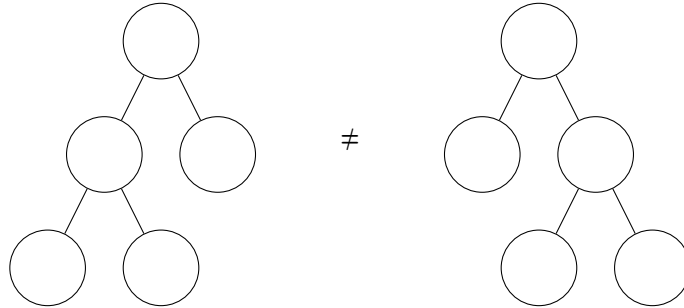
*Function* (OGF for short) by

$$A(z) = \sum_{n=0}^{\infty} a_n z^n .$$

We will write $[z^n]A(z) = a_n$.

We begin with a traditional example of the usefulness of OGFs.

**Example 2.2** (Rooted binary trees). Let us count rooted binary trees with $n$ nodes: trees start from the root and have one, two or no children at all. We allow the *empty tree* for convenience. The trees are *planar*; the order of the children matters.



Let us denote by $b_n$ the number of trees with $n$ nodes. Clearly $b_0 = 1, b_1 = 1$. And then we have the recurrence

$$b_{n+1} = \sum_{j=0}^{n} b_j b_{n-j} .$$

Let us introduce the OGF $B(z) = \sum_{n \geq 0} b_n z^n$. Multiplying the recurrence by $z^{n+1}$ and summing we have

$$\sum_{n \geq 0} b_{n+1} z^{n+1} = \sum_{n \geq 0} z^{n+1} \left( \sum_{j=0}^{n} b_j b_{n-j} \right) .$$

For convenience we define $b_j = 0$ for $j < 0$, so that we do not have to worry about the indexes of summation. Then

$$\sum_{n \geq 0} z^{n+1} \left( \sum_{j=0}^{n} b_j b_{n-j} \right) = z \sum_{j} b_j \sum_{n} b_{n-j} z^n = z \sum_{j} b_j z^j \sum_{n} b_{n-j} z^{n-j} = z(B(z))^2 .$$

As $\sum_{n \geq 0} b_{n+1} z^{n+1} = B(z) - b_0 = B(z) - 1$, we have deduced

$$B(z) - 1 = z(B(z))^2 \implies B(z) = 1 + zB((z))^2 .$$

– We solve[1], to obtain

$$B(z) = \frac{1 - \sqrt{1 - 4z}}{2z} .$$

– From the generalized Binomial Theorem $b_n = [z^n]B(z) = \binom{2n}{n} \frac{1}{n+1}$, the Catalan numbers.

For the moment OGFs are just a *formal* object. This is to say, we are not considering any notion of convergence, it is just a different way to write the sequence. In other words: we do not *yet* have the right to evaluate the series. Later we will see that all of these operations will make sense also analytically

---

[1] We will later see the analytic arguments that guarantee that this is the right solution.

within the so-called *radius of convergence* of the series. In this sense $\sum_{n=0}^{\infty} n! z^n$ is a perfectly "normal" power series, even though it converges just for $z = 0$.

We define the operations of sum and product as if we could operate with this infinite "polynomial". This yields what is called the *ring of Power Series*.

**Definition 2.3.** If $A(z) = \sum_{n=0}^{\infty} a_n z^n$ and $B(z) = \sum_{n=0}^{\infty} b_n z^n$, define

$$A(z) \pm B(z) := \sum_{n=0}^{\infty} (a_n \pm b_n) z^n, \quad A(z) \cdot B(z) := \sum_{n=0}^{\infty} c_n z^n,$$

where $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ es is the *Cauchy product*. Under these operations, the power series form a commutative ring.

Not every power series is invertible

**Proposition 2.4.** *A series $A(z) = \sum_{n=0}^{\infty} a_n z^n$ has a multiplicative inverse if and only if $a_0 \neq 0$.*

**Remark 2.5.** It is possible to define the ring of Power Series over arbitrary rings, and not just $\mathbb{C}$. In this case we demand that $a_0$ is invertible for the series $A(z)$ to be invertible.

A classical example of an inverse is the geometric series

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}.$$

This is easy to verify by computing the product $(1-z)\sum_{n=0}^{\infty} z^n = 1$.

**Example 2.6** (The OGF of the partial sums)**.** An interesting application of the geometric series is:

$$\frac{1}{1-z} \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} \left( \sum_{k=0}^{n} a_k \right) z^n.$$

We deduce

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}, \qquad \sum_{n=0}^{\infty} (n+1) z^n = \frac{1}{(1-z)^2}, \qquad \sum_{n=0}^{\infty} \left( \sum_{j=0}^{n} (j+1) \right) z^n = \frac{1}{(1-z)^3} \cdots$$

**Example 2.7** (OGF of Fibonacci numbers)**.** The Fibonacci numbers are defined by $f_0 = 0$, $f_1 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for $n \geq 0$. We are going to calculate $F(z) = \sum_n f_n z^n$.

Starting from the recurrence, we multiply by $z^{n+2}$ and sum:

$$\sum_{n=0}^{\infty} f_{n+2} z^{n+2} = \sum_{n=0}^{\infty} f_{n+1} z^{n+2} + \sum_{n=0}^{\infty} f_n z^{n+2}.$$

Factoring the extra factors $z$ we obtain

$$\sum_{n=0}^{\infty} f_{n+2} z^{n+2} = z \sum_{n=0}^{\infty} f_{n+1} z^{n+1} + z^2 \sum_{n=0}^{\infty} f_n z^n.$$

Finally, we identify that the first two series correspond to $F(z)$ without the first terms, namely $\sum_{n=0}^{\infty} f_{n+2} z^{n+2} = F(z) - f_0 - f_1 z^1 = F(z) - z$ and $\sum_{n=0}^{\infty} f_{n+1} z^{n+1} = F(z) - f_0 = F(z)$. Thus

$$F(z) - z = z F(z) + z^2 F(z) \implies F(z) = \frac{z}{1 - z - z^2}.$$

**Remark 2.8.** In passing, we note $[z^n]z^j A(z) = [z^{n-j}]A(z)$.

Given $A(z) = \sum_{n=0}^{\infty} a_n$ and $B(z) = \sum_{n=0}^{\infty} b_n$ , if $b_0 = 0$ we may define the composition $A(B(z))$.

We would like to define $A(B(z)) = \sum a_n (B(z))^n$, but we must make sense of this expression in the ring of power series. Observe that $[z^j](B(z))^n = 0$ for all $j < n$. Thus each coefficient of $A(B(z))$ may be defined as a finite sum:

$$[z^n]A(B(z)) = \sum_{j \le n} a_j [z^{n-j}](b_1 + b_2 z^1 + \ldots)^j \,.$$

On the other hand, if $b_0$, we note that this definition implies an infinite sum in order to determine the coefficients. We do not have any notion of convergence yet.

**Example 2.9.** Going back to the OGF of the Fibonacci numbers $F(z) = \frac{z}{1-z-z^2}$, we remark that

$$F(z) = z \frac{1}{1-(z+z^2)} = z \sum_{n=0}^{\infty} (z+z^2)^n = z \sum_{n=0}^{\infty} z^n \sum_j \binom{n}{j} z^j \,.$$

Extracting coefficients

$$f_n = \sum_{a+b=n-1} \binom{a}{b} = \sum_k \binom{k}{n-1-k} \,.$$

**Definition 2.10** (Differentiation). Given $A(z) = \sum_{n=0}^{\infty} a_n$, we define

$$A'(z) = \sum_{n=1}^{\infty} n a_n z^{n-1} \,.$$

Differentiating satisfies the classical product and quotient rules from calculus.

**Remark 2.11.** An important consequence is that $zA'(z)$ is the OGF of $na_n$.

**Example 2.12.** We show that

$$\sum_{n=0}^{\infty} \binom{n}{k} z^n = \frac{z^k}{(1-z)^{k+1}} \,.$$

Indeed, starting from $\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$ and differentiating $k$ times we have $\sum_{n=k}^{\infty} \frac{n!}{(n-k)!} z^{n-k} = \frac{k!}{(1-z)^{k+1}}$.

**Example 2.13.** We deduce that

**Definition 2.14** (Integration). Given $A(z) = \sum_{n=0}^{\infty} a_n$, we define

$$\int_0^z A(v)dv = \sum_{n=0}^{\infty} \frac{a_n}{n+1} z^{n+1} \,.$$

Integration satisfies the classical rules of calculus with respect to the derivative. For instance

$$\int_0^z A(v)B'(v)dv = A(v)B(v) - A(0)B(0) - \int_0^z A'(v)B(v)dv \,.$$

**Example 2.15.** We derive the OGF of the harmonic numbers $H_n := 1 + \frac{1}{2} + \ldots + \frac{1}{n}$.

Integrating $\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n$ we deduce[2] $\log\left(\frac{1}{1-z}\right) = \sum_{n=0}^{\infty} \frac{1}{n} z^n$. Finally, multiplying by $\frac{1}{1-z}$, we obtain the OGF of the partial sums of $n \mapsto \frac{1}{n}$, namely

$$\sum_{n=0}^{\infty} H_n z^n = \frac{1}{1-z} \log\left(\frac{1}{1-z}\right) \,.$$

---

[2]Strictly speaking, this is the formal definition of the power series $\log$. Analytically, since this definition is inspired by the classical result from calculus, the name is well-chosen as it will coincide within the radius of convergence $|z| < 1$.

**Exercise 2.16.** Find the OGF of $H_n^2$.

Here is a table of some basic OGFs:

| Sequence $a_n$ | OGF $F(z) = \sum a_n z^n$ |
|:---:|:---:|
| $1$ | $\dfrac{1}{1-z}$ |
| $n$ | $\dfrac{z}{(1-z)^2}$ |
| $\dfrac{1}{n}, \ n \geq 1$ | $\log\left(\dfrac{1}{1-z}\right)$ |
| $H_n, \ n \geq 1$ | $\dfrac{1}{1-z}\log\left(\dfrac{1}{1-z}\right)$ |
| $\binom{n}{m}, \ m \in \mathbb{Z}_{\geq 0}$ | $\dfrac{z^m}{(1-z)^{m+1}}$ |
| $\binom{\alpha}{n}, \ \alpha \in \mathbb{R}$ | $(1+z)^\alpha$ |
| Fibonacci $f_n$ | $\dfrac{z}{1-z-z^2}$ |
| $\dfrac{1}{n!}$ | $e^z$ |

## 2.2. Combinatorial Classes

**Definition 2.17.** A *combinatorial class* is a pair $(\mathcal{A}, |\cdot|_\mathcal{A})$, consisting of a countable set $\mathcal{A}$ of objects and a *size* function $|\cdot|_\mathcal{A}$ such that

- $|a|_\mathcal{A} \in \mathbb{Z}_{\geq 0}$ for all $a \in \mathcal{A}$,

- for every $n \in \mathbb{Z}_{\geq 0}$, the set of $a \in \mathcal{A}$ such that $|a|_\mathcal{A} = n$ is finite.

Given a combinatorial class $(\mathcal{A}, |\cdot|_\mathcal{A})$ we may define

$$A(z) = \sum_{a \in \mathcal{A}} z^{|a|}.$$

Alternatively, we may write $A(z) = \sum_{n=0}^\infty a_n z^n$ where $a_n$ is the number of elements of size $n$,

$$\mathcal{A}_n := \{a \in \mathcal{A} : |a| = n\}.$$

Combinatorial classes can be build by considering basic operations.

**Union** $\mathcal{A} = \mathcal{B} \cup \mathcal{C}$    Given combinatorial classes $\mathcal{B}$ and $\mathcal{C}$ with $\mathcal{B} \cap \mathcal{C} = \varnothing$, $\mathcal{A} = \mathcal{B} \cup \mathcal{C}$ is a combinatorial class with size function:

$$|a|_\mathcal{A} = \begin{cases} |a|_\mathcal{B} & \text{si } a \in \mathcal{B}, \\ |a|_\mathcal{C} & \text{si } a \in \mathcal{C}. \end{cases}$$

We remark that the OGFs satisfy $A(z) = B(z) + C(z)$.

**Product** $\mathcal{A} = \mathcal{B} \times \mathcal{C}$    Given combinatorial classes $\mathcal{B}$ and $\mathcal{C}$, the cartesian product $\mathcal{A} = \mathcal{B} \times \mathcal{C}$ is a combinatorial class with size function:

$$|(b, c)|_\mathcal{A} = |b|_\mathcal{B} + |c|_\mathcal{C}.$$

We remark that the OGFs satisfy $A(z) = B(z) \cdot C(z)$, due to the Cauchy product.

**Example 2.18** (Well-parenthesized strings)**.** The **class of well-parenthesized strings**

$$\mathcal{S} = \{\varepsilon, (), ()(), (()), \ldots\}$$

can be characterized by the formal equation (it is an unambiguous grammar):

$$\mathcal{S} = \varepsilon + (\mathcal{S})\mathcal{S}\,.$$

For the size, consider the number of opening parenthesis "(". Thus the equation translates into

$$S(z) = 1 + z\left(S(z)\right)^2\,.$$

Surprise surprise, this corresponds to Example 2.2. Thus $S(z) = \frac{1-\sqrt{1-4z}}{2z}$ and $[z^n]S(z) = \binom{2n}{n}\frac{1}{n+1}$.

### 2.3. Tree structures and the Lagrange Inversion Formula

**Definition 2.19.** We denote by $\mathcal{E}$ an empty element, with $|\mathcal{E}| = 0$. Similarly, we denote by $\mathcal{Z}$ an "atom", with $|\mathcal{Z}| = 1$.

**Example 2.20.** Full binary trees can be specified by

$$\mathcal{B} = \mathcal{E} + \mathcal{Z} \times \mathcal{B} \times \mathcal{B}\,,$$

that is, leaves have size $0$, and internal nodes size $1$. Thus the size is the number of internal nodes.

These are sometimes known as the Catalan trees: Catalan numbers count the number of full binary trees with $n$ internal nodes.

**Sequence** $\mathcal{A} = \mathrm{Seq}(\mathcal{B})$　　Given a combinatorial class $\mathcal{B}$, without elements of size $0$, $\mathcal{B}_0 = \varnothing$, we define the sequence $\mathcal{A} = \mathrm{Seq}(\mathcal{B})$ by

$$\begin{aligned}
\mathcal{A} &= \{(a_1, \ldots, a_k) : k \geq 0,\, a_i \in \mathcal{A}\} \\
&= \{\epsilon\} + \mathcal{A} + \mathcal{A} \times \mathcal{A} + \ldots\,,
\end{aligned}$$

with the size function corresponding to the cartesian products.

The generating functions are related by

$$A(z) = \frac{1}{1 - B(z)}\,.$$

**Example 2.21.** A general (plane[3]) tree consists of a root and a sequence of trees attached to it:

$$\mathcal{G} = \mathcal{Z} \times \mathrm{Seq}(\mathcal{G})\,.$$

We deduce $G(z) = \frac{z}{1-G(z)}$. Then $G(z) = \frac{1-\sqrt{1-4z}}{2}$.

Observe that $G(z) = zB(z)$ where $B(z)$ is the OGF of the Binary trees. In fact we can prove that $\mathcal{G} \simeq \mathcal{Z} \times \mathcal{B}$ by considering the classical "first-child, next-brother" argument (here we leave out the root).

---

[3]This means that the order of the children is important.

More generally, let $\Omega \subseteq \mathbb{Z}_{\geq 0}$ with $0 \in \Omega$. The set $\Omega$ specifies the possible arities of a node of the tree. Then, in an abuse of notation we write

$$\mathcal{A} = \mathcal{Z} \times \phi(\mathcal{A})\,, \qquad \phi(u) := \sum_{a \in \Omega} u^a\,.$$

In this case the OGF satisfies $A(z) = z\phi(A(z))$. Since $\phi(0) = 1$, a solution is actually guaranteed to exist, at least formally. In order to calculate the coefficients we use the following result:

**Theorem 2.22.** *Consider formal power series $f(u)$ and $\phi(u)$, with $\phi(0) \neq 0$. There is a unique power-series $u(t)$ satisfying*

$$u(t) = t\,\phi(u(t))\,.$$

*Further, the coefficients of $f(u(t))$ around $t = 0$ satisfy:*

$$[t^n]f(u(t)) = \frac{1}{n}[u^{n-1}]\{f'(u)\phi(u)^n\}\,.$$

We will prove this theorem later in Section 4.4, as a consequence of several results in Complex Analysis.

