ANALYTIC COMBINATORICS

SARAH FUJIMORI AND SRITEJA VIJAPURAPU

Abstract. In this paper, we will introduce methods to analyze ordinary generating functions of combinatorial classes using complex analysis, including an exponential bound and saddle point upper bounds. We apply these bounds for unary-binary trees and coding theory. We will assume basic knowledge of combinatorics and complex analysis.

1. Combinatorial Classes and Generating Functions

In this section, we introduce and provide examples of combinatorial classes and generating functions, which we will analyze later in the paper. We start with the following definition:

Definition 1.1. A *combinatorial class* $\mathcal{C}$ is defined as a finite set with a size function that satisfies the following properties:

(1) Every $c \in \mathcal{C}$ is a non-negative integer
(2) The number of elements of any size is finite.

We denote $\{c \in \mathcal{C} : \text{size}(c) = n\}$ as $\mathcal{C}_n$.

Definition 1.2. The *counting sequence* of a combinatorial class $\mathcal{C}$ is the sequence $C_0, C_1, C_2, \ldots$, where $C_i = |\mathcal{C}_i|$ for each nonnegative integer i.

Example. Let $\mathcal{W}$ be the set of binary words (i.e., strings of 0s and 1s). Then, for each nonnegative integer n, $\mathcal{W}_n$ is the set of binary words of length n. For example,

$$\mathcal{W}_2 = \{00, 01, 10, 11\}.$$

Since each character in a word of length n is either 0 or 1, we have $W_n = |\mathcal{W}_n| = 2^n$, and the counting sequence of $\mathcal{W}$ is $1, 1, 2, 4, \ldots$.

Example. Let $\mathcal{P}$ be the set of permutations. Then, for each nonnegative integer n, $\mathcal{P}_n$ is the set of permutations of n objects, and the counting sequence of $\mathcal{P}$ is $0!, 1!, 2!, \ldots$ since $P_n = |\mathcal{P}_n| = n!$.

Example. We define $\mathcal{E} = \{\epsilon\}$ as the class only containing the neutral object, and $\mathcal{Z}$ as the class containing a single object or node of size 1.

We now introduce generating functions:

Definition 1.3. Let $A_0, A_1, \ldots$ be a sequence. Then the *ordinary generating function* (OGF) of the sequence is the series

$$\sum_{n=0}^{\infty} A_n x^n.$$

Example. The generating function $E(z)$ of $\mathcal{E}$ is 1, and the generating function $Z(z)$ of $\mathcal{Z}$ is z.

We will also discuss labelled classes, as defined below:

Definition 1.4. A *labelled class of combinatorial objects* is a class $\mathcal{C}$ such that every element can be labeled with a distinct integer.

We say the class is *well-labeled* if the objects can be labeled with the integers from $\{1, ..., n\}$ and *weakly labeled* if not (as long as they are distinct).

We can also construct other combinatorial classes from existing ones:

Definition 1.5. (1) Sum:

Let $\mathcal{B}, \mathcal{C}$ be combinatorial classes. Then, the sum is defined by

$$\mathcal{A} = \mathcal{B} + \mathcal{C} = (\{\square\} \times \mathcal{B}) \cup (\{\diamond\} \times \mathcal{C})$$

where $\square$ and $\diamond$ are markers for elements of $\mathcal{B}$ and $\mathcal{C}$ respectively. We can picture this as painting elements of $\mathcal{B}$ blue and painting elements of $\mathcal{C}$ red, and then taking the union of these elements. Note that this ensures that $A_n = B_n + C_n$ regardless of whether $\mathcal{B}$ and $\mathcal{C}$ are disjoint.

(2) Cartesian Product:

Let $\mathcal{B}, \mathcal{C}$ be combinatorial classes. Then, the cartesian product $\mathcal{A} = \mathcal{B} \times \mathcal{C}$ is the set of ordered pairs of elements of $\mathcal{B}$ and $\mathcal{C}$. Note that $A_n \neq B_n C_n$, since the size of a pair $\alpha = (\beta, \gamma)$ is $|\beta| + |\gamma|$. Thus,

$$A_n = \sum_{k=0}^{n} B_k C_{n-k}.$$

(3) Sequence: SEQ

Let $\mathcal{B}$ be a combinatorial class. Then, we construct $\textsc{Seq}(\mathcal{B})$ by taking all sequences of elements of $\mathcal{B}$. Formally,

$$\textsc{Seq}(\mathcal{B}) = \{\epsilon\} + \mathcal{B} + (\mathcal{B} \times \mathcal{B}) + \cdots .$$

(4) Cycle: CYC

Let $\mathcal{B}$ be a combinatorial class. Then,

$$\textsc{Cyc}(\mathcal{B}) = (\textsc{Seq}(\mathcal{B}) \setminus \{\epsilon\})/\mathbf{S}$$

where $\mathbf{S}$ is the equivalence relation defined by

$$(\beta_1, \ldots, \beta_r)\mathbf{S}(\beta'_1, \ldots, \beta'_r)$$

if $(\beta'_1, \ldots, \beta'_r)$ can be obtained from $(\beta_1, \ldots, \beta_r)\mathbf{S}$ by a circular shift.

