CO 330 with Stephen Melczer*

Eason Li

2025 F

*See Prof's notes at https://enumeration.ca/

Contents

1 Introduction

Lecture 1 - Wednesday, September 03

We enumerate discrete structures that encode different objects (permutations, partitions, trees, networks, DNA sequences, lattice pathes, etc.).

We use tools in Pure Math/ CS to study concrete objects with applications in CS, physics, chemistry, bioinformatics, statistics, etc.

Definition 1.1: Combinatorial Class

A **combinatorial class** is a set $\mathcal{C}$ together with a weight function $\omega : \mathcal{C} \to \mathbb{N}$ such that there are a finite number of elements of any size, i.e.

$$\mathcal{C}_n = \omega^{-1}(n) = \{\sigma \in \mathcal{C} : \omega(\sigma) = n\}$$

is finite for all $n \in \mathbb{N}$.

This is the minimal structure needed for enumeration.

Example 1.1

Let $\mathcal{C} = \{\mathcal{E}, 0, 1, 00, 01, 10, 11, \ldots\}$ be the set of binary strings, where $\mathcal{E}$ denotes the empty string. If $\omega(\sigma) =$ length of σ, then $(\mathcal{C}, \omega)$ is a combinatorial class. If $\omega(\sigma) =$ number of zeros in σ, then $(\mathcal{C}, \omega)$ is *not* a combinatorial class.

Definition 1.2: Counting Sequence

The **counting sequence** of a combinatorial class $(\mathcal{C}, |\bullet|)$ is the sequence

$$(c_n) = c_0, c_1, c_2, \ldots$$

where $c_n = |\mathcal{C}_n|$ is the number of elements of size n in the class.

Example 1.2

If $(\mathcal{C}, |\bullet|)$ is the usual set of binary strings, then $c_n = 2^n$.

1.1 Usual Starting Point

The usual starting point is when we have a description of the class $\mathcal{C}$, and we wish to say something interesting about it. For instance, we could talk about:

- a closed formula, such as $c_n = 2^n$ in the example above;
- asymptotic behaviour, such as $\log(n!) \sim n \log n$;
- an efficient algorithm to compute f_N, the Fibonacci number;
- a recursive formula, for example, $f_{n+1} = f_{n+1} + f_n$.

Our general tools are bijections and generating functions. Bijections use old/ simpler objects to study new/ complicated objects, while generating functions give a data structure to store sequences and help determine their properties.

1.2 Bijections

Let A and B be two sets.

Definition 1.3: Injective

A function $f : A \to B$ is **injective** if $a \neq a'$ implies $f(a) \neq f(a')$.

Definition 1.4: Surjective

A function $f : A \to B$ is **surjective** if for any $b \in B$, there is $a \in A$ with $f(a) = b$.

Definition 1.5: Bijective

A function $f : A \to B$ is **bijective** if it is both injective and surjective.

Proposition 1.1

$f : A \to B$ is a bijection if and only if it has an inverse $g : B \to A$ meaning

$$f(g(b)) = b \qquad \text{and} \qquad g(f(a)) = a$$

for all $b \in B$ and $a \in A$. We write f^{-1} for the inverse.

Example 1.3

Show that $\mathbb{Z}$ and $2\mathbb{Z}$ are in bijection.

Lecture 2 - Friday, September 05

A *bijection of combinatorial classes* $(A, |\bullet|_A)$ and $(B, |\bullet|_B)$ is a bijection $f : A \to B$ that "preserves size" (elements of size n is sent to elements of size n, for all $n \in \mathbb{N}$).

Example 1.4

A permutation of size n is a rearrangement of $1, \dots, n$. A permutation matrix of size n is an $n \times n$ matrix with 0 and 1 entries such that every row and colume has exactly one 1's.

Show that the classes P of permutations and M of permutation matrices are in bijection.

Solution. The value of the i^{th} entry of the permutation is the position where the entry with 1 in the i^{th} row of the permutation matrix is. This has an inverse. □

Question 1.1. How do we find bijections?

We have some different way to find intuition of finding bijections. We could look at small examples to find patterns, or we can also relate to objects/ bijections we have already understood.