**Example 2.23.** Going back to general (plane) trees, we have $\phi(u) = \frac{1}{1-u}$ and we deduce

$$[z^n]G(z) = \frac{1}{n}[u^{n-1}]\frac{1}{(1-u)^n} = \frac{1}{n}\binom{2n-2}{n-1}\,.$$

Thus we have verified again the formula for the number of Catalan trees.

**Exercise 2.24.** Use the Lagrange Inversion Formula on the Catalan trees directly. [Hint. change the definition of size]

## 2.4. Unlabeled Powerset and Multiset construction

We begin this section with an important example that illustrates the Multiset construction nicely.

**Definition 2.25** (Integer partitions). A partition of $n \in \mathbb{Z}_{\geq 1}$ is a sequence of positive integers $a_1 \leq a_2 \leq \ldots \leq a_k$ such that $a_1 + a_2 + \ldots + a_k = n$.

In other words, these are all of the possible ways to sum $n$ if we disregard the order of the terms. For example:

$$7 = 7; 7 = 6 + 1; 7 = 5 + 2; 7 = 5 + 1 + 1; 7 = 4 + 3; 7 = 4 + 2 + 1 \ldots$$

An equivalent way to understand partitions is to decide, *how many ones*, *how many twos*, *how many threes*, etc. :

$$\mathcal{P} = \mathtt{Seq}(\mathbf{1}) \times \mathtt{Seq}(\mathbf{2}) \times \mathtt{Seq}(\mathbf{3}) \times \ldots$$

with size $|\mathbf{k}|_{\mathcal{P}} = k$ for each $k$.

Using the sequence construction we deduce the OGF of integer partitions:

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

The previous construction is precisely a *Multiset* of $\mathcal{I} = \{\mathbf{1}, \mathbf{2}, \ldots\}$.

**Definition 2.26** (Multiset). Given a combinatorial class $\mathcal{A}$, with $\mathcal{A}_0 = \varnothing$, its multiset is

$$\mathtt{MSet}(\mathcal{A}) = \prod_{a \in \mathcal{A}} \mathtt{Seq}(a)\,.$$

**Proposition 2.27.** *The OGF of* `MSet`$(\mathcal{A})$ *is*

$$M(z) = \prod_{n=1}^{\infty} \left( \frac{1}{1-z^n} \right)^{a_n} = \exp \left( \sum_{n=1}^{\infty} \frac{1}{n} A(z^n) \right).$$

*Proof.* We work formally with the exponential and logarithm. Write

$$\left( \frac{1}{1-z^n} \right)^{a_n} = \exp \left( a_n \log \left( \frac{1}{1-z^n} \right) \right).$$

At this point we use the expansion $\log \left( \frac{1}{1-z^n} \right) = \sum_{j=1}^{\infty} \frac{1}{j} z^{nj}$. Reversing the sums:

$$M(z) = \exp \left( \sum_{n=1}^{\infty} a_n \sum_{j=1}^{\infty} \frac{1}{j} z^{nj} \right) \exp \left( \sum_{j=1}^{\infty} \frac{1}{j} \left( \sum_{n=1}^{\infty} a_n z^{nj} \right) \right).$$

Here we recognize $\sum_{n=1}^{\infty} a_n z^{nj} = A(z^j)$ and we are done. $\square$

For integer partitions we deduce:

$$P(z) = \exp \left( \sum_{n=1}^{\infty} \frac{1}{n} \frac{z^n}{1-z^n} \right).$$

Now suppose we allowed each item at most once. This construction is called the PowerSet:

**Definition 2.28** (PowerSet)**.** Given a combinatorial class $\mathcal{A}$, with $\mathcal{A}_0 = \varnothing$, its set is

$$\text{PSet}(\mathcal{A}) = \prod_{a \in \mathcal{A}} \left( \mathcal{E} + a \right).$$

**Proposition 2.29.** *The OGF of* `PSet`$(\mathcal{A})$ *is*

$$M(z) = \prod_{n=1}^{\infty} \left( 1 + z^n \right)^{a_n} = \exp \left( \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} A(z^n) \right).$$

Here is a summary of the unlabeled constructions and their corresponding generating functions:

| Construction | OGF |
| :---: | :---: |
| $\mathcal{E}$ | $1$ |
| $\mathcal{Z}$ | $z$ |
| $\mathcal{A} + \mathcal{B}$ | $A(z) + B(z)$ |
| $\mathcal{A} \times \mathcal{B}$ | $A(z) \times B(z)$ |
| $\text{Seq}(\mathcal{A})$ | $\frac{1}{1-A(z)}$ |
| $\text{MSet}(\mathcal{A})$ | $\exp \left( \sum_{n=1}^{\infty} \frac{1}{n} A(z^n) \right)$ |
| $\text{PSet}(\mathcal{A})$ | $\exp \left( \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} A(z^n) \right)$ |

## 2.5. Parameters and Multivariate Generating Functions

We begin this section with a toy example:

**Example 2.30.** Integer compositions are like integer partitions, except that order matters !

That is to say, an integer composition of $n$ is a vector of positive integers $(x_1, \ldots, x_k)$ (for any length $k$) such that $x_1 + \ldots + x_k = n$. Consider $n$ to be the size, we have the combinatorial specification

$$\mathcal{C} = \mathrm{Seq}(\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots\}) \simeq \mathrm{Seq}(\mathrm{Seq}_{\geq 1}(\mathcal{Z})) \,.$$

[explain the specification of the integers as a sequence before]

Thus we find,

$$C(z) = \frac{1}{1 - \frac{z}{1-z}} = \frac{1-z}{1-2z} \,, \qquad [z^n]C(z) = 2^n - 2^{n-1} = 2^{n-1} \,, \text{ for } n \geq 1.$$

Now consider the following question:

What is the average number of terms in an integer composition of $n$ ?

We solve this problem by introducing an extra formal variable $u$. This variable will "mark" the number of terms. The idea is that we will obtain a formula for the bivariate generating function

$$C(z, u) = \sum_{n, k \geq 0} c_{n,k} z^n u^k \,,$$

where $c_{n,k}$ is the number of compositions of $n$ with $k$ terms, i.e.,

$$c_{n,k} = \#\{(x_1, \ldots, x_k) \in \mathcal{C}_n\} \,.$$

Looking at the specification of $\mathcal{C}$, we note that the number of terms is simply the length of the outer Seq. We introduce an atom $\mathcal{U}$ with generating function $u$, and we have the specification

$$\mathcal{C} = \mathrm{Seq}(\mathcal{U} \times \mathrm{Seq}_{\geq 1}(\mathcal{Z})) \implies C(z, u) = \frac{1}{1 - u\frac{z}{1-z}} \,,$$

for the bivariate class. In all, we have inserted the atom $\mathcal{U}$ in order to mark the quantity of interest.

In order to finish the example, we remark that the expected value can be written in terms of the bivariate generating function. Indeed

$$\partial_u C(z, 1) = \sum_{n \geq 0} \left( \sum_{k \geq 1} c_{n,k} \cdot k \right) z^n \,, \quad C(z, 1) = \sum_{n \geq 0} \left( \sum_{k \geq 1} c_{n,k} \right) z^n = C(z) \,,$$

and therefore the average for $n$ is

$$\mathbb{E}_n[k] = \frac{[z^n]\partial_u C(z, 1)}{[z^n]C(z, 1)} \,.$$

We have $\partial_u C(z, 1) = \frac{z}{1-z}\left(1 - \frac{z}{1-z}\right)^{-2} = \frac{z(1-z)}{(1-2z)^2} = \frac{z}{1-2z} + \frac{z^2}{(1-2z)^2}$. Therefore, recalling that $[z^n]\frac{1}{(1-z)^2} = n + 1$ we obtain

$$[z^n]\partial_u C(z, 1) = 2^{n-1} + 2^{n-2}(n-1) \sim n2^{n-2} \,.$$

In all we deduce that $\mathbb{E}_n[k] \sim \frac{n}{2}$.

**Exercise 2.31.** The result for compositions has a simple combinatorial explanation. Find it.

This example has introduced most of the important concepts. Bivariate (or multivariate) generating functions arise in order to account for parameters of the objects studied.

In addition to the size, we introduce a parameter $\chi: \mathcal{A} \to \mathbb{Z}_{\geq 0}$, and define

$$\mathcal{A}_{n,k} = \{a \in \mathcal{A} : |a| = n, \, \chi(a) = k\} .$$

We have the bivariate generating function

$$A(z, u) = \sum_{a \in \mathcal{A}} z^{|a|} u^{\chi(a)} = \sum_{n,k \geq 0} a_{n,k} z^n u^k .$$

The dictionary of constructions works exactly as before, adding the new atom $\mathcal{U}$ of OGF $u$, if the parameter (or parameters) $\chi$ is additive[4], namely

$$\chi((a,b)) = \chi(a) + \chi(b) ,$$

for the product.

As we saw, the average of $\chi$ are related to the derivative in $u$

**Proposition 2.32.**

$$\mathbb{E}_n[\chi] = \frac{[z^n] \partial_u A(z, 1)}{[z^n] A(z, 1)} = \frac{\sum_k k \cdot a_{n,k}}{a_n} .$$

And if the distribution were not uniform? We consider the probability generating functions (PGF)

$$P^{\langle \mathcal{A} \rangle}(z, u) := \sum_{n,k \geq 0} \mathbf{P}_n^{\langle \mathcal{A} \rangle}(\chi = k) \cdot z^n u^k , \qquad P^{\langle \mathcal{A} \rangle}(z, 1) = \sum_{n=0}^{\infty} 1 \cdot z^n = \frac{1}{1 - z} .$$

Cartesian products translate to products if there is independence, but there is a no dictionary a priori.

We can still find the moments by differentiation

$$(u \partial_u)^1 P(z, u) \Big|_{u=1} = \sum_{n=0}^{\infty} \mathbb{E}_n[\chi] z^n , \quad (u \partial_u)^2 P(z, u) \Big|_{u=1} = \sum_{n=0}^{\infty} \mathbb{E}_n[\chi^2] z^n , \quad \ldots$$

## 3. Rational Functions: a first taste of coefficient asymptotics

Rational functions have very simple asymptotics which we can completely characterize without the full analytic machinery. Still, they serve to introduce the flavor of results we will find later on.

We give two applications of the asymptotics for rational functions. In Section 3.4 we perform the analysis of the Euclidean Algorithm for polynomials over Finite Fields. In Section 3.3 we study the link between generating functions and regular languages. This will yield a simple proof that, for instance, the language of well-parenthesized words (Example 2.18) is not regular.

---

[4]In the book [3] the term used is *inherited*.

## 3.1. Definitions and examples

Let us come back to the Fibonacci numbers $\{f_n\}_{n=0}^{\infty}$ and their generating function

$$F(z) = \frac{z}{1 - z - z^2} \ .$$

We may apply partial fractions to this function. Let $r_1$ and $r_2$ be the roots of $1 - z - z^2 = 0$. Namely $r_1 = \phi^{-1}$ and $r_2 = -\phi$ where $\phi = (1 + \sqrt{5})/2$ satisfies $\phi^2 = \phi + 1$. Then

$$F(z) = \frac{c_1}{r_1 - z} + \frac{c_2}{r_2 - z} ,$$

for certain coefficients $c_1$ and $c_2$ we must calculate.

First, remark that

$$\frac{c_j}{r_j - z} = \frac{c_j/r_j}{1 - z/r_j} = \frac{c_j}{r_j} \sum_{n=0}^{\infty} r_j^{-n} z^n ,$$

for $j = 1$ and $j = 2$. Thus we have $f_n = c_1 r_1^{-n-1} + c_2 r_2^{-n-1} = c_1 \phi^{n+1} + c_2 (-\phi)^{-n-1}$.

Finally, calculating $c_1 = \frac{1}{\sqrt{5}}$, $c_2 = \frac{\phi}{\sqrt{5}}$ and observing that $c_2(-\phi)^{-n-1} \to 0$ we deduce $f_n \sim \frac{1}{\sqrt{5}} \phi^{n+1}$.

**Remark 3.1.** The power series $F(z)$ converges absolutely for $|z| < \phi^{-1}$. This is seen from the convergence of the series $\sum_{n=0}^{\infty} r_j^{-n} z^n$ for $j = 1$ and $j = 2$.

This example is typical of *rational functions.*

**Definition 3.2** (Rational function). A function $f(z)$ is said to be *rational* if and only if $f(z) = \frac{p(z)}{q(z)}$ with $p(z)$ and $q(z)$ polynomials.

**Note.** Henceforth we suppose that $q(0) \neq 0$. This is necessary for $f(z)$ to be a proper power-series.

Obtaining the asymptotics of a rational function $f(z) = \frac{p(z)}{q(z)}$ comes down to partial fractions. Before introducing the general method we show one further example.

**Example 3.3** (Change making with two coins). Let $a$ and $b$ be coprime positive integers (the coin types). In how many ways can we represent $n$ as $n = xa + yb$ with integers $x, y \geq 0$ ?

Let $a_n$ be the number of representations, being a Multiset we have

$$A(z) = \sum a_n z^n = \frac{1}{1 - z^a} \times \frac{1}{1 - z^b} \ .$$

All of the roots of $1 = z^a$ and $1 = z^b$ are roots of unity. Since $a$ and $b$ are coprime, all *roots are simple except $z = 1$* that is a *double root*. By partial fractions we obtain

$$A(z) = \frac{A}{(1 - z)^2} + \frac{B}{1 - z} + \sum_{u:u^b=1, u\neq 1} \frac{c_u}{1 - z/u} + \sum_{u:u^a=1, u\neq 1} \frac{c_u}{1 - z/u} ,$$

for certain constants. We deduce that

$$a_n = (n + 1) A + B + \sum_{u:u^b=1, u\neq 1} c_u u^{-n} + \sum_{u:u^a=1, u\neq 1} c_u u^{-n} .$$

Since we are dealing with roots of unity, we deduce the leading term $a_n \sim n \times A$. The constant $A$ can be computed easily $A = \lim_{z \to 1}(1 - z)^2 A(z) = \frac{1}{ab}$ .

**Exercise 3.4.** Describe the general case in which we have $k$ coins, $a_1, \ldots, a_k \geq 1$ with $\gcd(a_1, \ldots, a_k) = 1$. This is known as Schur's Theorem.

## 3.2. General coefficients and asymptotics

Coming back to the general case $f(z) = \frac{p(z)}{q(z)}$, by the Fundamental Theorem of Algebra (this is proved in Corollary 4.17 below) $q(z)$ has exactly $\deg(q(z))$ zeros, maybe with multiplicity greater than 1. Let $r_1, \ldots, r_d$ be its distinct zeroes, and let $m_1, \ldots, m_d$ be their repsective multiplicities, i.e.,

$$q(z) = c\,(z - r_1)^{m_1} \ldots (z - r_d)^{m_d}$$

for some constant $c > 0$.

Let us suppose that $\deg p(z) < \deg q(z)$, else $\frac{p(z)}{q(z)} = c(z) + \frac{r(z)}{q(z)}$ where $c(z)$ is the quotient of the division and $r(z)$ the remainder. By partial fractions there are $c_1^{\langle 1 \rangle}, \ldots, c_1^{\langle m_1 \rangle}, \ldots, c_d^{\langle 1 \rangle}, \ldots c_d^{\langle m_d \rangle}$ such that

$$f(z) = \sum_{j=1}^{d} \sum_{k=1}^{m_j} \frac{c_j^{\langle k \rangle}}{(1 - z/r_j)^k}\ .$$

Let us look at each term. Recalling Example 2.12,

$$\frac{c_j^{\langle k \rangle}}{(1 - z/r_j)^k} = c_j^{\langle k \rangle} \sum_{n=0}^{\infty} \binom{n + k - 1}{n} r_j^{-n} z^n\ .$$

We deduce

$$[z^n]f(z) = \sum_{j=1}^{d} \sum_{k=1}^{m_j} c_j^{\langle k \rangle} \binom{n + k - 1}{n} r_j^{-n}\ .$$

Even though this is an exact formula, it is not very practical, as we must compute all of the coefficients $c_j^{\langle k \rangle}$ and roots $r_j$. For convenience suppose that $\gcd(p(z), q(z)) = 1$, else we could reduce the fraction. This implies that, for each $j = 1, \ldots, d$, we must have $c_j^{\langle m_j \rangle} \neq 0$.