(5) Multiset: MSET

Let $\mathcal{B}$ be a combinatorial class. Then, the multiset is the set of finite subsets where repetitions of elements are allowed. Formally,

$$\textsc{Mset}(\mathcal{B}) = \textsc{Seq}(\mathcal{B})/\mathbf{R}$$

where $\mathbf{R}$ is the equivalence relation defined by

$$(\beta_1, \ldots, \beta_r)\mathbf{R}(\beta'_1, \ldots, \beta'_r)$$

if $(\beta'_1, \ldots, \beta'_r)$ can be obtained from $(\beta_1, \ldots, \beta_r)\mathbf{S}$ by a permutation.

(6) Powerset: PSET

Let $\mathcal{B}$ be a combinatorial class. We define $\textsc{Pset}(\mathcal{B})$ as the subset of $\textsc{Mset}(\mathcal{B})$ with no repetitions.

As we will see in later sections, we can use these constructions to compute generating functions for classes of objects.

Proposition 1.6. *These objects correspond to the following generating function constructions:*

$$\textit{Sum: } \mathcal{A} = \mathcal{B} + \mathcal{C} \implies A(z) = B(z) + C(z)$$
$$\textit{Cartesian Product: } \mathcal{A} = \mathcal{B} \times \mathcal{C} \implies A(z) = B(z)C(z)$$
$$\textit{Sequence: } \mathcal{A} = \textsc{Seq}(\mathcal{B}) \implies A(z) = \frac{1}{1 - B(z)}$$
$$\textit{Cycle: } \mathcal{A} = \textsc{Cyc}(\mathcal{B}) \implies A(z) = \sum_{k=1}^{\infty} \frac{\varphi(k)}{k} \log\left(\frac{1}{1 - B(z^k)}\right)$$
$$\textit{Multiset: } \mathcal{A} = \textsc{Mset}(\mathcal{B}) \implies A(z) = \prod_{n \geq 1} (1 - z^n)^{-B_n} = \exp\left(\sum_{k=1}^{\infty} \frac{1}{k} B(z^k)\right)$$
$$\textit{Power set: } \mathcal{A} = \textsc{Pset}(\mathcal{B}) \implies A(z) = \prod_{n \geq 1} (1 + z^n)^{B_n} = \exp\left(\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} B(z^k)\right)$$

Proof. The sum and cartesian product identities follow from Definition 1.5.

The OGF for the sequence can be derived from the sum and product identities. We have

$$\textsc{Seq}(\mathcal{B}) = \{\epsilon\} + \mathcal{B} + (\mathcal{B} \times \mathcal{B}) + \cdots$$

which corresponds to the generating function

$$1 + B(z) + B(z)^2 + \cdots = \frac{1}{1 - B(z)}$$

as desired.

The rest of the proofs are similar, so we will not go through them; we refer the reader to [FS09, Theorem I.1]. □

2. Computable Bounds

In this section, we introduce the Inversion Lemma and the Computability of Growth Theorem, which tell us about the radius of convergence of an OGF.

Theorem 2.1 (Inversion Lemma)**.** *Suppose we have a function f that is analytic on a space Ω and we have a $z_0 \in \Omega$. Let $f'(z_0) \neq 0$. Then, there exists a region $\Omega_1 \in \Omega$ with $z_0 \in \Omega_1$ and a $C > 0$ such that $|f(z) - f'(z)| > C|z - z'|$ for all $z, z' \in \Omega_1$.*

Corollary 2.2. *f maps Ω_1 and $f(\Omega_1)$ bijectively.*

Theorem 2.3 (Computability of Growth)**.** *Suppose we have an unlabelled class that admits an iterative specification in terms of $(\textsc{Pset}, \textsc{Seq}, \textsc{Cyc}, \textsc{Mset}; +, \times)$ beginning with (1,Z). Then the radius of convergence of the OGF of $\mathcal{C}$ is either $+\infty$ or a positive computable number.*

Before we prove this, we will need some more background. In general, we know quite easily how to check that a power series that converges is analytic within the disc of convergence: the definitions can help us check this. Another interesting property is that the series must have at least one singularity on the boundary of the disc, while having none on the inside. This is characterized by the theorem below.