Bijections allow us to give *combinatorial proofs* for identites of the form $LHS = RHS$:

1. Find sets A and B with $|A| = LHS$ and $|B| = RHS$;
2. Prove that A and B are in bijection;
3. We conclude that $LHS = RHS$.

Recall that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is the number of ways to pick k elements from $\{1, \dots, n\}$.

Example 1.5

Give a combinatorial proof that $\binom{n}{k} = \binom{n}{n-k}$ for all $n, k \in \mathbb{N}$ with $0 \leq k \leq n$.

Proof. Let A be the set of subsets of $\{1, \dots, n\}$ with k elements and let B be the set of subsets of $\{1, \dots, b\}$ with $n-k$ elements. The bijection is just sending $a \in A$ to $[n] \setminus a \in B$. □

Question 1.2. How do we do combinatorial proofs?

We shall find the right interpretation for both sides.

For instance

Sequence	*Interpretation*
$n!$	permutation
2^n	subsets of $\{1, \dots, n\}$, binary string of length n, integer composition of size $n+1$
A^n	strings on the symbols $\{0, \dots, A-1\}$
$\binom{n}{k}$	subsets of $\{1, \dots, n\}$ of size k
$\binom{n+t-1}{t-1}$	stars and bars
$a \times b$	Cartesian product/ pairs of sets with size a and b
$a + b$	disjoint union of sets with size a and b
$\binom{a+b}{a}$	lattice paths from $(0,0)$ to (a,b) using steps $(0,1)$ and $(1,0)$

Lecture 3 - Monday, September 08

Yapping about sage math the whole lecture today.

Lecture 4 - Wednesday, September 10

Let $\mathcal{C}$ be a combinatorial class with counting sequence

$$(c_n) = c_0, c_1, \ldots$$

How can we represent c_n? A "nice" closed form may not exist. We need a data structure for sequence.

Definition 1.6: Generating Function

The **generating function** of a class $\mathcal{C}$ is a series

$$C(x) = \sum_{n \geq 0} c_n x^n = \sum_{\sigma \in \mathcal{C}} x^{|\sigma|}$$

This is also called the GF of c_n.

Question 1.3. What kind of series is this?

Example 1.6

If $c_n = 2^n$, then $C(x) = \sum_{n \geq 0} 2^n x^n$ is a convergent series when $|x| < \frac{1}{2}$.

Example 1.7

If $c_n = n!$, then $C(x) = \sum_{n \geq 0} (n!) x^n$ is a convergent series when $x = 0$.

We don't want to worry about convergence. Also, we might want series where coefficients are not just real/ complex numbers (i.e., a series in x where coefficients are polynomials in y).
To get around this, we define **formal power series**.

Definition 1.7: Ring

A **ring** if a set R together with two operations $+$ and $\times$ (from $R \times R$ to R) and two special elemetns 0 and 1 such that

- $(a+b)+c = a+(b+c)$;
- $a+b = b+a$;
- $a+0 = a$;
- $\forall a \in R, \exists (-a) \in R, a+(-a) = 0$;
- $(a \times b) \times c = a \times (b \times c)$;
- $1 \times a = a \times 1 = a$
- $a \times (b+c) = (a \times b) + (a \times c)$;
- $(b+c) \times a = (b \times a) + (c \times a)$.

Example 1.8

$\mathbb{C}^{n\times n}$ form a ring. (notice that this ring is not commutative).

Example 1.9

$\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ are all commutative ring.

Comment 1.1

If $a \times b = 0$ implies $a = 0 = b$, then R has no *zero divisors*.

Definition 1.8: Integral Domain

A commutative ring with no zero divisors is called an **integral domain**.

Definition 1.9: Field

A **field** is an integral domain where for any $a \in R$ with $a \neq 0$, there is some $a^{-1} \in R$ with $a \cdot a^{-1} = 1$.

1.3 Ring of Formal Power Series

Definition 1.10: Ring of Formal Power Series

Let R be an integral domain, the **ring of formal power series** with coefficients in R is the set $R[[x]]$ of formal expressions

$$\sum_{n=0}^{\infty} c_n x^n = c_0 + c_1 x + c_2 x^2 + \cdots \qquad \text{with each } c_j \in R$$

We define *addition* by

$$\sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n = \sum_{n\geq 0} (a_n + b_n) x^n$$

and we define *multiplication* by

$$\left(\sum_{n\geq 0} a_n x^n\right)\left(\sum_{n\geq 0} b_n x^n\right) = \sum_{n\geq 0}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n$$

Lemma 1.1

$R[[x]]$ is an integral domain.