**Remark 3.5.** Note that $\binom{n+k-1}{n} = \frac{n^{k-1}}{(k-1)!} + O(n^{k-2})$ as $n \to \infty$.

Define $\rho \triangleq \min_{j=1,\ldots,d} |r_j|$. Observe that all terms involving $r_j$ with $|r_j| > \rho$ are negligible compared to those with $|r_j| = \rho$. Still, the dominant terms involving $|r_j| = \rho$ could cancel each other.

**Remark 3.6.** Here $\rho$ is corresponds to the *radius of convergence* of $f(z)$ as a power-series. The roots $r_j$ such that $|r_j| = \rho$ are known as the *dominant singularities*.

**Theorem 3.7.** *Consider a rational function* $f(z) = \frac{p(z)}{q(z)}$, *with* $q(0) \neq 0$, $\deg p(z) < \deg q(z)$ *and* $\gcd(p(z), q(z)) = 1$. *Let* $r_1, \ldots, r_d$ *be the distinct roots of* $q(z)$ *and let* $m_1, \ldots, m_d$ *be their respective multiplicities.*

*There exist polynomials* $\Pi_j$ *for* $j = 1, \ldots, d$ *such that*

$$[z^n]f(z) = \sum_{j=1}^{d} \Pi_j(n) r_j^{-n}\ .$$

*Moreover* $\deg(\Pi_j) = m_j - 1$.

We remark that, when there is a single singularity $r_j$ on the radius of convergence $|z| = \rho$ we have

$$[z^n]f(z) \sim c_j^{\langle m_j \rangle} \frac{n^{m_j - 1}}{(m_j - 1)!} \times r_j^{-n}\ .$$

Moreover, we must have $\rho = r_j$, else we could prove that some coefficient would not be positive.

**Remark 3.8.** Given the roots $r_j$, it is simple to compute the coefficients $c_j^{\langle m_j \rangle}$:

$$c_j^{\langle m_j \rangle} = \lim_{z \to r_j} f(z) \times (1 - z/r_j)^{m_j}.$$

**Example 3.9.** We give an example of cancellation of the dominant singularities. Consider

$$\frac{1}{1 - z^3} = \sum_{n=0}^{\infty} z^{3n} \longleftrightarrow \{1, 0, 0, 1, 0, 0, 1, 0, 0, \ldots\}.$$

In this case the roots are $r_0 = 1$, $r_1 = e^{2\pi i/3}$, and $r_2 = e^{4\pi i/3}$,

$$\frac{1}{1 - z^3} = \frac{1/3}{1 - z} + \frac{1/3}{1 - z/e^{2\pi i/3}} + \frac{1/3}{1 - z/e^{4\pi i/3}}.$$

Later we will learn more about the singularities $r_1, \ldots, r_d$, in the case that the coefficients of $f(z)$ are non-negative. Pringsheim's Theorem (Theorem 4.39) tells us that the radius of convergence $\rho$ is necessarily a singularity. Moreover, if there are several dominant singularities, these must be *evenly spaced* on the circle $|z| = \rho$, as in the previous example. This is known as Daffodil's Lemma (**??**).

We summarize here the case of only one dominant singularity:

**Proposition 3.10.** *Let $f(z)$ be an OGF that can be represented as a rational function. Suppose $z = \rho > 0$ were the only dominant singularity of $f(z)$, and that for some $m \in \mathbb{Z}_{\geq 1}$*

$$f(z) \sim \frac{c}{(1 - z/\rho)^m}, \quad (z \to \rho), \quad \implies \quad [z^n]f(z) \sim c\frac{n^{m-1}}{(m-1)!}\rho^{-n}.$$

**Remark 3.11.** This result also works if there are other dominant singularities, but all of them have **strictly** smaller multiplicity, as roots, than $m$. This was the case in Example 3.3.

Later on we will generalize Proposition 3.10 to more general functions, as well as non-integer $m$. See the Transfer Theorem below (Theorem 5.7).

### 3.3. The generating functions of regular languages

In this section we relate languages and generating functions. We begin with a classical result.

**Theorem 3.12.** *Let $\Sigma$ be a finite alphabet and let $L$ be a regular language over $\Sigma$. Let $L(z) = \sum_{n=1}^{\infty} a_n z^n$ be the counting generating function of $L$, namely $a_n = \#\{w \in \Sigma^n : w \in L\}$.*

*The generating function $L(z)$ is rational.*

*Proof.* We recall that any regular language $L$ is recognized by a DFA (Deterministic Finite Automaton), and conversely. The advantage of a DFA is that we can be sure that there is a unique path: we count accepted words only once.

Thus consider a DFA over a finite alphabet $\Sigma = \{a_1, \ldots, a_k\}$ of letters, with states $Q = (s_1, \ldots, s_m)$, initial state $s_1$ and transitions $\delta : Q \times \Sigma \to Q$. Let $S$ be the set of final or accepting states.

Let us introduce a symbolic variable $x_a$ for each $a \in \Sigma$ and define the transition matrix $P((x_a)_{a \in \Sigma})$

$$[P]_{i,j} = \sum_{a \in \Sigma : \delta(i,a)=j} x_a.$$

Then the power matrices, generalizing the case of Markov Chains,

$$M = P^k, \qquad [M]_{i,j} = \sum_{w \in \Sigma^k : \delta(i,w)=j} x_w,$$

where $x_w = x_{w_1} \dots x_{w_k}$ if $w = w_1 \dots w_k$ with $w_1, \dots, w_k \in \Sigma$. Note that, essentially, $x_w = x_{a_1}^{c_1} \dots$ where $c_1$ is the number of occurrences of the symbol $a_1$ in $w$, and so on.

Then we can extract, formally, the terms corresponding to the accepted words as

$$(1\,0\,0\dots)P^k(v_Q),$$

where $(v_Q)$ is the column vector having 1s on the entries associated with the accepting states and $0$ elsewhere.

Letting $x_a = z$ for all $a \in \Sigma$ we just count the length (instead of the count of each letter)

$$P(z, \dots, z) = zA,$$

with $[A]_{i,j} = \#\{a \in \Sigma : \delta(i,a) = j\}$. We obtain

$$(1\,0\,0\dots)P^k v_Q = a_k z^k.$$

Summing over $k$ we obtain

$$(1\,0\,0\dots)(\mathrm{Id}_{m,m} - zA)^{-1}(v_Q) = (1\,0\,0\dots)(\mathrm{Id}_{m,m} - P(z, \dots, z))^{-1}(v_Q) = L(z),$$

where we write $P(z, \dots, z) = Az$.

We claim this is a rational function. It is enough to prove that the entries of the matrix $(\mathrm{Id}_{m,m} - zA)^{-1}$ are rational functions. This is indeed the case: rational functions $\mathbb{C}(z)$ form a field ! Hence we can perform the Gaussian Algorithm. The rows of $\mathrm{Id}_{m,m} - zA$ cannot be linearly dependent, else this would also be the case when evaluating at $z = 0$. $\qquad\square$

**Applications.**   We show to examples of how to use this result to prove that certain languages are not regular.

– Consider the language of the well-parenthesized strings. Its counting OGF:

$$L(z) = \frac{1 - z - \sqrt{1 - 4z}}{2z}$$

which is not rational. Moreover, its coefficients are of the form $a_n \sim c\frac{4^n}{\sqrt{n}}$.

– Consider the language of strings $0^p$ with $p$ prime. This language is not rational either. Indeed

$$Q(z) = \frac{1}{1 - z}L(z) = \frac{1}{1 - z} \sum_{p \text{ prime}} z^p = \sum_{n \geq 1} \pi(n)z^n,$$

where $\pi(n) = \#\{p \text{ prime} : p \leq n\}$ is the prime counting function. Here $\pi(n) \sim \frac{n}{\log n}$ by the Prime Number Theorem. This is in fact a contradiction to $Q(z)$ being rational.

Indeed, it is clear that $Q(z)$ has radius of convergence $\rho = 1$. Moreover, $(1 - z)Q(z) \to \infty$ as $z \to 1^-$ as there are infinitely many primes. Thus, if $Q(z)$ were rational, then $\rho = 1$ must have multiplicity at least 2. However, we show that $Q(z) = o\big(\frac{1}{(1-z)^2}\big)$ as $z \to 1^-$ over the reals, which is absurd. This is a consequence of the following more general result:

**Proposition 3.13.** *Consider sequences $a_k, b_k \geq 0$ and let $A(z) = \sum_{k=0}^{\infty} a_k z^k$ and $B(z) = \sum_{k=0}^{\infty} b_k z^k$, converging in $|z| < 1$. Suppose $a_k = o(b_k)$, and $B(t) \to \infty$ as $t \to 1^-$. Then $A(t) = o(B(t))$ as $t \to 1^-$.*

*Proof.* Consider $\varepsilon > 0$ arbitrary. For large enough $k$ we have $0 \leq a_k \leq \varepsilon b_k$, say for $k \geq N_\varepsilon$. Then

$$A(t) = \sum_{k < N_\varepsilon} a_k t^k + \sum_{k \geq N_\varepsilon} a_k t^k \leq \sum_{k < N_\varepsilon} a_k + \varepsilon \sum_{k \geq N_\varepsilon} b_k t^k \leq \sum_{k < N_\varepsilon} a_k + \varepsilon B(t) \,.$$

Dividing by $B(t) > 0$,

$$0 \leq \frac{A(t)}{B(t)} \leq \frac{1}{B(t)} \sum_{k < N_\varepsilon} a_k + \varepsilon \,,$$

and letting $t \to 1^-$ we obtain $0 \leq \limsup_{t \to 1^-} \frac{A(t)}{B(t)} \leq \varepsilon$. Since $\varepsilon > 0$ was arbitrary, we are done. $\qquad \square$

**Remark 3.14.** Similarly, we can prove that if $a_k/b_k \to L$ with $L > 0$, then $A(t)/B(t) \to L$ as $t \to 1^-$.

Back to our case, since $\pi(n)/n \to 0$, we deduce that $Q(t) = o(\frac{1}{(1-t)^2})$ as $t \to 1^-$. This is absurd if the multiplicity of $\rho = 1$ were at least 2.

Note that the previous proof works for any sequence $a_k$ with $\#\{k : a_k \leq n\} \to \infty$ sub-linearly.

**Remark 3.15.** For the interested reader, it is possible to avoid the Prime Number Theorem, and prove $\pi(n)/n \to 0$ in an intuitive way. The natural density of the primes greater than $K$ is $\leq \prod_{p \leq K}(1 - \frac{1}{p}) \leq \exp(-\sum_{p \leq K} 1/p)$ and the harmonic sum of prime numbers is divergent $\sum_{p \leq K} 1/p \to \infty$.

### 3.4. The Euclidean Algorithm for polynomials over Finite Fields

In this section we are going to perform the average analysis of the Euclidean Algorithm to compute the gcd of a pair of polynomials over a finite field. The interested reader is referred to [1] for a full account, including the multiple gcd, limit laws, and the integer case.

We recall that a finite field has $q = p^m$ elements, for some prime $p$. For simplicity, you may think of the case $m = 1$, in which the multiplicative inverse of $a \neq 0$ is simply $a^{p-2}$, due to Fermat's Little Theorem. In general, $\mathbb{F}_q$ is unique up to isomorphism, and is produced as the quotient field of $\mathbb{F}_p[x]$ by an irreducible polynomial of degree $m$.

**The euclidean algorithm**   Consider as input a pair of polynomials $(a(x), b(x))$ from a finite field $F$ with $|F| = q$. The Euclidean Algorithm proceeds as follows. If $\deg a(x) < \deg b(x)$, swap them. Write $r_{-1}(x) \triangleq a(x)$ and $r_0(x) \triangleq b(x)$. At each step $i = 0, 1, \ldots$ we perform the division of $r_{i-1}(x)$ by $r_i(x)$

$$r_{i-1}(x) = q_i(x) r_i(x) + r_{i+1}(x) \,,$$

where $\deg r_{i+1}(x) < \deg r_i(x)$, until we obtain $r_{k+1}(x) = 0$ and declare $\gcd(a(x), b(x)) = r_k(x)$. The number of steps employed is the number of divisions, namely $k$ such that $r_{k+1}(x) = 0$ for the first time. Write $k = C(a(x), b(x))$ to mean the "cost" of the pair.

Observe, conversely, that knowing whether we swapped the input polynomials, $\gcd(a(x), b(x)) = r_k(x)$ and $q_k(x), \ldots, q_1(x)$ uniquely determine the input pair $(a(x), b(x))$.

**The random model**   For the input we suppose that $a(x)$ and $b(x)$ are monic polynomials (i.e., their leading coefficient is 1), and consider the sums of degrees as the size for the pair:

$$\Omega_n \triangleq \{(a(x), b(x)) : \deg a(x) + \deg b(x) = n \,, a(x), b(x) \text{ monic polynomials}\} \,.$$

Our input is going to be a pair from $\Omega_n$ taken uniformly at random.

**Analysis on average**   Now that we have described the algorithm and the model, we proceed to the analysis. We are going to characterize the bivariate generating function

$$F(z, u) = \sum_{(a(x),b(x))\in\Omega} z^{\deg a(x)+\deg b(x)} u^{C(a(x),b(x))} \,.$$

The average over $\Omega_n$ is then

$$\mathbf{E}_n[C] = \frac{[z^n]\partial_u F(z,1)}{[z^n]F(z,1)} \,,$$

as explained in Section 2.5.

*Symbolic step.* First we require a symbolic characterization of $F(z, u)$. This is done by a careful analysis of the algorithm. As we remarked, the initial pair can be characterized uniquely by the gcd and the sequence of quotients $q_1(x), \ldots, q_k(x)$. Note that $q_1(x)$ must be monic, as we have supposed that both $a(x)$ and $b(x)$ are. Also, since the gcd in principle is just defined up to a multiple factor, we can pick the gcd to be monic. Under these conditions, given $(a(x), b(x))$, the choice of whether two swap the input, the choice of $q_1(x), q_2(x), \ldots, q_k(x)$ and $\gcd(a(x), b(x))$ is unique and viceversa.

We introduce the following auxiliary OGFs:

- The OGF of monic polynomials: $U(z) = \frac{1}{1-qz}$.

- The OGF of all polynomials of degree at least one: $G(z) = (q-1)\frac{qz}{1-qz}$.

We prove the following symbolic equation in two formal variables $z$ and $t$,

$$U(z) \cdot U(t) = U(zt) \times (1 + (U(z) - 1) + (U(t) - 1)) \times \frac{1}{1 - G(zt)} \,.$$

This is interpreted as follows. The LHS corresponds to the input pairs $(a(x), b(x))$ and we mark by $z$ the degree of $a(x)$, and by $t$ the degree of $b(x)$.

The RHS will rebuild the pair from the process of the Euclidean Algorithm:

- The factor $U(zt)$ on the RHS corresponds to the gcd, which is monic for it to be a bijection.

- The factor $(1 + (U(z) - 1) + (U(t) - 1))$ corresponds to $q_1(x)$, which is also monic. It turns out that $q_1(x)$ may either be $1$ in the case $\deg a(x) = \deg b(x)$, or come from either the division of $a(x)$ by $b(x)$, or $b(x)$ by $a(x)$ depending on which has the largest degree.

- Finally, the factor $\frac{1}{1-G(zt)}$ corresponds to a sequence of general polynomials $q_2(x), q_3(x), \ldots, q_k(x)$ which contribute to the degrees of both $a(x)$ and $b(x)$ equally.