Theorem 2.4. *Suppose we have a function $f(z)$ that is analytic at the origin. If $f(z)$ has an expansion at the origin with finite radius R, then $f(z)$ necessarily has a singularity on the boundary of the disc of convergence, and $|z| = R$.*

Proof. Let's take the expansion

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

Assume the radius of convergence for f is R. Now it suffices to prove that there exists a singularity on $|z| = R$. Suppose BWOC that for some $\rho > R$, f is analytic in the disc $|z| < \rho$. By Cauchy's coefficient formula, as we integrate along the circle with radius $r = (R + \rho)/2$, the coefficient of $[z^n]f(z)$ is $O(r^{-n})$. However, we know from earlier that the series expansion of f would need to converge in a disc of radius $r > R$, forming a contradiction. □

This theorem is helpful, but we need a broader generalization to prove computability of growth. More specifically, we need to address *any* series. In our case, we need generating functions. This is known as Pringsheim's theorem.

Theorem 2.5 (Pringsheim's Theorem)**.** *Suppose we have a function $f(z)$ that has a series expansion at the origin with nonnegative coefficients and radius of convergence R. Then, $z = R$ is a singularity of $f(z)$.*

The proof of this theorem is out of the scope of this paper, but the idea involves noticing that the series expansion of $f(z)$ to the left of R will have positive coefficients and as a result, converge in a disc that is larger than the disc of convergence, forming a contradiction.

Proof of Theorem 2.3. Suppose for each class $\mathcal{F}$, we have the generating function $F(z)$. Now, define ρ_F as the radius of convergence and τ_F as $F(\rho_F)$. Now, assign the ordered pair $\langle \rho_F, \tau_F \rangle$ to $F(z)$. Let's take a look at the unlabelled case first. If an unlabelled class $\mathcal{G}$ is finite, then its OGF $G(z)$ will be a polynomial. If $\mathcal{G}$ is infinite, then $G(z)$ will diverge at $z = 1$, implying that the radius of convergence, or ρ_G, will be at most 1. A sufficient condition to determine whether or not a class is finite is if one of the unary constructors intervenes in the specification.

Let $\mathcal{F} = \textsc{Seq}(\mathcal{G})$. This means that $G(z)$ needs to be nonconstant and $G(0) = 0$. By the induction hypothesis, we can say that $0 < \rho_G < +\infty$ and $\tau_G = +\infty$. Since G is increasing and continuous along the positive axis, the IVT implies that there must exist a β such that $G(\beta) = 1$ and $0 < \beta < \rho_G$. Define the quasi-inverse of $G(z)$ as $F(z) = (1 - G(z))^{-1}$ for $z \in (0, \beta)$. As $z \to \beta^-$, $F(z) \to +\infty$. So, the smallest singularity of F in the positive axis is β. By Pringsheim's theorem, $\rho_F = \beta$. This also implies that $\tau_F = +\infty$.

□

3. Coefficient Asymptotics

In this section, we discuss methods to find asymptotics for coefficients of OGFs based on their singularities.

Definition 3.1. A sequence $\{a_n\}$ is of *exponential order* K^n, which we denote by $a_n \bowtie K^n$, if $\limsup |a_n|^{\frac{1}{n}} = K$.

Theorem 3.2 (Exponential Growth Formula)**.** *Suppose $f(z)$ is analytic at $z = 0$, and define R as the modulus of a singularity nearest to 0, i.e.*

$$R = \sup\{r \geq 0 : f \text{ analytic in } |z| < r\}.$$

Then, the coefficients $f_0, f_1, \ldots$ satisfy

$$f_n \bowtie \left(\frac{1}{R}\right)^n.$$

If f has nonnegative coefficients, we can take

$$R = \sup\{r \geq 0 : f \text{ analytic in } 0 \leq z < r\}.$$

Proof. Let f be a function that is analytic at the origin such that its series expansion at $z = 0$ has a finite radius of convergence R. To show Theorem 3.2, we want to show that f must have a singularity on the boundary $|z| = R$.