Note 1.1

This is not a field as, for example, x has no inverse.

Lemma 1.2

Let $A(x) = \sum_{n\geq 0} a_n x^n \in R[[x]]$, there exists $B(x) \in R[[x]]$ with $A(x)B(x) = 1$ if and only if a_0 is invertible in R. Such a $B(x)$ is the multiplicative inverse of $A(x)$ and often written as $A(x)^{-1}$ or $\frac{1}{A(x)}$.

Comment 1.2

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

Lecture 5 - Friday, September 12

Example 1.10

Prove that $\dfrac{1}{1-2x} = \sum_{n\geq 0} 2^n x^n$ as formal power series $\mathbb{Q}[[x]]$.

Proof. We want to show that $1-2x$ is the multiplicative inverse of $\sum_{n\geq 0} 2^n x^n$. by definition,

$$\begin{aligned}(1-2x)\sum_{n\geq 0} 2^n x^n &= \sum_{n\geq 0} 2^n x^n - (2x)\sum_{n\geq 0} 2^n x^n \\ &= 1 + \sum_{n\geq 1} 2^n x^n - \sum_{n\geq 0} 2^{n+1}x^{n+1} = 1\end{aligned}$$

as desired. $\square$

1.3.1 Ring of Laurent Series

Definition 1.11: Ring of Laurent Series

If R is an integral domain, then the **ring of Laurent series** with coefficients in R is the set of formal expressions

$$R((x)) = \left\{\sum_{n=\ell}^{\infty} c_n x^n : c_j \in R \quad \forall j \text{ and } \ell \in \mathbb{Z}\right\}$$

where $\sum_{n=\geq \ell} a_n x^n + \sum_{n\geq m} b_n x^n = \sum_{n\geq \min(\ell,m)} (a_n+b_n)x^n$, and $\left(\sum_{n\geq \ell} a_n x^n\right)\left(\sum_{n\geq m} b_n x^n\right) = \sum_{n\geq \ell+m}\left(\sum_{k=\ell}^{n-m} a_n b_{n-k}\right)x^n$.

Comment 1.3

Laurent series only have a finite number of negative expressions.

Example 1.11

We have $x^{-5} + x^{-2} + x + \cdots \in \mathbb{Q}((x))$, but $\sum_{n \in \mathbb{Z}} x^n$ is not.

Lemma 1.3

If R is a field, then $R((x))$ is a field.

Getting back to our original motivation, we use formal power series as generating functions that form data structure for sequences. Because GF are algebraic objects, we can specify them with algebraic equations.

1.3.2 Analytic (Generalized) Binomial Theorem

Theorem 1.1: Analytic Binomial Theorem

Let K be a field contained in $\mathbb{C}$ (such as $\mathbb{Q}$). If $\alpha = r/s$ for $r, s \in \mathbb{Z}$ and $s > 0$, then the equation $y^s = (1+z)^r$ has a solution

$$y(z) = \sum_{k \geq 0} \binom{\alpha}{k} z^k \in K[[z]]$$

where we extend the definition of binomial coefficients by

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-k+1)}{k!} \quad \text{where } \alpha \in \mathbb{Q}, k \in \mathbb{N}$$

The equation $y^s = (1+z)^r$ has at most s distinct solutions, obtained by multiplying $y(z)$ by any of the numbers in $\{t \in K : t^s = 1\}$.

Comment 1.4

We also write $(1+z)^\alpha$ for the series $y(z)$.

Exercise 1.1

Find the coefficient of z^n in the expansion of $(1+z)^{-1/2}$.

Solution. The Analytic Binomial Theorem implies the coefficient of interest is

$$\begin{aligned}\binom{-1/2}{n} &= \frac{(-1/2)(-1/2-1)\cdots(-1/2-n+1)}{n!} \\ &= (-1)^n 2^{-n} \frac{(1)(3)(5)\cdots(2n-1)}{n!} \cdot \frac{2^n \cdot n!}{2^n \cdot n!} \\ &= (-1)^n 4^{-n} \frac{2n!}{n!n!} = (-1)^n 4^{-n} \binom{2n}{n}\end{aligned}$$

as desired. □

Exercise 1.2

Show that $(1-4x)^{-1/2} = \sum_{n\geq 0} \binom{2n}{n} x^n$.