Following this decomposition, we now understand that $C$ corresponds to the length of the sequence on the last step plus one:

$$F(z, u) = U(z^2) \times (2U(z) - 1) \times \frac{u}{1 - uG(z^2)} \,.$$

*Analytic step.* The analytic step involves just rational functions in this case, as both $U(z)$ and $G(z)$ are rational:

$$F(z, u) = \frac{u(1 + qz)}{(1 - qz)(1 - z^2(q + u(q^2 - q)))} \,.$$

Then

$$\partial_u F(z,1) = \frac{1-qz^2}{(1+qz)(1-qz)^3}\,, \qquad F(z,1) = \frac{1}{(1-qz)^2}\,.$$

By looking at the leading terms,

$$[z^n]\partial_u F(z,1) \sim \left(\frac{q-1}{2q}\right) \cdot \frac{n^2}{2} q^n\,, \qquad [z^n]F(z,1) = (n+1)q^n\,.$$

Therefore we obtain $\mathbf{E}_n[C] \sim \frac{q-1}{4q}n$ as $n \to \infty$.

**Exercise 3.16.** What if the input pair $(a(x), b(x))$ satisfied $\deg a(x) \geq \deg b(x)$ and the size was $|(a(x), b(x))| = \deg a(x)$ ?

## 4. First principles of the Analytic Theory of Generating Functions

### 4.1. Introduction

Generating functions are a bridge between discrete mathematics, on the one hand, and continuous analysis (particularly complex variable theory) on the other. [...]

To omit those [analytical] parts of the subject [...] is like listening to a stereo broadcast of, say, Beethoven's Ninth Symphony, using only the left audio channel.

– Herbert S. Wilf, preface of *generatingfunctionology* [5], 1989.

In what follows, we see our generating functions as functions in the complex plane. When the series $f(z) = \sum_{n=0}^{\infty} a_n z^n$ converges, its analytical properties (as a function) are strongly related to the asymptotic growth of its coefficients.

We will see that, if

$$[z^n]f(z) \sim \theta(n)\,\rho^{-n}\,,$$

1. **First principle of coefficient asymptotics**: the radius of convergence $\rho$ of the power series $f(z)$ corresponds to the exponential growth of the coefficients.

2. **Second principle of coefficient asymptotics**: the sub-exponential factor $\theta(n)$ is related to the type of singularties of $f(z)$.

In this section we discuss the first principle and introduce the notion of singularities.

### 4.2. Radius of Convergence

We start by studying when the series actually defines a function. For this to be the case we want the series to converge absolutely.

We recall that a series $\sum_n c_n$ converges if and only if $\lim_{N\to\infty} \sum_{n\leq N} c_n$ exits. Still, the series might be ill-defined in the following sense: a reordering of the term may converge to a different value, or even worse, fail to converge at all[5].

**Example 4.1.** The series $\sum_{n=1}^{\infty}(-1)^{n+1}\frac{1}{n}$ converges conditionally

- $\sum_{n=1}^{\infty}(-1)^{n+1}\frac{1}{n} = \sum_{n=0}^{\infty}\left(\frac{1}{4n+1} + \frac{1}{4n+3} - \frac{1}{4n+4} - \frac{1}{4n+6}\right) = \log 2$,

---

[5]This is Riemann's rearrangement theorem.

- but, changing the order, $\sum_{n=0}^{\infty} \left( \frac{1}{4n+1} + \frac{1}{4n+3} - \frac{1}{2n+2} \right) = \frac{3}{2} \log 2$.

To solve this issue we consider absolute convergence. A series $\sum_n c_n$ converges absolutely if and only if $\sum_n |c_n|$ converges. When this happens, we are allowed to reorder the terms as we please.

We note that, in the case of a power-series $f(z) = \sum_{n=0}^{\infty} a_n z^n$, if $f(z)$ converges absolutely for some $z_0$, then by comparison it converges absolutely for $|z| \le |z_0|$ too.

**Definition 4.2** (Radius of convergence). The radius of convergence of $f(z) = \sum_{n=0}^{\infty} a_n z^n$ is $\rho \ge 0$ (maybe $\rho = \infty$) such that the series converges absolutely for $|z| < \rho$ and diverges for $|z| > \rho$.

The following theorem proves the **first principle of coefficient asymptotics**.

**Theorem 4.3** (Cauchy-Hadamard). *The radius of convergence $0 \le \rho \le \infty$ of a power-series $f(z) = \sum_{n \ge 0} a_n z^n$ is determined by*

$$\rho = \frac{1}{\limsup\limits_{n \to \infty} |a_n|^{1/n}} . \tag{4.1}$$

*In other words, when $0 < \rho < \infty$, for every $\epsilon > 0$:*

- *we have $|a_n|^{1/n} < \frac{1}{\rho} + \epsilon$ for all $n$ large enough,*

- *we have $|a_n|^{1/n} > \frac{1}{\rho} - \epsilon$ for an infinite number of $n$'s.*

*Proof.* Let $R$ denote the RHS of (4.1). We show that $\sum_{n \ge 0} |a_n||z|^n$ is convergent for $|z| < R$ and that $\lim_n |a_n z^n| \ne 0$ for $|z| > R$. This shows that $R = \rho$, the radius of convergence. For the proof we suppose $0 < R < \infty$, the other cases are easily treated separately.

– Let $|z| < R$. We show that $\sum_{n \ge 0} |a_n||z|^n$ is convergent. For any $\epsilon > 0$ we have $|a_n|^{1/n}|z| < \frac{|z|}{R} + |z|\epsilon$ for all large enough $n$. Here $\frac{|z|}{R} < 1$ so we may pick $\epsilon > 0$ small enough so that $\frac{|z|}{R} + |z|\epsilon < \frac{|z|}{R} + R\epsilon < 1$. Then our series is dominated by the converging $\sum \theta^n$ with $\theta = \frac{|z|}{R} + R\epsilon$.

– Consider $|z| > R$. For any $\epsilon > 0$ we have $|a_n|^{1/n} > \frac{1}{R} - \epsilon$ for infinitely many $n$. Since $\frac{|z|}{R} > 1$, we may choose $\epsilon > 0$ small enough so that $\theta := \frac{|z|}{R} - |z|\epsilon > 1$. Then $|a_n|^{1/n}|z| > \theta > 1$ for infinitely $n$. It follows that $\lim_n |a_n z^n| \ne 0$, which makes it impossible for $\sum_n a_n z^n$ to be convergent. $\qquad \square$

This result implies already simple upper-bounds for the coefficients:

- Suppose $0 < \rho < \infty$. Then for every fixed $\varepsilon > 0$, $|a_n| = o((\frac{1}{\rho} + \varepsilon)^n)$.

- Suppose $\rho = \infty$. Then for every fixed $R > 0$ we have $|a_n| = o(R^{-n})$.

Within the radius of convergence power-series are very well-behaved: we may integrate and differentiate term by term, obtaining the integral or derivative of the corresponding function. Both things will be consequences of the uniform convergence of the power-series within the radius of convergence. We prove these results in the next section, where we introduce complex differentiation and integration. For the moment we just remark the continuity.

**Proposition 4.4.** *Consider a power-series $f(z)$ with radius of convergence $\rho > 0$. Then $f(z)$, as a complex-valued function, is continuous on the disc $|z| < \rho$.*

*Proof.* Let $r < \rho$. We note that, by comparison with the series $f(r) = \sum a_n r^n$ we have that $f(z)$ converges uniformly on $|z| \le r$. As clearly each of the terms of the sum is continuous, a uniformly

convergent series of continuous functions is continuous too. Since $r < \rho$ is arbitrary, the result follows.
□

**Example 4.5** (The Kraft-McMillan inequality)**.** Consider alphabet $\mathcal{A} = \{a_1, \ldots, a_k\}$ and $\mathcal{B} = \{\mathbf{0}, \mathbf{1}\}$, the binary alphabet. A **binary code** $c: \mathcal{A}^\star \to \mathcal{B}^\star$ is a morphism, i.e., it satisfies $c(xy) = c(x)c(y)$. A code $c$ is said to be *uniquely decodable* iff $c$ is injective.

We prove the following Kraft-McMillan inequality:

If a **binary code** $c: \mathcal{A}^\star \to \mathcal{B}^\star$ is uniquely decodable, then

$$\sum_{a \in \mathcal{A}} 2^{-|c(a)|} \leq 1\,.$$

*Proof.* Let $A(z) = \sum_{w \in \mathcal{A}^\star} z^{|c(w)|}$. As we have a morphism, $A(z) = \frac{1}{1-C(z)}$, $C(z) = \sum_{w \in \mathcal{A}} z^{|c(w)|}$.

Since the code $c$ is decodable, we must have $[z^n]A(z) \leq 2^n$. This means that $A(z)$ converges absolutely for $|z| < 1/2$. If $\rho_A$ is the radius of convergence of $A(z)$, then $\rho_A \geq 1/2$.

Suppose for the sake of contradiction that $C(1/2) = \sum_{a \in \mathcal{A}} 2^{-|c(a)|} > 1$. Then, by continuity, there exists $0 \leq r < 1/2$ such that $C(r) = 1$. But then $A(t) \to \infty$ as $t \to r^-$, using $A(z) = \frac{1}{1-C(z)}$. This is a contradiction to the fact that $r < \rho_A$ and so $A(r) < \infty$ and $A(z)$ is continuous at $z = r$. □

The radius of convergence $\rho$ of a power-series $f(z) = \sum_{n=0}^\infty a_n z^n$ corresponds to the smallest absolute value of a *singularity* of the function $f(z)$. This will be proved in Theorem 4.15. A singularity is a point in which the function $f(z)$ either cannot be defined, or ceases to be smooth.

This result is very intuitive and useful. However, in order to prove it formally, we first need two basic result from complex analysis: Cauchy's Integral Theorem for holomorphic (complex-differentiable) functions.

## 4.3. Fundamental results from Complex Analysis

> When I was taking complex analysis, I remember someone saying "Complex analysis is the Disneyland of mathematics" because so many incredible theorems turn out to be true.
> – From a comment by John D. Cook in MathOverflow here.

There are good reasons for this quote. For starters, in complex analysis, being differentiable once means being differentiable infinitely many times (and having a power-series expansion) ! In fact, differentiation is integration. Following the Taylor expansion, this means that we can extract coefficients by integration. This is Theorem 4.21, and it is base result for coefficient extraction. Still, this is not the only incredible result and I hope that this brief introduction will be also of intrinsic interest to the reader.

### 4.3.1  Differentiation and integration

A complex function can be described as a function from an **open** subset $\mathcal{D}$ of $\mathbb{R}^2$ to $\mathbb{R}^2$. Write $f(x, y) \triangleq f(x + i y) = g(x, y) + i h(x, y)$, where $g: \mathcal{D} \to \mathbb{R}$ and $h: \mathcal{D} \to R$ are the real and imaginary parts of $f(x + i y)$ respectively. Defining differentiability as in the case of multi-variable functions would miss the fact that we may now perform divisions in $\mathbb{C}$. Here is the definition.

**Definition 4.6** (Differentiability)**.** Let $f:\mathcal{D} \to \mathbb{C}$ be a function, where $\mathcal{D} \subseteq \mathbb{C}$ is an open set. We say $f$ is *differentiable* at $z_0 \in \mathcal{D}$ if and only if

$$\lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0},$$

exists, and we will denote this number by $f'(z_0)$. A function differentiable at each point of an open set $\mathcal{D}$ is said to be *holomorphic* on $\mathcal{D}$.

This notion of differentiability is much stronger than that of $\mathbb{R}$. Taking $z_0 = (x, y)$ and $\epsilon \in \mathbb{R}$,

$$\lim_{\epsilon \to 0} \frac{f(x + \epsilon, y) - f(x, y)}{\epsilon} = \partial_x g + i\, \partial_x h, \qquad \lim_{\epsilon \to 0} \frac{f(x, y + \epsilon) - f(x, y)}{\epsilon\, i} = \partial_y h - i\, \partial_y g.$$

Both of this expressions must equal $f'(z_0)$ when $f$ is differentiable. Thus

$$\partial_x g = \partial_y h, \qquad \partial_x h = -\partial_y g. \tag{4.2}$$

These are known as the **Cauchy-Riemann equations**. We conclude that not any function $f$ differentiable over $\mathbb{R}^2$ can be differentiable in the complex plane. Moreover, if $g$ and $h$ are both twice continuously differentiable we deduce $\partial_x^2 g + \partial_y^2 g = 0$ and $\partial_x^2 h + \partial_y^2 h = 0$, they are harmonic functions.

We now define line-integration on the complex plane.

**Definition 4.7** (Curve)**.** A *curve* $\alpha:[a, b] \to \mathbb{C}$ is a continuous map. The point $\alpha(a)$ is said to be the starting point and $\alpha(b)$ the ending point. Moreover

- The curve is said to be *closed* if $\alpha(a) = \alpha(b)$.

- The curve is said to be *simple* if $\alpha(t) \neq \alpha(s)$ for all $t, s$ with $a < t < s < b$.

- The curve is said to be *smooth* if $\alpha$ is differentiable.

- The curve is said to be *piecewise-smooth* if there are $t_1, \ldots, t_k$, for some $k$, with $t_0 = a \leq t_1 \leq \ldots \leq t_k \leq b = t_{k+1}$ such that $\alpha|_{[t_i, t_{i+1}]}$ is smooth for $i = 0, \ldots, k$.

**Convention.**  Henceforth, unless explicitly stated, curves are assumed to be piecewise-smooth.

There are some equivalent terms used in the literature. In the context of complex integration, often a curve is called a *path* or *path of integration*, and a closed curve is called a *contour* or *contour of integration*. A closed curve is sometimes called a *loop*.

**Definition 4.8** (Complex line integral)**.** Let $\gamma:[a, b] \to \mathbb{C}$ be a piecewise-smooth curve. We define

$$\int_\gamma f(z)dz := \int_a^b f(\gamma(t))\gamma'(t)dt.$$

If the curve is closed, the integral symbol is substituted by $\oint$.

The value of the integral does not depend on the parametrization. Namely, if two curves are just a reparameterization of one another, the integral is the same.

**Proposition 4.9.** *Let $\mathcal{D}$ be an open set. Let $\alpha:[c, d] \to \mathcal{D} \subset \mathbb{C}$ be a piece-wise smooth curve and let $\varphi:[a, b] \to [c, d]$ be continuously differentiable, with $\varphi(a) = c, \varphi(b) = d$.*

*Then, for any continuous function $f:\mathcal{D} \to \mathbb{C}$,*

$$\int_\alpha f(z)dz = \int_{\alpha \circ \varphi} f(z)dz.$$

An important remark is that, the value of a line integral can be bounded in terms of the length of the curve. The length of a curve $\alpha:[a,b] \to \mathbb{C}$ is $\ell(\alpha) := \int_a^b |\alpha'(t)| dt$.

**Proposition 4.10.** *Let $\mathcal{D}$ be an open set. Let $f: \mathcal{D} \to \mathbb{C}$ be continuous and let $\alpha:[a,b] \to \mathcal{D}$ be a curve on $\mathcal{D}$. If $|f(z)| \leq M$ for all $z \in \alpha([a,b])$, then*

$$\left| \int_\alpha f(z) dz \right| \leq \ell(\alpha) \times M.$$

Note that, if the continuous function $f(z)$ has a primitive $F(z)$, i.e., $F'(z) = f(z)$, then we have

$$\int_\alpha f(z) dz = F(\alpha(b)) - F(\alpha(a)).$$

Thus, a function with a primitive integrates to zero on any closed curve.

**Lemma 4.11.** *Let $C$ be a circle centered at the origin $z = 0$, traversed counter-clockwise. Then*

$$\oint_C \frac{dz}{z} = 2\pi i, \qquad \text{and} \qquad \oint_C z^m dz = 0, \qquad m \in \mathbb{Z} \smallsetminus \{-1\}.$$

*Proof.* The circle can be parametrized by $\gamma(t) = re^{it}$, with $t \in [0, 2\pi]$, if its radius is $r > 0$. By definition $\oint_C z^m dz = \int_0^{2\pi} r^m e^{mit}(ire^{it}) dt = ir^{m+1} \int_0^{2\pi} e^{(m+1)it} dt$. Now, if $m = -1$ this is just $2\pi i$. For $m \neq -1$ we use the primitive $\frac{e^{(m+1)it}}{(m+1)i}$ to obtain $0$. $\qquad\square$

**Remark 4.12.** This implies that $1/z$ does not have a primitive. Of course, there is the logarithm, but it cannot be defined on a whole circle around $z = 0$ due to continuity problems. More about this later.