Assume for the sake of contradiction that f does not have a singularity on this boundary, i.e. that f is analytic in the disk $|z| < \rho$ for some $\rho > R$. Using Cauchy's coefficient formula, we can determine that the coefficient $[z^{-n}]f(z)$ is $O(r^{-n})$ where $r = (R + \rho)/2$. However, this would mean that the series expansion of f at $z = 0$ does actually converge in the disk $|z| < r$, where $r > R$. This is a contradiction to R being the radius of convergence, so the proof is complete. □

Theorem 3.3 (Saddle Point Upper Bounds)**.** *Suppose $f(z)$ is analytic in $|z| < R$ for $0 < R \leq \infty$. Define $M(f; r)$ for $r \in (0, R)$ by*

$$M(f; r) = \sup_{|z|=r} |f(z)|.$$

Then, for any $r \in (0, R)$, we have the bounds

$$[z^n]f(z) \leq \frac{M(f; r)}{r^n} \implies [z^n]f(z) \leq \inf_{r\in(0,R)} \frac{M(f; r)}{r^n}$$

where $[z^n]f(z)$ denotes the nth coefficient of $f(z)$. If f has nonnegative coefficients at 0, we have

$$[z^n]f(z) \leq \frac{f(r)}{r^n} \implies [z^n]f(z) \leq \inf_{r\in(0,R)} \frac{f(r)}{r^n}.$$

Proof. We refer the reader to [FS09, Proposition IV.1]. □

4. Unary-Binary Trees

In this section, we introduce and apply singularity analysis to Motzkin numbers and unary–binary trees.

Definition 4.1. The nth **Motzkin number** M_n is the number of paths from $(0, 0)$ to $(n, 0)$ satisfying the following conditions:

(1) The path cannot dip below the y-axis.
(2) The path only moves to the right, so from a point (a, b), it can move to $(a+1, b+1)$, $(a + 1, b)$, or $(a + 1, b - 1)$.

The Motzkin paths for $n = 4$ are shown in Figure 1.

Note that by looking at the y coordinates of each path, we can interpret the nth Motzkin number as the number of sequences of nonnegative integers $a_0, a_1, \ldots, a_n$ of length $n + 1$ starting and ending with 0, and satisfying the condition that $|a_i - a_{i-1}| \leq 1$ for each $1 \leq i \leq n$.

Definition 4.2. We call a vertex in a rooted tree T a **branching point** if it has at least two edges pointing out of it.

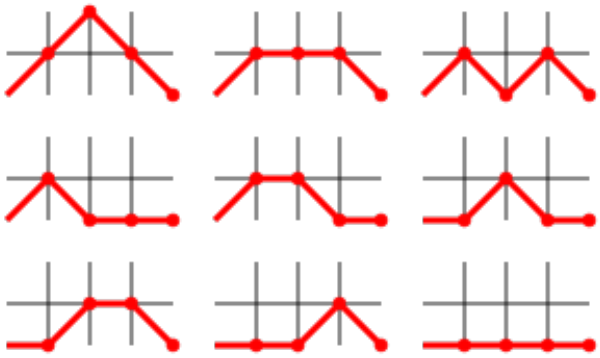

Figure 1. Motzkin paths for $n = 4$.

Definition 4.3. A **unary-binary tree** is a rooted tree with unlabeled vertices such that there are at most two edges out of every vertex, and there are no branching points on odd levels.

Let $\mathscr{E}_n$ denote the set of unary-binary trees on $n+1$ vertices.

Theorem 4.4. *For each positive integer n, $|\mathscr{E}_n| = M_n$.*

Proof. We refer the reader to [KPP96] for the proof. □

Proposition 4.5. *The generating function corresponding to plane unlabelled unary-binary trees is*

$$U(z) = \frac{1 - z - \sqrt{1 - 2z - 3z^2}}{2z} = z + z^2 + 2z^3 + \cdots$$

Proof. Let $\mathcal{M}$ denote the class of unary-binary trees. Notice that

$$\mathcal{M} = \mathcal{Z} \times \textsc{Seq}_{\leq 2}(\mathcal{M}).$$

From this identity, we can extract the generating function: the generating function for $\mathcal{Z}$ is just z, and the function for $\textsc{Seq}_{\leq 2}(\mathcal{M})$ is the finite geometric series $1 + M(z) + M^2(z) = \frac{M^3(z)-1}{M(z)-1}$. Thus, we can rewrite the identity in terms of generating functions and solve for $M(z)$:

$$M(z) = z\frac{M^3(z) - 1}{M(z) - 1}$$

Rearranging to form a quadratic equation,

$$M(z)^2 + \left(1 - \frac{1}{z}\right) M(z) + 1 = 0$$

Using the quadratic formula,

$$M(z) = \frac{\left(-1 + \frac{1}{z}\right) \pm \sqrt{\left(1 - \frac{1}{z}\right)^2 - 4}}{2} = \frac{\left(-1 + \frac{1}{z}\right) \pm \sqrt{-3 - \frac{2}{z} + \frac{1}{z^2}}}{2}$$