Lecture 6 - Monday, September 15

Comment 1.5

The notation $[x^n]F(x)$ was invented in Waterloo.

1.3.3 Generating Function Examples

Remember that the generating function for a combinatorial class $\mathcal{C}$ is the series

$$C(x) = \sum_{n\geq 0} c_n x^n = \sum_{\sigma\in\mathcal{C}} x^{|\sigma|}$$

where c_n is the number of objects of size n. By default, we consider them to be elements of $\mathbb{Q}[[x]]$.

Example 1.12

How many ways are there to make change for n cents using 1 cent, 5 cents, 10 cents, and 25 cents coins?

Solution. Let M to be the combinatorial class with set $M = \mathbb{N}^4$ with size function $|(a,b,c,d)| = a+5b+10c+25d$. The generating function for this class is

$$\begin{aligned} M(x) = \sum_{(a,b,c,d)\in\mathbb{N}^4} x^{|(a,b,c,d)|} = \sum_{a,b,c,d\geq 0} x^{a+5b+10c+25d} &= \left(\sum_{a\geq 0} x^a\right)\left(\sum_{b\geq 0} x^{5b}\right)\left(\sum_{c\geq 0} x^{10c}\right)\left(\sum_{d\geq 0} x^{25d}\right) \\ &= \frac{1}{1-x}\cdot\frac{1}{1-x^5}\cdot\frac{1}{1-x^{10}}\cdot\frac{1}{1-x^{25}} \end{aligned}$$

For instance,

$$M(x) = 1 + \cdots + 242x^{100} + \cdots$$

which means that there are 242 ways to make change for 100 cents. In general, we have the following methods to find the number $[x^n]M(x)$:

1. compute directly $[x^n]M(x)$ for any fixed n;
2. get a linear recurrence for $m_n = [x^n]M(x)$;
3. get a "closed formula";
4. get asymptotics, i.e., $m_n \sim n^3/7500$.

□

Example 1.13

The generating function for the number of ways to roll two dice. We have

$$D = \{(a, b) \in \{0, \dots, 6\}^2\} \quad \text{and} \quad |(a, b)| = a + b$$

We observe that the GF in fact has two different factorizations:

$$\begin{aligned} D(x) &= (x + x^2 + x^3 + x^4 + x^5 + x^6)^2 \\ &= (x + 2x^3 + 2x^4 + x^4)(x + x^3 + x^4 + x^5 + x^6 + x^8) \end{aligned}$$

The second GF represents the *Sicherman dice* with faces $(1, 2, 2, 3, 3, 4)$ and $(1, 3, 4, 5, 6, 8)$.

Example 1.14

Consider a sequence of formal power series $F_0(x), F_1(x), F_2(x), \dots$, in $R[[x]]$. We say that the sequence $(F_k(x))_n$ **formally converges** if for every $n \in \mathbb{N}$, there exists $L \in \mathbb{N}$ and $c_n \in R$ such that

$$[x^n]F_k(x) = c_n \quad \text{whenever } k \geq L$$

i.e., eventually, all coefficients stabalize. When this holds, we write

$$\lim_{k \to \infty} F_k(x) = \sum_{n \geq 0} c_n x^n \in R[[x]]$$

For instance, the sequence $(F_k(x) := 2^k x^k)_k$ converges to 0, and the sequence $(F_k(x) := 1 + x + x^2 + \cdots + x^k)$ converges to the series $\sum_{n \geq 0} x^n$. Moreover, suppose we have

$$F_0(x) = 1, \qquad F_k(x) = \frac{1}{1 - x/k}$$

then the sequence $(F_k(x))_k$ does not converge because, for example, $[x^1]F_k(x) = 1/k$ which does not stabalize.