The closed curve (contour) $\alpha$ is said to be positively oriented when it is traversed counter-clockwise.
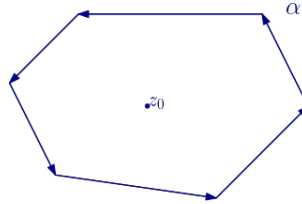


Observe that Lemma 4.11 is already significant. If $f(z) = \sum a_n z^n$ converges on some positive radius $\rho > 0$, integration term by term (due to uniform convergence) yields

$$[z^n]f(z) = \frac{1}{2\pi i} \oint_C \frac{f(z)}{z^{n+1}} dz, \tag{4.3}$$

where $C$ is any positively-oriented circle of radius $r < \rho$ around $z = 0$.

In the next section we explain that this formula actually works for any function $f(z)$ is complex-differentiable in the region containing $|z| \leq r$. This is a fundamental result: with this formula we can prove that there must be a singularity on the circle $|z| = \rho$ where $\rho$ is the radius of convergence.

**Definition 4.13** (Singularity). Let $\mathcal{D} \subset \mathbb{C}$ be an open set. A holomorphic function $f: \mathcal{D} \to \mathbb{C}$ is said to have a singularity at $z_0 \in \partial\mathcal{D}$ if and only if it there is no holomorphic extension $f: \tilde{\mathcal{D}} \to \mathbb{C}$ of $f$, with $\mathcal{D} \subset \tilde{\mathcal{D}}$ and $z_0 \in \tilde{\mathcal{D}}$.

In Section 4.3.2 we prove that being holomorphic is equivalent to being analytic. Thus we speak of analytic extension rather than holomorphic extension.

**Example 4.14.** For example, $f(z) = \sum_{n \geq 0} z^n$ satisfies $f(z) = \frac{1}{1-z}$ for $|z| < 1$. We remark that $\tilde{f}(z) = \frac{1}{1-z}$ is an analytic extension of $f(z)$ to $\mathbb{C} \smallsetminus \{1\}$. On the radius of convergence we have $z = 1$, which is a singularity.

**Theorem 4.15.** *Let* $f(z) = \sum_n a_n z^n$ *be a power-series with radius of convergence* $\rho < \infty$, *then there must be at least one singularity on the circle* $|z| = \rho$.

*Proof.* We show this result assuming that Eq. (4.3) holds on any open domain containing $C$ and its interior, in which $f(z)$ can be extended analytically. Thus, we are supposing Theorems 4.19 and 4.21

Suppose $f(z)$ could be extended analytically to every point in $|z| = \rho$. This means that, for every point on $|z| = \rho$ there is an open ball in which $f(z)$ is analytic. As the circle $|z| = \rho$ is compact, we can extract a finite open sub-covering and have a finite number of these ball cover the whole circle $|z| = \rho$. This means that there must exist a radius $R' > \rho$ such that $f(z)$ is analytic on $|z| \leq R'$.

Let $r = (\rho + R')/2 < R'$ and consider $C$ the circle $|z| = r$ traversed counter-clockwise. Then, by our assumption,

$$a_n = [z^n]f(z) = \frac{1}{2\pi i} \oint_{|z|=r} \frac{f(z)}{z^{n+1}} dz \,,$$

and by the triangular inequality

$$|a_n| \leq \frac{\max_{|z|=r} |f(z)|}{r^n} \,.$$

By Theorem 4.3 this means that $f(z) = \sum a_n z^n$ has a radius of convergence $\rho \geq r$, a contradiction because $r = (\rho + R')/2 > \rho$. $\qquad\square$

If there were no singularity, that is, we have what is called an *entire function*, then the function must be either unbounded or constant everywhere.

**Theorem 4.16** (Liouville)**.** *If* $f : \mathbb{C} \to \mathbb{C}$ *is bounded and entire, it is constant.*

*Proof.* Following the previous proof, if $\max_{|z|=r} |f(z)| \leq M$ for any $r$, by taking $r \to \infty$ we obtain $a_n = 0$ for all $n \geq 1$. Hence $f(z)$ is constant if it is bounded. Note, again, that we are assuming that Eq. (4.3) holds more generally. $\qquad\square$

A famous corollary is the Fundamental Theorem of Arithmetic. Of course, by a simple induction, having always one root means that a polynomial of degree $n$ has exactly $n$ complex roots.

**Corollary 4.17.** *A non-constant polynomial* $p(z)$ *over* $\mathbb{C}$ *must have at least one complex root.*

*Proof.* If it did not, then $1/p(z)$ would be entire and bounded. Then constant, an absurd. $\qquad\square$

### 4.3.2   Equivalence between analytic and holomorphic: Cauchy's Integral Formula

A "seemingly" big family of holomorphic functions is given by the so called *Analytic Functions*, the functions that locally have a power-series expansion. In this section we explain that, in fact, being analytic and holomorphic are equivalent concepts.

**Definition 4.18** (Analytic function)**.** A function $f : \mathcal{D} \to \mathbb{C}$ will be said to be analytic at a point $z_0 \in \mathcal{D}$ if and only if there is an open disk $D(z_0, r) = \{z : |z - z_0| < r\}$ in $\mathcal{D}$, around $z_0$, such that

$$f(z) = \sum_{n \geq 0} c_n (z - z_0)^n \,,$$

is absolutely convergent for $z \in D(z_0, r)$. Further, $f$ is said to be analytic on $\mathcal{D}$ if and only if it is analytic at each point $z_0 \in \mathcal{D}$.

Analytic functions are differentiable in the disc where they converge, hence an analytic function is clearly holomorphic. We will now prove that both concepts are actually equivalent. That is why, after this section, we simple use the term **analytic**.

**Theorem 4.19** (Analytic equals Holomorphic). *A function $f$ is holomorphic on a region $\mathcal{D}$ if and only if it is analytic there.*

We give a sketched proof. The following fundamental result is a key step in the proof.

**Theorem 4.20** (Cauchy-Goursat Theorem). *Let $\mathcal{D}$ be a convex domain, and let $f: \mathcal{D} \to \mathbb{C}$ be holomorphic on $\mathcal{D} \smallsetminus \{p\}$ for some $p \in \mathcal{D}$, and continuous in $p$. Then $\oint_C f(z)dz = 0$ for every closed curve $C \subset \mathcal{D}$.*

We require the following intermediate result

**Theorem 4.21** (Cauchy's Integral Formula). *Consider $\mathcal{D}$ to be a convex domain, let $w \in \mathcal{D}$, let $\alpha$ be a simple closed curve in $\mathcal{D}$ such that $z_0$ is surrounded by $\alpha$, and let $f: \mathcal{D} \to \mathbb{C}$ be holomorphic in $\mathcal{D}$.*

$$f(z_0) = \frac{1}{2\pi i} \oint_\alpha \frac{f(z)}{z - z_0} dz. \tag{4.4}$$

*Proof.* We prove this supposing that $1 = \frac{1}{2\pi i} \oint_\alpha \frac{dz}{z - z_0}$. This is true for a circle $\alpha = C$ centered at $z_0$. In the case of a simple closed curve, $\alpha$ can be deformed into $C$ continuously. We can prove that $\frac{1}{2\pi i} \oint_\alpha \frac{dz}{z - z_0}$ is an integer for any closed curve (see Remark 4.22). Hence it remains one through the deformation.

Due to our supposition

$$\frac{1}{2\pi i} \oint_\alpha \frac{f(z)}{z - z_0} dz - f(z_0) = \frac{1}{2\pi i} \oint_\alpha \frac{f(z) - f(z_0)}{z - z_0} dz,$$

which we wish to prove equals $0$. The function $\frac{f(z) - f(w)}{z - w}$ is differentiable at the points $z \neq w$, and can be made continuous at $z = z_0$ by defining it to be $f'(w)$ for $z = w$. Now, the Cauchy-Goursat Theorem implies that the integral over a closed curve is $0$. $\qquad\square$

**Remark 4.22.** Define $\mathrm{ind}_\alpha(z_0) \triangleq \frac{1}{2\pi i} \oint_\alpha \frac{dz}{z - z_0}$, known as the winding number of $\alpha$ with respect to $z_0$. This number can be proven to be always an integer [4, Thm.10.10]. Intuitively, it defines the number of times the curve $\gamma$ "winds" around $z_0$ counter-clockwise. If it does so clockwise, it is counted $-1$.

With this definition, the general version of Cauchy's Integral Theorem reads:

$$\mathrm{ind}_\alpha(z_0) f(z_0) = \frac{1}{2\pi i} \oint_\alpha \frac{f(z)}{z - z_0} dz. \tag{4.5}$$

In this case $\alpha$ need not be a simple closed curve. Observe that if $z_0$ is not surrounded by $\alpha$, then the integral is $0$ as expected.

**Remark 4.23.** The hypothesis that $\mathcal{D}$ be a convex domain can be relaxed significantly: it is enough that the domain be "simply connected", meaning that simple closed curves can be deformed continuously into a point. This is the formal version of "there are no *holes*" in $\mathcal{D}$.

**Proof of Theorem 4.19**   Let $z_0 \in \mathcal{D}$, and consider $R > 0$ so that $B(z_0, R) \subseteq \mathcal{D}$. We give an explicit series development there.

Let $0 < r < R$ and consider $w \in \mathcal{D}$ with $|w - z_0| < r$. We can write

$$\frac{f(z)}{z - w} = \frac{f(z)}{\left(1 - \frac{w - z_0}{z - z_0}\right)(z - z_0)} \,.$$

Here $\left|\frac{w - z_0}{z - z_0}\right| < \frac{r}{R} < 1$ if we choose $z$ to be in the circle of radius $R$, centered at $z_0$, thus we get that

$$\frac{1}{1 - \frac{w - z_0}{z - z_0}} = \sum_{n \geq 0} \left(\frac{w - z_0}{z - z_0}\right)^n,$$

converges uniformly for such a choice of $z$. Let $\gamma$ be a circle of radius $R$ centered at $z_0$, and traverse in counter-clockwise direction, we get

$$f(w) = \frac{1}{2\pi i} \oint_\alpha \frac{f(z)}{z - w} dz = \sum_{n \geq 0} \left(\frac{1}{2\pi i} \oint_\alpha \frac{f(z)}{(z - z_0)^{n+1}} dz\right) (w - z_0)^n,$$

by exploiting that uniform convergence implies that we may switch the sum and the integral. $\qquad\square$

**Corollary 4.24.** *We have*
$$f^{(n)}(z_0) = \frac{n!}{2\pi i} \oint_\alpha \frac{f(z)}{(z - z_0)^{n+1}} dz, \tag{4.6}$$

*for each $n \geq 0$.*

The corollary follows from the uniqueness of the power-series representation and the Taylor-expansion.

## 4.4. Residues: Rouché's Theorem, Lagrange Inversion Formula and other consequences

The following is essentially an extension of Cauchy's Integral Formula. First we need to extend the series expansion into a two-sided expansion: a Laurent expansion.

**Theorem 4.25** (Laurent expansion). *Let $f(z)$ be analytic on an annulus $\{z : \varrho < |z - z_0| < \rho\}$. Then there are functions $g(z)$ and $h(z)$, analytic on $D(z_0, \rho)$ and $D(z_0, 1/\varrho)$ respectively, such that $f(z) = g(z) + h(1/z)$. Moreover, the decomposition is unique if $h(0) = 0$. On the annulus we may write*

$$f(z) = \sum_{n=-\infty}^{\infty} a_n(z - z_0)^n,$$

*where $g(z) = \sum_{n=0}^{\infty} a_n z^n$ and $h(z) = \sum_{n=1}^{\infty} a_{-n} z^n$.*

*Proof.* It is essentially the same proof as for the form of the Taylor expansion. $\qquad\square$

**Definition 4.26** (Residue). Suppose $f(z)$ is analytic on an annulus around $z = z_0$ and suppose the Laurent expansion is $f(z) = \sum_{n=-\infty}^{\infty} a_n(z - z_0)^n$ uniformly on that annulus. The coefficient $a_{-1}$ is called the *residue* of $f(z)$ at $z_0$. We write $\texttt{res}(f(z); z = z_0) = a_{-1}$.

**Theorem 4.27** (Residues). *Let $\mathcal{D}$ be a convex [or simply-connected] domain. Suppose that $f$ is analytic on $\mathcal{D}$ except maybe on a finite number of points $z_1, \dots, z_k \in \mathcal{D}$.*

*Then, for any simple closed curve $\alpha$ on $\mathcal{D} \smallsetminus \{z_1, \ldots, z_k\}$ we have*

$$\oint_\alpha f(z)dz = 2\pi i \sum_{z_i \in \texttt{Int}(\alpha)} \texttt{res}(f(z); z = z_i).$$

*Here* $\texttt{Int}(\alpha)$ *represents the bounded region delimited by* $\alpha$.

The residues formula follows by subtracting the lower part of the Laurent expansion at each $z_j$, obtaining removable singularities at each. In fact, we may substitute the contour by a sum of small circles around each singularity. Then we recall that if $C$ is a small circle around $z = 0$,

$$\oint_C z^m dz = \begin{cases} 0 & \text{if } m \neq -1, \\ 2\pi i & \text{if } m = -1. \end{cases}$$

**Remark 4.28.** In the case of a meromorphic function $f(z) = p(z)/q(z)$ at $z = z_0$, the residue can be computed either by taking the formal division, or by

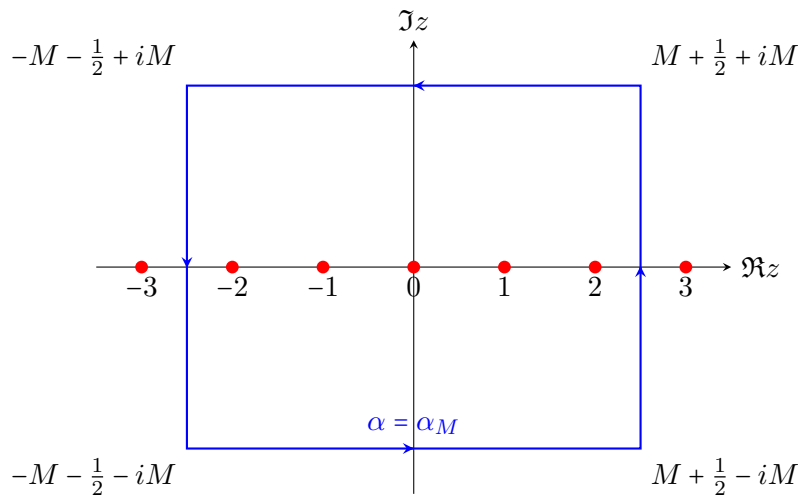$$g(z) := ((z - z_0)^m f(z)), \qquad \texttt{res}(f(z); z = z_0) = g^{(m-1)}(z_0)/(m-1)!,$$

where $m$ is the order of the pole at $z = z_0$.