$$= \frac{-z + 1 \pm \sqrt{-3z^2 - 2z + 1}}{2z}.$$

To decide which of these solutions is the correct one, we find the Taylor series of both (since the coefficients correspond to the Motzkin numbers). We have:

$$\frac{-z+1+\sqrt{-3z^2-2z+1}}{2z} = \frac{1}{z} - 1 - z - z^2 - 2z^3 - 4z^4 - 9z^5 - 21z^6 + \cdots,$$
$$\frac{-z+1-\sqrt{-3z^2-2z+1}}{2z} = z + z^2 + 2z^3 + 4z^4 + 9z^5 + 21z^6 + \cdots$$

so $U(z) = M(z) = \frac{-z+1-\sqrt{-3z^2-2z+1}}{2z}$ as desired. □

Proposition 4.6. *Applying the exponential growth formula,* $U_n \bowtie 3^n$.

Proof. Note that we can factor the quadratic inside the square root and write $U(z)$ as

$$U(z) = \frac{1 - z - \sqrt{(-3z+1)(z+1)}}{2z}.$$

Notice that $U(z)$ has branch points at $z = \frac{1}{3}$ and $z = -1$. The closest singularity to the origin is $\frac{1}{3}$, so we can take $R = \frac{1}{3}$ in Theorem 3.2 and obtain the bound $U_n \bowtie 3^n$. □

5. Coding Theory

Coding theory, in essence, is the study of error-correcting codes. Any two devices need to somehow communicate with one another in order to work, such as a CD and media player. If the medium by which data is converted is somehow corrupted or destroyed, then some type of error correction needs to be in place, and this is exactly what error-correcting code does.

The most basic building block of coding theory is the *bit.*

Definition 5.1. A *bit* is any string of binary digits.

Now, we turn to some coding theory bounds. We will look into the Singleton bound, which is considered to be the simplest of code bounds.

Theorem 5.2. *Suppose we have a code* C *of length* n *and a minimum distance* d *over an alphabet with size* q*. Then,* $|C| \leq q^{n-d+1}$.

Proof. BWOC suppose $|C| > q^{n-d+1}$. The pigeonhole principle implies that there must exist two codewords c_1 and c_2 where $c_1 \neq c_2$ such that they agree on the first $n-d+1$ locations. However, the distance between c_1 and c_2 will be less than d, forming a contradiction. □

A result of this theorem is we now have a bound on the rate of the function as relative distance that is independent of the alphabet. Now let's take a look at another bound known as the Plotkin bound. We will assume the following lemma in proving it.

Lemma 5.3. *Suppose we have* $v_1, ..., v_m$ *as unit vectors in* $\mathbb{R}^n$.

1. *If* $\langle v_i, v_j \rangle \leq -\epsilon$ *for all* $1 \leq i < j \leq m$*, then* $m \leq 1 + \frac{1}{\epsilon}$.
2. *If* $\langle v_i, v_j \rangle \leq 0$ *for all* $1 \leq i < j \leq m$*, then* $m \leq 2n$.

Now let's establish some preliminary bounds then move on to the Plotkin bound.

Theorem 5.4. *Let's say we have a binary code* C *of block length* n *and distance* d.

1. *If* $d > n/2$*, then* $|C| \leq \frac{2d}{2d-n}$
2. *If* $d \geq n/2$*, then* $|C| \leq 2n$

Theorem 5.5 (Plotkin Bound)**.** *If a binary code C has block length n and distance $d < n/2$, then $|C| \leq d \cdot 2^{n-2d+2}$.*

Proof. Define $l = n - 2d + 1$ and the set $S = \{1, 2, ..., l\}$. For every $a \in \{0,1\}^l$, define C_a to be a subcode of C which consists of all codewords that contain a in the first l positions projected on $S^c = \{1, 2, ..., n\} \setminus S$. Each C_a is a binary code with block length $n - l = 2d - 1$. By Theorem 5.4, we can say that $|C_a| \leq 2d$. Since $|C| = \sum_{a \in \{0,1\}^l} |C_a|$, we assert that $|C| \leq 2d \cdot 2^l = d \cdot 2^{n-2d+2}$. □

References

[FS09] Philippe Flajolet and Robert Sedgewick. *Analytic combinatorics*. cambridge University press, 2009.

[KPP96] Alexander Kuznetsov, Igor Pak, and Alexander Postnikov. Trees associated with the motzkin numbers. *journal of combinatorial theory, Series A*, 76(1):145–147, 1996.