This allows us to talk about the convergence of infinite series of power series. We say that $\sum_{k \geq 0} F_k(x)$ exists as a formal power series if $S_n = \sum_{k \geq 0}^{n} F_k(x)$ formally converges, and we write

$$\lim_{n \to \infty} S_n = \sum_{k \geq 0} F_k(x)$$

Theorem 1.2

Let $A, B \in R[[x]]$ be two formal power series. If $A(x)$ is a polynomial, then $A(B(x))$ always exists. If $A(x)$ has a infinite number of non-zero coefficients, then $A(B(x))$ exists if and only if $[x^0]B(x) = 0$.

Proof. If $A(z)$ has only a finite number of non-zero coefficients then

$$A(B(z)) = \sum_{n\geq 0} a_n B(z)^n$$

is a finite sum of formal series on the right-hand side, which is always formally summable. Suppose now that A has an infinite number of non-zero coefficients. If $B(0) = 0$ then

$$B(z)^n = (b_1 z + \cdots)^n = b_1^n z^n + \cdots$$

so that $[z^\ell]B(z)^k = 0$ if $k > \ell$. In particular,

$$[z^\ell] \sum_{k=0}^{N} a_k B(z)^k = [z^\ell] \sum_{k=0}^{\ell} a_k B(z)^k$$

does not depend on N whenever $N \geq \ell$. Thus, the coefficients of the partial sums defining $A(B(z))$ stabilize and the composition exists. Conversely, if $B(0) = b_0 \neq 0$ then

$$[z^0] \sum_{k=0}^{N} a_k B(z)^k = a_0 + a_1 b_0 + \cdots + a_N b_0^{N-1}$$

Because $b_0 \neq 0$ and an infinite number of the a_i are non-zero, this partial sequence will not stabilize as N grows, meaning the composition is not defined. □

Lecture 7 - Wednesday, September 17

1.3.4 Formal Derivative, Formal Integral, Formal Exp, Formal Log

Let $F(x) = \sum_{n\geq 0} f_n x^n$ be an element of $R[[x]]$.

Definition 1.12: Formal Derivative

The **formal derivative** of $F(x)$ is

$$F'(x) = \sum_{n\geq 1} n f_n x^{n-1} = \sum_{n\geq 0} (n+1) f_{n+1} x^n$$

Definition 1.13: Formal Integral

If the positive integers has multiplicative inverse in R, then the **formal integral** of F is defined as

$$\int F(x) = \sum_{n\geq 0} \frac{f_n}{n+1} x^{n+1}$$

If the positive integers has multiplicative inverse in R, we define

$$\exp(x) = \sum_{n\geq 0} \frac{x^{n+1}}{n!}$$

and the formal logarithm

$$\log(1+x) = \int \frac{1}{1+x} = \sum_{n\geq 1} \frac{(-1)^n}{n} x^n$$

We then define $(1+x)^\alpha = \exp(\alpha \log(1+x))$. The Generalized Binomial Theorem (see section 1.3.2) further generalizes to

$$(1+x)^\alpha = \sum_{n\geq 0} \binom{\alpha}{n} x^n$$

1.3.5 Rule for Extracting Coefficients

We have the following rules for extracting coefficients:

1. `Addition`: $[x^n](A(x)+B(x)) = [x^n]A(x) + [x^n]B(x)$;
2. `Multiplication`: $[x^n](A(x)B(x)) = \sum_{k=0}^{n}[x^k]A(x)[x^{n-k}]B(x)$, this further yields us the following rule: $[x^n]c \cdot A(x) = c[x^n]A(x)$ for some constant c;
3. `Coefficients scaling`: $[x^n]A(px) = p^n[x^n]A(x)$ for some p a constant;
4. `Monomial Multiplication`: $[x^n]x^kA(x) = [x^{n-k}]A(x)$;
5. `Binomial Theorem`;
6. `Negative Binomial Theorem`: if t is a positive integer, then $\binom{-t}{n} = (-1)^n\binom{n+t-1}{t-1}$;

1.4 Combinatorial Construction

Lecture 8 - Friday, September 19

Recall a combinatorial class $(\mathcal{C}, \omega)$ has a generating function $C(x)$. We want to build a class out of other classes and relate their generating functions.
`Base Case`:

- Atomic Class: $\mathbb{Z}$ = class with one object of size 1;
- Neutral Class: $\mathcal{E}$ = class with one object of size 0.