**Example 4.29.** We prove that $\sum_{n=1}^\infty \frac{1}{n^2} = \frac{\pi^2}{6}$.

Consider $f(z) = \frac{1}{z^2} \frac{\cos(\pi z)}{\sin(\pi z)}$. A calculation using Remark 4.28 shows that

$$\texttt{res}(f(z); z = j) = \begin{cases} \frac{1}{\pi j^2}, & j \neq 0, \\ -\frac{\pi^2}{3}, & j = 0. \end{cases}$$

Consider the contour $\alpha = \alpha_M$ given by a rectangle with sides $z(t) = M + 1/2 + it$ for $t = [-M, M]$, $z(t) = (M + 1/2) \cdot (1 - 2t) + iM$ for $t \in [0,1]$, $z(t) = -M - 1/2 - it$ for $t = [-M, M]$ and $z(t) = -(M + 1/2) \cdot (1 - 2t) - iM$ for $t \in [0,1]$. The contour is pictured below



Thus,

$$\oint_\alpha f(z)dz = 4\pi i \sum_{j=1}^M \frac{1}{\pi j^2} - 2\pi i \frac{\pi^2}{3}$$

But we can show that $\oint_\alpha f(z)dz \to 0$ as $M \to \infty$. Indeed, we recall that

$$\frac{\cos(\pi z)}{\sin(\pi z)} = i\frac{e^{\pi i z} + e^{-\pi i z}}{e^{\pi i z} - e^{-\pi i z}}.$$

- On the horizontal lines we have

$$|f(z)| \le \frac{1}{M^2}\frac{e^{\pi M} + e^{-\pi M}}{e^{\pi M} - e^{-\pi M}} \implies \left|\int_{\alpha_i} f(z)dz\right| \le \frac{1}{M^2}\frac{e^{\pi M} + e^{-\pi M}}{e^{\pi M} - e^{-\pi M}} \times (M+1) \to 0.$$

- On the vertical line $z = M + 1/2 + it$,

$$\frac{\cos(\pi z)}{\sin(\pi z)} = i\frac{e^{-\pi t}(-1)^M i + e^{\pi t}(-1)^{-M}(-i)}{e^{-\pi t}(-1)^M i - e^{\pi t}(-1)^{-M}(-i)} = i\frac{e^{-\pi t} - e^{-\pi t}}{e^{-\pi t} + e^{-\pi t}}.$$

  Hence its absolute value is less than $1$. And we deduce again that the integral tends to $0$.

- On the vertical line $z = -M - 1/2 + it$, we have a similar bound.

Thus, taking $M \to \infty$ we deduce the sum of the series.

Another important consequence is the argument principle: if $f(z)$ is meromorphic and does not vanish on the image of the simple closed curve $\alpha$,

$$\frac{1}{2\pi i}\oint_\alpha \frac{f'(z)}{f(z)}dz = N(0) - N(\infty), \qquad (4.7)$$

where $N(0)$ is the number of $0$s surrounded by $\alpha$ and $N(\infty)$ the number of poles surrounded by $\alpha$. This is a simple verification using the Residues Theorem.

**Theorem 4.30** (Rouché's Theorem)**.** *Let $\mathcal{D}$ be a simply-connected [e.g., convex, star-shaped,...] and let $\alpha$ be a simple closed curve on $D$. Let $f(z)$ and $g(z)$ be analytic functions on $\mathcal{D}$.*

*If $|g(z)| < |f(z)|$ for each $z \in \texttt{Image}(\alpha)$, then $f(z)$ and $f(z) + g(z)$ have the same number of zeros in the interior of $\alpha$, counting multiplicities.*

*Proof.* We apply Equation 4.7 to $h_s(z) := f(z) + sg(z)$, $s \in [0,1]$. The integral actually varies continuously on $s$. Hence we deduce the conclusion. $\square$

**Theorem 4.31** (Inverse Function Theorem)**.** *Let $f(z)$ be analytical on some circle $|z| < R$, with $f(0) = 0$, $f'(0) \ne 0$ and $f(z) \ne 0$ for $0 < |z| < R$.*

*There is a unique $z = g(w)$, analytic at $w = 0$, which is the local inverse of $f(z) = w$ with $g(0) = 0$.*

*Proof.* Formally, the coefficients of $g$ are uniquely defined from $g(f(z)) = z$. Thus it is enough to show the existence.

Let $0 < r < R$. Define

$$g(w) = \frac{1}{2\pi i}\oint_{|v|=r} \frac{vf'(v)}{f(v) - w}dv.$$

The integrand is well-defined provided that $w$ is sufficiently small, because $\min_{|v|=r}|f(v)| > 0$ by our conditions. Thus $g(w)$ is well-defined on some neighborhood of $w = 0$. Moreover, we remark that $g(w)$ is actually holomorphic. This can be verified directly $g'(w) = \frac{1}{2\pi i}\oint_{|v|=r}\frac{vf'(v)}{(f(v)-w)^2}dv$.

We claim $g(w)$ is the inverse we look for. First, we remark that

$$\texttt{res}\left(\frac{vf'(v)}{f(v)-f(z)}; v = z\right) = \frac{zf'(z)}{f'(z)} = z\,,$$

which is a simple pole. Hence, if we can prove that the only zero of the denominator is $v = z$, the Residue Theorem tells us that $g(f(z)) = z$.

We prove that there is only one $v$ with $|v| < r$ such that $f(v) = f(z)$. Let $w = f(z)$. Supposing we are in a small enough neighborhood of $z = 0$, $|f(s)| > w = |f(z)|$. By Rouché's Theorem (Theorem 4.30), we conclude that $f(s)$ and $f(s) - w$ have the same number of zeros on $|s| < r$, i.e., a simple zero.    □

Now we are ready to prove the Lagrange Inversion Theorem. We recall it here.

**Theorem 2.22.** *Consider formal power series $f(u)$ and $\phi(u)$, with $\phi(0) \neq 0$. There is a unique power-series $u(t)$ satisfying*

$$u(t) = t\,\phi(u(t))\,.$$

*Further, the coefficients of $f(u(t))$ around $t = 0$ satisfy:*

$$[t^n]f(u(t)) = \frac{1}{n}[u^{n-1}]\{f'(u)\phi(u)^n\}\,.$$

*Proof.* For the proof we follow [5]. First, we may suppose $f$ and $\phi$ are polynomials, as we are interested in some coefficient $t^n$, thus truncating all larger degrees. This means that, for example, $f'(u)(\phi(u))^n$ is analytical (in fact, entire). Moreover, $t(u) := u/\phi(u)$ is also analytic in some neighborhood of $u = 0$, since the set of roots of $\phi(u) = 0$ is discrete, being a polynomial.

We have

$$\begin{aligned}
[u^{n-1}]\{f'(u)(\phi(u))^n\} &= [u^{n-1}]\{f'(u)(u/t(u))^n\} \\
&= [u^{-1}]\left\{\frac{f'(u)}{(t(u))^n}\right\} \\
&= \frac{1}{2\pi i}\oint_C \frac{f'(u)}{(t(u))^n}du \\
&= \frac{1}{2\pi i}\oint_{C'} t^{-n}f'(u(t))u'(t)dt \\
&= [t^n]\{t\tfrac{d}{dt}f(u(t))\} \\
&= n\,[t^n]\,f(u(t))\,.
\end{aligned}$$

Here the first and second equalities are direct. The third equal sign is the Residue Theorem (Theorem 4.27) applied to the meromorphic function $u \mapsto f'(u)/(t(u))^n$, in some small enough circle $C$ around $u = 0$. The fourth equal sign needs some explaining. We show that the inverse of $t(u)$, which we write $u(t)$, exists and is unique on some neighborhood of $t = 0$. Indeed, $g(u) = u/\phi(u)$ satisfies the hypothesis of Theorem 4.31 since $\phi(0) = 1$. Thus, making $C$ still smaller if needed, we may apply the inversion theorem and set $u = u(t)$ and the equality is the change of variables, where $C' = t(C)$. The fifth equality is Cauchy's Integral Theorem, and the last one is clear.    □

## 4.5. Analytic functions and singularities

A singularity is a point in which the function ceases to be analytic/holomorphic. Here is a table of the different categories of singularities:

| Type | Condition | Example |
|------|-----------|---------|
| Pole $(n)$ | $(z-a)^n f(z) \to$ finite | $\frac{1}{(z-a)^2}$ |
| Essential | No limit | $e^{1/z}$ |
| Branch | Multi-valued | $\sqrt{z}, \log z$ |

### 4.5.1   The logarithm and branch singularities

Unlike the real case, the logarithm has several possible definitions on the complex plane. We recall that $e^{2\pi i k} = 1$ for every $k \in \mathbb{Z}$, hence if $z = \exp(u)$ also $z = \exp(u + 2\pi i k)$.

We define

$$\log z \triangleq \log|z| + \arg(z) \times i\,, \tag{4.8}$$

where $\arg(z)$ is comprised in $(-\pi, \pi]$. This is known as the *main branch* of the logarithm.



Imaginary part of log(z) over the complex plane
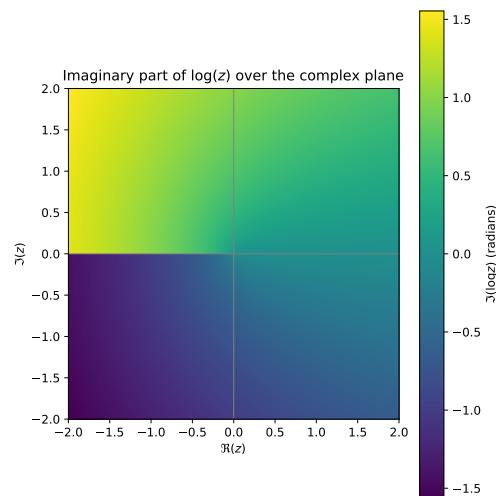
Looking at the picture of the imaginary part of the logarithm, we realize that there is a discontinuity on the $(-\infty, 0)$. When we tend to the semi-line $(-\infty, 0)$ from the semi-plane $\Im(z) > 0$ we have $\arg(z) \to \pi$, while from the semi-plane $\Im(z) < 0$ we have $\arg(z) \to -\pi$. In fact, we see that the logarithm cannot be extended continuously to the semi-line $(-\infty, 0]$.

Using the logarithm we may define square roots in all generality. For $\alpha \notin \mathbb{Z}$ we define:

$$z^\alpha \triangleq \exp(\alpha \times \log z)\,, \qquad z \in \mathbb{C} \smallsetminus (-\infty, 0]\,.$$

We remark again that this produces the same issues that with the logarithm.

**Example.** $z \mapsto \sqrt{z}$ is analytic on $\mathbb{C} \smallsetminus (-\infty, 0]$, but cannot be extended.



Argument of $\sqrt{z}$ over the complex plane
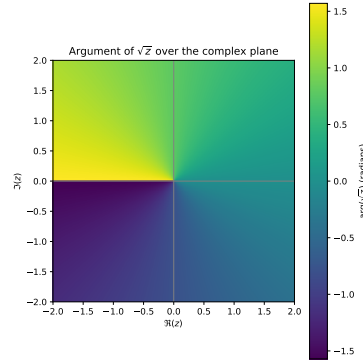
**Exercise 4.32.** Suppose $\alpha \in \mathbb{Z}$. Why is $z \mapsto \exp(\alpha \times \log z)$ well-defined on $z \neq 0$ in this case?

### 4.5.2  Analytic extension

We have seen that the logarithm and non-integer powers of $\alpha$ cannot be extended beyond $\mathbb{C} \smallsetminus (-\infty, 0]$. This is quite strong: thy cannot even be extended to a continuous function on $\mathbb{C} \smallsetminus \{0\}$.

This is not always the case. Sometimes functions defined on some domain can be extended. A key result is that the analytic extension is unique.

**Proposition 4.33.** *Consider a domain $\mathcal{D}$ [open and path connected], and let $f : \mathcal{D} \to \mathbb{C}$ analytic.*

*If there exists a sequence $(z_n)_n$ of distinct points in $\mathcal{D}$ such that $f(z_n) = 0$ and $z_n \to z_\infty \in \mathcal{D}$, then $f(z) \equiv 0$.*

*Proof.* We may assume without loss of generality that $z_n \neq z_\infty$ for all $n$.

The function $f(z)$ is analytic at $z = z_\infty$. Hence $f(z) = \sum_{n \geq 0} a_n (z - z_\infty)^n$ on some disk $D(z_\infty, r)$.

For all $k$ sufficiently large, $z_k \in D(z_\infty, r)$. Thus $f(z_k) - f(z_\infty) = \sum_{n \geq 1} a_n (z_k - z_\infty)^n$. But $f(z_k) - f(z_\infty) = 0$, hence $\sum_{n \geq 1} a_n (z_k - z_\infty)^n = 0$ and dividing by $z_k - z_\infty \neq 0$ we obtain $\sum_{n \geq} a_{n+1} (z_k - z_\infty)^n = 0$. Since $z_k \to z_\infty$, this means $a_1 = 0$ too. The argument continues and we prove that $a_n = 0$ for all $n$.

We deduce that $f(z) \equiv 0$ for $z \in D(z_\infty, r)$. The argument then follows by connectedness. $\qquad\square$

A key corollary is the following:

**Theorem 4.34.** *Uniqueness of the analytic extension Let us consider domains $\mathcal{D} \subset \hat{\mathcal{D}}$. Let $f : \mathcal{D} \to \mathbb{C}$ and suppose $\hat{f} : \hat{\mathcal{D}} \to \mathbb{C}$ is analytic and satisfies $\hat{f}|_{\mathcal{D}} \equiv f$.*

*Then $\hat{f}$ is the unique analytic extension of $f$ to $\hat{\mathcal{D}}$.*

*Proof.* Two analytic extensions must coincide on $\mathcal{D}$. Then the result follows from Proposition 4.33. $\qquad\square$

**Example 4.35.** We consider two examples:

- The geometric series $f(z) = \sum_{n=0}^{\infty} z^n$ defines an analytic function on $|z| < 1$.

  We know that $f(z) = \frac{1}{1-z}$ holds for $|z| < 1$: $\tilde{f}(z) = \frac{1}{1-z}$ is its analytic extension to $\mathbb{C} \smallsetminus \{1\}$.

- There is a unique analytic extension to $\mathbb{C} \smallsetminus (-\infty, 0]$ of the function $t \mapsto \log t$, defined on $t \in \mathbb{R}_{>0}$. [use Proposition 4.33]

A simple example of analytic extension is the following

**Theorem 4.36** (Removable singularities). *Let $\mathcal{D}$ be open. If $f(z)$ is analytic on $\mathcal{D} \smallsetminus \{z_0\}$ and bounded as $z \to z_0$, then it can be analytically extended to $z_0$.*

*Proof.* Without loss of generality suppose $z_0 = 0$. Define $h(z) = z^2 f(z)$ for $z \neq 0$, and $h(0) = 0$. We can verify that $h(z)$ is differentiable at $z = 0$. Indeed $(h(z) - 0)/z = zf(z) \to 0$ as $z \to 0$ by the boundedness of $f(z)$. Hence it is analytic on $\mathcal{D}$. Consider its power-series development at $z = 0$, $h(z) = \sum_{n \geq 0} a_n z^n$. It is easy to verify that $a_0 = a_1 = 0$. Then $h(z) = z^2 f(z)$ implies $f(z) = \sum_{n \geq 0} a_{n+2} z^n$ for $z \neq 0$, but, of course, the series on the right is an analytic extension also for $z = 0$. $\qquad\square$

**Example 4.37.** The function $\sin(z)/z$ has a removable singularity at $z = 0$.

**Example 4.38.** Let us determine the radius of convergence of $f(z) = \frac{z}{e^z - 1}$. We see that the singularities can occur only when $e^z = 1$, i.e., $z = 2\pi i k$ for some $k \in \mathbb{Z}$. The singularity at $z = 0$ is removable, since the limit exists. The rest are indeed poles of order one since

$$\lim_{z \to z_k} (z - z_k) f(z) = \lim_{z \to z_k} z \frac{z - z_k}{e^z - e^{z_k}} = z_k \frac{1}{e^{z_k}} = z_k \,,$$

for $z_k = 2\pi i k$ with $k \neq 0$. The singularities closest to the origin are $2\pi i$ and $-2\pi i$. Thus $\rho = 2\pi$.

### 4.5.3 Dominant singularities

We already know that if a power-series $f(z)$ has radius of convergence $\rho < \infty$, then there must be some singularity at $|z| = \rho$.

If the coefficients $f(z) = \sum_{n \geq 0} f_n z^n$ are non-negative, $f_n \geq 0$, we can say a lot more regarding the position of the singularities.

Firstly, we can say that $z = \rho$ is itself a singularity.

**Theorem 4.39** (Pringsheim's Theorem). *Suppose $f(z)$ is analytic at the origin, and that the coefficients in the expansion are all non-negative. If the radius of convergence is $\rho < \infty$, then $\rho$ is a singularity of $f$.*

*Proof.* We follow [3]. Suppose otherwise, then there is $\epsilon > 0$ such that $f(z)$ can be made analytic in the open ball $D(\rho, \epsilon)$. Now let $0 < h < \frac{1}{3}\epsilon$ and $z_0 = \rho - h$.

We note that, as $f(z) = \sum_{n \geq 0} f_n z^n$, then $f(z) = \sum_{n \geq 0} f_n \left((z - z_0) + z_0\right)^n$ and so, by developing the binomials on the right

$$f(z) = \sum_{n \geq 0} f_n \sum_{m \geq 0} \binom{n}{m} z_0^{n-m} (z - z_0)^n$$

$$= \sum_{m \geq 0} \left( \sum_{n \geq 0} \binom{n}{m} f_n z_0^{n-m} \right) (z - z_0)^n \,,$$

which is valid for real $z \in [z_0, z_0 + h)$ because in such a case all of the terms are positive. This means that the coefficients of the power series expansion of $f(z)$ are necessarily equal to $g_m = \sum_{n \geq 0} \binom{n}{m} f_n z_0^{n-m} \geq 0$.

Next observe that, since $f$ remains analytic within a disc of $z_0$ containing $\rho + H$, we have the convergent

series

$$f(\rho + h) = \sum_{m \geq 0} g_m (2h)^m$$

$$= \sum_{m \geq 0} \left( \sum_{n \geq 0} \binom{n}{m} f_n z_0^{n-m} \right) (2h)^m$$

$$= \sum_{n \geq 0} f_n \left( \sum_{m \geq 0} \binom{n}{m} (2h)^m z_0^{n-m} \right)$$

$$= \sum_{n \geq 0} f_n (z_0 + 2h)^n$$

$$= \sum_{n \geq 0} f_n (\rho + h)^n \,,$$

where interchanging the summations is valid because all of the terms are positive. Therefore we have $f_n = o((\rho + h)^{-n})$, but this is absurd, since this would mean the radius of convergence is then at least $\rho + h/2 > \rho$. $\qquad\square$

[Daffodil]

## 5. Coeficient Asymptotics

### 5.1. Meromorphic functions: the "almost" rational functions

Meromorphic functions are essentially "locally" rational functions:

**Definition 5.1.** A function $f : \mathcal{D} \to \mathbb{C}$ is meromorphic at $z_0 \in \mathcal{D}$ if and only if, on a neighborhood of $z = z_0$, $f(z) = \frac{g(z)}{h(z)}$ for some $g(z)$ and $g(z)$ analytic at $z = z_0$.

**Example 5.2.** The function $D(z) = \frac{1}{1-2z} \log\left(\frac{1}{1-z}\right)$ behaves locally like a rational function around $z \sim 1/2$. Indeed, $D(z) \sim \frac{1}{1-2z} \log(2)$. Thus

$$D(z) - \frac{1}{1-2z} \log(2) = \frac{1}{1-2z} \left( \log\left(\frac{1}{1-z}\right) - \log 2 \right) \to -1 \,,$$

as $z \to 1/2$, where we have applied L'Hôpital's rule. This means, by Theorem 4.36, that the singularity is removable and that

$$F(z) = D(z) - \frac{1}{1-2z} \log(2) \,,$$

is analytic at $z = 1/2$. Thus we have increased the radius of convergence from $\rho_D = 1/2$ to $\rho_F = 1$.

By the Cauchy-Hadamard Theorem, see Theorem 4.3, we deduce

$$[z^n]D(z) - [z^n]\frac{1}{1-2z} \log(2) = [z^n]F(z) = O((1+\epsilon)^n)$$

for every $\epsilon > 0$. That is $[z^n]D(z) = 2^n \log 2 + O((1+\epsilon)^n)$.

Of course, this is a toy example as $[z^n]D(z) = \sum_{j=1}^{n} 2^{n-j}/j$, which we can directly work with. But notice that generalizes very easily to more difficult functions.

**Genral method.** This is typical of meromorphic functions: the singularities are poles that can be "cleaned" as if the functions were rational.

---

– Consider $g(z) = \sum_{n \geq a} g_n (z - z_0)^n$ y $h(z) = \sum_{n \geq b} h_n (z - z_0)^n$ with[6] $b > a$:

$$\frac{g(z)}{h(z)} = \frac{\sum_{n \geq a} g_n (z - z_0)^n}{\sum_{n \geq b} h_n (z - z_0)^n} = (z - z_0)^{a-b} \times \sum_{n=0}^{\infty} c_n (z - z_0)^n,$$

where the last factor is analytic at $z = z_0$.

– Expanding

$$\frac{g(z)}{h(z)} = \frac{c_0}{(z - z_0)^{b-a}} + \frac{c_1}{(z - z_0)^{b-a-1}} + \ldots + \frac{c_{b-a-1}}{z - z_0} + \texttt{analytic at } z = z_0.$$

In conclusion

$$\tilde{f}(z) := f(z) - \left( c_0 \frac{1}{(z - z_0)^{b-a}} + c_1 \frac{1}{(z - z_0)^{b-a-1}} + \ldots + c_{b-a-1} \frac{1}{z - z_0} \right),$$

is analytic at $z = z_0$. Thus we essentially obtain the coefficients as if the function were rational.

## 5.2. Analysis of run-length encoding

One of the advantages of meromorphic functions is that we do not need a complete knowledge of the function, we just need to know that the dominant singularities behave as poles. We give an example of this.

**Input.**　Consider an infinite binary words $W = 0^{X_1} 1 0^{X_2} 1 \ldots$ where $X_1, X_2, \ldots$ are iid random variables with distribution $p(k) = \Pr(X = k)$, $q(k) = \Pr(X \geq k)$.

Fixing $n \geq 0$, we intend to encode $W_n = w_1 w_2 \ldots w_n$, the prefix of the first $n$ bits.

Given a code[7] $c\colon \{0, 1\}^\star \to \{0, 1\}^\star$ we are interested in

$$\tfrac{1}{n} |c(W_n)|,$$

which is the rate of output bits per input bit.

**Runlength encoding.**　We say that a code $c\colon \{0, 1\}^\star \to \{0, 1\}^\star$ is a *runlength encoding* iff it satisfies $c(0^i 1 w) = c(0^i 1) c(w)$ for all $i \geq 0$ and $w$.

Writing $\ell_i = |c(0^i 1)|$ and $r_i = |c(0^i)|$ for each $i$, we remark that

$$|c(0^{i_1} 1 \ldots 0^{i_k} 1 0^j)| = \ell_{i_1} + \ldots + \ell_{i_k} + r_j.$$

We suppose, wlog, that $r_i = O(\ell_i)$ and $\ell_i = O(i)$.

**Simplifying hypothesis.**　We suppose that $A(z) = \sum_k p(k) z^k$ is analytic on $|z| \leq 1 + \delta$ for some fixed $\delta > 0$.

---

[6]Otherwise there would be no singularity due to Theorem 4.36.
[7]See Example 4.5.

**Main result.**   We are going to prove that

$$\lim_{n\to\infty} \frac{1}{n} |c(W_n)| = \frac{\mathbb{E}[|c(0^X 1)|]}{\mathbb{E}[|0^X 1|]} , \tag{5.1}$$

in probability.

**Convergence in probability.**   We recall that $a_n \to L$ in probability if and only if, for each $\varepsilon > 0$ we have $\Pr\{|a_n - L| \ge \varepsilon\} \to 0$. Similarly we say that $a_n \sim b_n$ in probability iff $a_n/b_n \to 1$ in probability.

How to prove this?

**Proposition 5.3.** *Consider a sequence of random variables $(X_n)$ such that $e_n = \mathbb{E}[X_n] \to \infty$. If $\mathbb{E}[X_n^2] \sim e_n^2$ as $n \to \infty$, we have that $X_n \sim e_n$ in probability.*

*Proof.* This is a direct consquence of Chebyshev's inequality.  Equivalently the statement holds if $\mathtt{Var}(X_n) = O(e_n^2)$.  □

**Proof of the result.**   We define

$$F(z,y) = \sum_{w\in\{0,1\}^\star} \mathbf{P}_{|w|}(w) z^{|w|} y^{|c(w)|} = \sum_k z^k \sum_{w\in\{0,1\}^k} \mathbf{P}_k(w) y^{|c(w)|} ,$$

where $\mathbf{P}_k(w)$ is the probability of $W_k = w$, for a given $w \in \{0,1\}^k$.

The firt key observation is the following:

**Lemma 5.4.** *Let $A(z,y) = \sum_k p(k) z^k y^{\ell_k}$ and $B(z,y) = \sum_k q(k) z^k y^{r_k}$,*

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

*Proof.* Essentially, we decompose the words into a sequence of $0^\star 1$ followed by a tail $0^\star$.  The PGFs $A(z,y)$ is the generating function of the blocks $0^\star 1$, while $B(z,y)$ is the PGF of the tail of $0$s. Since each block $0^\star 1$ is independent, we may apply the same dictionary.  □

We begin by considering the expected value. As explained in Section 2.5, the OGF of $\mathbb{E}[|c(W_n)|]$ is

$$\partial_y F(z,1) = \frac{\partial_y B(z,1)}{1 - z\, A(z,1)} + z\frac{B(z,1)\partial_y A(z,1)}{(1 - z\, A(z,1))^2} .$$

In order to simplify this, observe that, being PGFs,

$$\frac{1}{1-z} = F(z,1) = \frac{B(z,1)}{1 - z\, A(z,1)} . \tag{5.2}$$

A few remarks are in order

1. $B(z,1)$ is analytic at $|z| \le 1 + \epsilon$, and $B(1,1) = \mathbb{E}[|0^X 1|]$,

2. The derivatives $\partial_y A(z,1)$ and $\partial_y B(z,1)$ are also analytic on $|z| \le 1 + \epsilon$. In addition $\partial_y A(z,1) = \mathbb{E}[|c(0^X 1)|]$.

---

[7]Remember $p(k) = \Pr(X = k)$, $q(k) = \Pr(X \ge k)$, $\ell_k = |c(0^k 1)|$, $r_k = |c(0^k)|$.

3. The function $z \mapsto \frac{1}{1-zA(z,1)}$ is meromorphic on $|z| \le 1 + \epsilon$, with a simple pole at $z = 1$

$$\frac{1}{1-zA(z,1)} = \frac{(B(z,1))^{-1}}{1-z} \sim \frac{(B(1,1))^{-1}}{1-z} .$$

Looking at the contributions at $z = 1$, for the asymptotics it is enough to consider the largest power of $(1 - z\,A(z,1))^{-1}$ only:

$$\partial_y F(z,1) \sim \frac{1}{(1-z)^2} \frac{\partial_y A(1,1)}{B(1,1)} = \frac{1}{(1-z)^2} \frac{\mathbb{E}[|c(0^X 1)|]}{\mathbb{E}[|0^X 1|]} .$$

Thus, since it is meromorphic, we extract the asymptotics as with rational functions (see **??**) :

$$\mathbb{E}[|c(W_n)|] \sim n \frac{\mathbb{E}[|c(0^X 1)|]}{\mathbb{E}[|0^X 1|]} .$$

To apply Proposition **??**, we obtain the asymptotics of the second moment

$$\mathbb{E}[|c(W_n)|^2] = [z^n]\Big\{(y\partial_y)^2 F(z,1)\Big\} .$$

Calculating:

$$(y\partial_y)^2 F(z,1) = \frac{\partial_y B(z,1)}{1-zA(z,1)} + z \frac{B(z,1)\partial_y A(z,1)}{(1-zA(z,1))^2}$$

$$+z\frac{\partial_y B(z,1)\partial_y A(z,1)}{(1-zA(z,1))^2} + z\frac{B(z,1)\partial_y^2 A(z,1)}{(1-zA(z,1))^2} + 2z^2 \frac{B(z,1)(\partial_y A(z,1))^2}{(1-zA(z,1))^3} .$$

Now, by the same argument, we just look at the term with the denominator of the highest power when $z \to 1$:

$$(y\partial_y)^2 F(z,1) \sim 2\frac{B(z,1)(\partial_y A(1,1))^2}{(1-zA(z,1))^3} = \frac{2}{(1-z)^3}\left(\frac{\mathbb{E}[|c(0^X 1)|]}{\mathbb{E}[|0^X 1|]}\right)^2 .$$

From which we deduce $\mathbb{E}[|c(W_n)|^2] \sim 2\frac{n^2}{2}\left(\frac{\mathbb{E}[|c(0^X 1)|]}{\mathbb{E}[|0^X 1|]}\right)^2$                    □

## 5.3. Transfer Theorem

For the moment we have treated polar singularities. The asymptotics for this case are derived as for rational functions. But what about other kinds of singularities and domains?

We have briefly mentioned other singularities. For instance, in Example 2.2 we had a square-root singularity, for which we applied Newton's Binomial Theorem.

We recall that

$$\sum_{n\ge 1} H_n z^n = \frac{1}{1-z}\log\left(\frac{1}{1-z}\right)$$

where $H_n = \frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{n}$ are the harmonic numbers, and $H_n = \log n + \gamma + o(1)$ where $\gamma$ is the Euler-Mascheroni constant.

**Example 5.5.** Consider now

$$A(z) = \sum a_n z^n = \frac{1}{(1-z)^2} \log\left(\frac{1}{1-z}\right),$$

what are the coefficients like?

Integrating we find

$$\sum \frac{a_n}{n+1} z^{n+1} = \int_0^z A(u)du = \int_0^z \frac{1}{(1-u)^2} \log\left(\frac{1}{1-u}\right) du.$$

Integrating by parts

$$\int_0^z \frac{1}{(1-u)^2} \log\left(\frac{1}{1-u}\right) du = \frac{1}{1-z} \log\left(\frac{1}{1-z}\right) - \int_0^z \frac{du}{(1-u)^2} = \frac{1}{1-z} \log\left(\frac{1}{1-z}\right) - \frac{z}{1-z}.$$

Hence we deduce that $a_n/(n+1) \sim H_n$, i.e., $a_n \sim n \log n$.

**Exercise 5.6.** Find the asymptotics of the coefficients of $\log\log\left(\frac{1}{1-z}\right)$ directly.

Many kinds of asymptotics can be derived as above from simple considerations, and/or the Newton Generalized Binomial. But there is a more general result, that systematically covers all of these cases, without the need to consider each of them specifically. Moreover, and **very** importantly, it just requires a local estimate of the asymptotics of the generating function around its main singularity. We do not need an exact formula for the generating function.
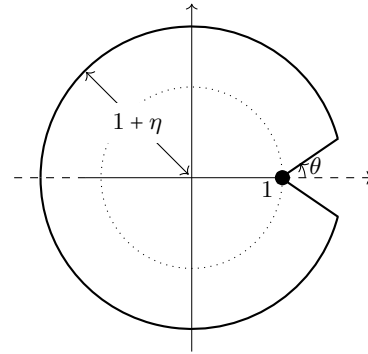
Such a theorem is called a *Transfer Theorem*. It transfers asymptotics for the function at its dominant singularity to asymptotics for the coefficients.

Let us consider more general domains than $\mathbb{C} \smallsetminus [1, \infty)$:

"Camembert" or "Pacman" 🟡 domain:

$$\Delta(\theta, \eta) = \{z : |z| \le 1 + \eta, \quad \arg(z-1) \ge \theta\}.$$

Suppose $f(z)$ were analytic on $\Delta(\theta, \eta)$, except possible at $z = 1$.



**Theorem 5.7** (Transfer Theorem – Flajolet, Odlyzko [2]). *If* $f(z) \sim \frac{1}{(1-z)^\alpha} \left(\log(\frac{1}{1-z})\right)^\beta$ *when* $z \to 1$, $\alpha \ne -1, -2, \ldots$, *then*

$$[z^n]f(z) \sim \frac{n^{\alpha-1}}{\Gamma(\alpha)} (\log n)^\beta.$$

**The Gamma Function.**   For $\mathfrak{R}(z) > 0$ we may define

$$\Gamma(z) \triangleq \int_0^\infty t^{z-1} e^{-t} dt.$$

- This function satisfies $\Gamma(z+1) = z\Gamma(z)$: it extends the factorials $\Gamma(n+1) = n!$, $n \in \mathbb{Z}_{\ge 0}$.

- We can also prove[8] that $\Gamma(\frac{1}{2}) = \sqrt{\pi}$, and consequently $\Gamma(-\frac{1}{2}) = -2\sqrt{\pi}$

The Gamma function can be analytically extended to $\mathbb{C} \smallsetminus \{-1, -2, \ldots\}$. In fact, it is often defined by[9]

$$\frac{1}{\Gamma(z)} = ze^{\gamma z} \prod_{n=1}^{\infty} \left[ \left(1 + \frac{z}{n}\right) e^{-z/n} \right],$$
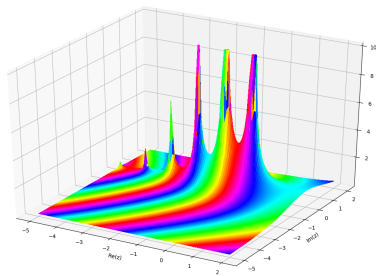
where $\gamma \triangleq \lim_{n \to \infty} (H_n - \log n)$ is the Euler-Mascheroni constant.

This function appears often in the Analysis of Algorithms. It is important to note the following property

**Proposition 5.8.** *The Gamma function can be analytically extended to* $\mathbb{C} \smallsetminus \{-1, -2, \ldots\}$ *and it has simple poles at the negative integers*

$$\Gamma(z) \sim \frac{(-1)^n / n!}{z + n},$$

*as* $z \to -n$.



**Important remarks.**

- The singularity can be $\rho \neq 1$: apply result to a $g(z) = f(z/\rho)$.

- We may substitute $(\log \frac{1}{1-z})^{\beta}$ for any finite product $(\log \frac{1}{1-z})^{\beta_1} (\log \log \frac{1}{1-z})^{\beta_2} (\log \log \log \frac{1}{1-z})^{\beta_3} \cdots$.

- It applies changing $\sim$ for bounds such as $O$ and $o$.

- Can be generalized to any finite number of singularities on $|z| = 1$.

### 5.4. Analysis of Quicksort

We give a first simple application of the Transfer Theorem. You most likely know that the number of comparisons performed by QuickSort over a random permutation of $n$ numbers is $O(n \log n)$ on average. Actually, it is $\sim 2n \log n$ on average and, moreover, it is $\sim 2n \log n$ in probability! That is to say: it is $\Theta(n \log n)$ with high probability.

First, we suppose that the input is an array of $n$ uniform elements from $[0, 1]$. This clearly corresponds to a permutation of $n$ elements. Second, we suppose that the pivot is always the first element in the array. Of course, this is not a good idea in practice, but for our ranom model this does not change a thing, as all elements are uniform.

The algorithm of QuickSort can be realized as a tree: a binary search tree (BST). The root of the tree is the pivot (the first element in the array), which is a uniform element, the left-branch $T_L$ contains all elements smaller than the pivot, and the right-branch $T_R$ all elements larger than the pivot.

---

[8]A change of variables brings us to the Gaussian integral $\int_{-\infty}^{\infty} e^{-t^2} dt = \sqrt{\pi}$.
[9]This is Weierstrass' definition. The notation $\Gamma$ was introduced by Legendre.
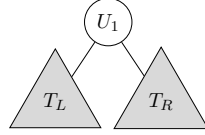
What is the cost in comparisons at this stage? It is $|T_L| + |T_R|$. Then this continues recursively on $T_L$ and $T_R$. We remark that, at the end, the cost is the average depth of the nodes of the tree!

Hence let us look at the algorithm the other way around. First we pick the pivot uniformly at random, and then we work recursively: the elements in $T_L$ belong to $[0, U_1]$ and those from $T_R$ to $[U_1, 1]$. Rescaling the intervals, this is just the same process.

Define $F(z, u) = \sum_{n,k} p_n(k) z^n u^k$ where $p_n(k)$ is the probability that a tree with $n$ nodes costs $k$ for the algorithm.

**Proposition 5.9.**

$$F(z, u) = 1 + \int_0^z (F(zu, u))^2 dz$$

From this we can find the expected value and the second moment. In fact, we are going to use Proposition 5.3 in order to prove that the number of comparisons is $\sim 2n \log n$ in probability.

**Proposition 5.10.** *The number of comparisons $C_n(\pi)$ required by Quicksort on a uniform random permutation $\pi$, satisfies $C_n \sim 2n \log n$ in probability.*

– We begin by computing the first moment, the expected value. Differentiating the equation we have

$$\partial_u F(z, 1) = \int_0^z 2F(z, 1)\,(z\partial_z F(z, 1) + \partial_u F(z, 1))dz\,.$$

Since $F(z, 1) = \frac{1}{1-z}$, it follows that $\partial_z F(z, 1) = \frac{1}{(1-z)^2}$. Thus, if we let $g(z) := \partial_u F(z, 1)$ we obtain

$$g'(z) = \frac{2}{1-z}\left(\frac{z}{(1-z)^2} + g(z)\right)\,.$$

We consider [more about this in a second]

$$(g(z) \cdot (1-z)^2)' = (1-z)^2 \times \left(g'(z) - \frac{2}{1-z}g(z)\right) = (1-z)^2 \frac{2z}{(1-z)^3} = \frac{2z}{1-z}\,.$$

Integrating

$$g(z) \cdot (1-z)^2 = 2\log\left(\frac{1}{1-z}\right) - 2z \implies g(z) = \frac{2}{(1-z)^2}\log\left(\frac{1}{1-z}\right) - \frac{2}{(1-z)^2}\,.$$

We deduce that the expected value is $[z^n]g(z) \sim 2n \log n$.

– The second moment requires heavier calculations, but can be simplified by Singular Integration (see below). We differentiate again:

$$\partial_u^2 F(z, 1) = 2\int_0^z \left(\partial_u F(z,1)(z\partial_z F(z,1) + \partial_u F(z,1)) + F(z,1)\left(z^2\partial_z^2 F(z,1) + 2z\partial_z\partial_u F(z,1) + \partial_u^2 F(z,1)\right)\right)dz\,.$$

Let $f(z) = \partial_u^2 F(z, 1)$. Then

$$f'(z) = 2\left(g(z)\left(\frac{z}{(1-z)^2} + g(z)\right) + \frac{1}{1-z} \cdot \left(\frac{2z^2}{(1-z)^3} + 2zg'(z) + f(z)\right)\right)\,.$$

Defining $K(z) := f(z) \cdot (1-z)^2$ as before, we can verify that

$$K'(z) = (1-z)^2 \times 2\left( g(z)\left( \frac{z}{(1-z)^2} + g(z) \right) + \frac{1}{1-z} \cdot \left( \frac{2z^2}{(1-z)^3} + 2zg'(z) \right) \right).$$

We need not compute the whole RHS here. It is enough to compute the asymptotic equivalent as $z \to 1$. Note that $g'(z) \sim \frac{2}{1-z} g(z)$ as $z \to 1$, comparing terms we deduce

$$K'(z) = (1-z)^2 \times 2(g(z))^2 + O(g(z)),$$

as $z \to 1$.

The following is a particular case of singular integration. Actually, in our case, it would be enough to consider that all terms are of the form $\frac{1}{(1-z)^a}(\log \frac{1}{1-z})^b$ with $a, b$ non-negative integers.

**Lemma 5.11** (Singular integration [3, Theorem VI.9]). *Let $r(z)$ be $\Delta$-analytic and satisfy $r(z) = O((1-z)^{-2}\log(1-z))$ on some neighborhood of $z = 1$. Then $\int_0^z r(u)du = O((1-u)^{-1}\log(1-u))$.*

*Proof.* We decompose the integral into two parts. The arc made of those $\zeta$ such that $|1-\zeta| = |1-z|$, from the real line to $z$, and the line segment from $0$ to $r = 1 - |1-z|$. Suppose $|1-z|$ is small enough so that $|r(\zeta)| \le K|1-\zeta|^{-2}|\log(1-\zeta)|$ for a fixed constant $K > 0$, on the circle part of the path.

In order to bound, we may assume that $|1-z|$ is also small enough so that $\log \frac{1}{|1-\zeta|} \ge 2\pi$. Thus, on the arc we have $|r(\zeta)| \le K|1-\zeta|^{-2}|\log(1-\zeta)| \le 2K|1-\zeta|^{-2}(\log \frac{1}{|1-\zeta|})$. The arc has length at most $2\pi|1-\zeta|$ and the result follows for this part of the integral.

For the line segment from $0$ to $r$ we just need to compare with the real integral $\int_0^r \frac{1}{(1-x)^2}\log \frac{1}{1-x}dx = \frac{1}{1-r}\log \frac{1}{1-r} - \frac{r}{1-r}$. Thus we are done because $1-r = |1-z|$ and $|\log(\frac{1}{1-z})| \ge \log \frac{1}{|1-z|}$. $\qquad\square$

Now, by singular integration we deduce

$$K(z) \sim 2\int_0^z (1-z)^2 \times (g(z))^2 dz$$

$$= 8\int_0^z \frac{1}{(1-z)^2}\log\left(\frac{1}{1-z}\right)^2 dz$$

$$= \frac{8}{1-z}\log\left(\frac{1}{1-z}\right)^2 - 16\int_0^z \frac{1}{1-z}\log\left(\frac{1}{1-z}\right)dz$$

where we have integrated by parts. The latter integral can be computed to be $\frac{1}{1-z}\log\frac{1}{1-z} - \frac{z}{1-z}$, which is negligible compared to the first term $\frac{8}{1-z}\log\left(\frac{1}{1-z}\right)^2$.

It follows that $f(z) \sim \frac{8}{(1-z)^3}\log\left(\frac{1}{1-z}\right)^2$ as $z \to 1$. Thus $[z^n]f(z) \sim 4n^2\log(n)^2$ and we are done.

**A parenthesis regarding ODEs.** In general, the equation $u'(z) = a(z)u(z) + b(z)$ has a unique solution.

**Theorem 5.12.** *Suppose $a(z)$ and $b(z)$ are analytic at $z = 0$, then on a neighborhoof of $z = 0$*

$$u(z) = \exp\left(\int_0^z a(v)dv\right) \cdot \left(u(0) + \int_0^z \exp\left(-\int_0^u a(v)dv\right) \cdot b(u)du\right).$$

*Proof.* Define $v(z) := \exp\left(-\int_0^z a(v)dv\right) \cdot u(z)$. We obtain

$$v'(z) = \exp\left(-\int_0^z a(v)dv\right) \cdot \left(u'(z) - a(z)u(z)\right) = \exp\left(-\int_0^z a(v)dv\right) \cdot b(z).$$

The result follows by integrating.                                                                      □

## 6. The saddle-point inequality

### 6.1. The inequality

**Proposition 6.1** (Saddle-point bounds). *Assume $f(z)$ is analytic for $|z| < \rho$ with $0 < \rho \leq \infty$. Let us define $M(f;r) = \sup_{|z|=r} |f(z)|$ for $0 < r < \rho$. Then, for any $r \in (0, \rho)$ we have*

$$\left|[z^n]f(z)\right| \leq \frac{M(f;r)}{r^n}, \qquad \text{and so} \qquad \left|[z^n]f(z)\right| \leq \inf_{r \in (0,\rho)} \frac{M(f;r)}{r^n}, \tag{6.1}$$

*what is more, when $f(z)$ has non-negative coefficients at $0$ we have*

$$[z^n]f(z) \leq \frac{f(r)}{r^n}, \qquad \text{and so} \qquad [z^n]f(z) \leq \inf_{r \in (0,\rho)} \frac{f(r)}{r^n}. \tag{6.2}$$

*Proof.* We recall that we have

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

where the circle is positively-oriented. It follows then, by taking absolute values and using the triangle inequality, that

$$\left|[z^n]f(z)\right| \leq \frac{1}{2\pi} \oint_{|z|=r} \frac{|f(z)|}{|z|^{n+1}} d|z| = \frac{1}{2\pi} \oint_{|z|=r} \frac{|f(z)|}{r^{n+1}} d|z| \leq \frac{M(f;r)}{r^n},$$

which proves (6.1). Next for (6.2) we observe that when $f_k = [z^k]f(z)$ is non-negative for each $k$, we have

$$f_n \leq \frac{f_0}{r^n} + \ldots + f_n + \ldots + f_k r^{k-n} + \ldots = \frac{f(r)}{r^n},$$

which proves (6.2).                                                                                      □

**Remark 6.2.** Observe that, by differentiating, the bound in (6.2) can be optimized by choosing $r$ such that $\frac{\partial}{\partial r}\left(\frac{f(r)}{r^n}\right) = 0$, that is, such that

$$r\frac{f'(r)}{f(r)} = n, \tag{6.3}$$

of course, when this makes sense in view of the domain.

### 6.2. Example: integer partitions

We are going to show the following simple bound for integer partitions:

**Proposition 6.3.** *For any $c > \exp(\frac{\pi^2}{12}) = 2.276\ldots$, we have $p(n) \leq c \times \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$ for large enough $n$.*

The actual asymptotic is $p(n) \sim \frac{1}{4\sqrt{3}n} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$, a result due originally to Hardy and Ramanujan. A full, accessible and succinct account can be found in Analytic Number Theory by Donald J. Newman.

*Proof.* We are going to apply the saddle-point bound. First remark that $P(z) = \prod_{n=1}^{\infty}\left(\frac{1}{1-z^n}\right)$ can be rewritten as

$$P(z) = \exp\left(\sum_{n=1}^{\infty} \frac{1}{n}\frac{z^n}{1-z^n}\right).$$

We recall that $\frac{1-z^n}{1-z} = 1 + z + \ldots + z^{n-1}$, hence

$$\log P(z) = \frac{1}{1-z}\sum_{n=1}^{\infty} \frac{1}{n} \times \frac{z^n}{1+z+\ldots+z^{n-1}}.$$

For real $r > 0$ we have $1 + r + \ldots + r^{n-1} \geq nr^{n-1}$, thus

$$\log P(r) \leq \frac{1}{1-r}\sum_{n=1}^{\infty} \frac{1}{n^2}r = \frac{\pi^2}{6}\frac{r}{1-r}.$$

We conclude that, for $F(z) = \exp\left(\frac{\pi^2}{6}\frac{z}{1-z}\right)$,

$$[z^n]P(z) \leq \frac{P(r)}{r^n} \leq \frac{F(r)}{r^n}.$$

Let us apply the saddle-point bound to the function $F(z)$ instead of $P(z)$. The saddle-point equation is $n = \frac{z}{(1-z)^2}$. A good enough approximation of the saddle-point is $r = 1 - \frac{\pi}{\sqrt{6n}}$.

Then

$$F(r)/r^n = \exp\left(\pi\sqrt{\frac{n}{6}}\right) \times \left(1 - \frac{\pi}{\sqrt{6n}}\right)^{-n}.$$

We remark that, for $t \in (0,1)$,

$$\log\left(\frac{1}{1-t}\right) = t + \frac{t^2}{2} + \frac{t^3}{3} + \ldots \leq t + \frac{t^2}{2}\sum_{k=0}^{\infty} t^k = t + \frac{t^2}{2(1-t)}.$$

Hence $\left(1 - \frac{\pi}{\sqrt{6n}}\right)^{-n} \leq \exp\left(\pi\sqrt{\frac{n}{6}} + \frac{\pi^2}{12\cdot(1-\pi/\sqrt{6n})}\right)$ and the result follows by summing exponents. $\quad\square$

**Exercise 6.4.** Find a similar bound for the integer partitions into distinct parts.

## References

[1] Valérie Berthé, Loïck Lhote, and Brigitte Vallée. Probabilistic analyses of the plain multiple gcd algorithm. *Journal of Symbolic Computation*, 74:425–474, 2016.

[2] Philippe Flajolet and Andrew M. Odlyzko. Singularity analysis of generating functions. *SIAM J. Discrete Math.*, 3(2):216–240, 1990.

[3] Philippe Flajolet and Robert Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009.

[4] Walter Rudin. *Real and complex analysis, 3rd ed.* McGraw-Hill, Inc., USA, 1987.

[5] Herbert S. Wilf. *Generatingfunctionology*. A. K. Peters, Ltd., USA, 2006.