`Construction`:

- **Sum**: Let (A, ω_A) and (B, ω_B) be combinatorial classes, then the sum $C = A + B$ is the new combinatorial class whose set of objects is the *disjoint union* of the objects in A and the objects in B. The size of $\sigma \in C$ is defined as

$$|\sigma|_C = \begin{cases} |\sigma|_A & \text{if } \sigma \in A \\ |\sigma|_B & \text{if } \sigma \in B \end{cases}$$

Lemma 1.4

If $C = A + B$, then $C(x) = A(x) + B(x)$.

Proof. Because the union is disjoint,

$$c_n = a_n + b_n \qquad \text{for all } n \in \mathbb{N}$$

as desired. □

- **Product**: Let (A, ω_A) and (B, ω_B) be combinatorial classes, then the product $C = A \times B$ is the new combinatorial class whose elements are all pairs $\{(a, b) : a \in A, b \in B\}$ with size defined as

$$|(a, b)|_C = |a|_A + |b|_B$$

Lemma 1.5

If $C = A \times B$, then $C(x) = A(x)B(x)$.

Proof. We have

$$C(x) = \sum_{\sigma \in C} x^{|\sigma|_C} = \sum_{a \in A, b \in B} x^{|a|_A + |b|_B} = \left(\sum_{a \in A} x^{|a|_A}\right)\left(\sum_{b \in B} x^{|b|_B}\right) = A(x)B(x)$$

as desired. □

- **Product**: For any class (A, ω_A), we define

$$A^k = \underbrace{A \times A \times \cdots \times A}_{k \text{ terms}}$$

and we define $A^0 = \mathcal{E}$.

- **Sequence**: If (A, ω_A) is a combinatorial class with NO objects of size zero, we define the class

$$SEQ(A) = \mathcal{E} + A + A^2 + A^3 + \cdots$$

i.e., $SEQ(A)$ contains all finite length tuples of elements in A. This is a combinatorial class because A has no object of size zero, so A^k has objects of size at least k.

Lemma 1.6: String Lemma

If $C = SEQ(A)$ then $C(x) = \dfrac{1}{1 - A(x)}$.

Note 1.2

We know that $[x^0]A(x) =$ the number of objects of size 0 in A, which is zero, so $[x^0](1 - A(x)) = 1$, which means that the fraction above exists.

Proof. As formal power series,

$$C(x) = 1 + A(x) + A(x)^2 z + \cdots = \sum_{k\geq 0} A(x)^k = \frac{1}{1 - A(x)}$$

as desired. □

1.4.1 Combinatorial Construction Examples

Example 1.15: Binary strings

Let B = class of binary strings where size is defined by the length. A binary string is a finite sequence of 0's and 1's, where each 0 and 1 adds one to the size of a string, so we have

$$B = SEQ(Z_0, Z_1)$$

and the generating function is $B(x) = \dfrac{1}{1-2x}$, so there are $[x^n]B(x) = 2^n$ binary string of length n.

Example 1.16: Integer compositions

The class C of integer compositions contains all finite length tuples $(a_1, \ldots, a_\ell)$ of positive integers where $|(a_1, \ldots, a_\ell)| = a_1 + \cdots + a_\ell$. Let P be the class of positive integers, then $C = SEQ(P)$. We know that $P = \{1, 2, 3, \ldots\}$, and

$$P(x) = x + x^2 + x^3 + \cdots$$

Thus

$$C(x) = \frac{1}{1 - P(x)} = \frac{1}{1-2x} - \frac{x}{1-2x}$$

If $n \geq 1$, there are $[x^n]C(x) = 2^n - 2^{n-1}$ compositions of size n and there are $[x^0]C(x) = 1$ composition of size 0.

You can modify these constructions. For instance, we can define

$$SEQ_{even}(A) = \mathcal{E} + A^2 + A^4 + \cdots = \frac{1}{1 - A(x)^2}$$

$$SEQ_{\geq k}(A) = A^k + A^{k+1} + A^{k+2} + \cdots = \frac{A(x)^k}{1 - A(x)^2}$$

$$\vdots$$

Example 1.17: Rooted planar binary tree

A (rooted planar) binary tree is either empty, or single vertex followed by a left binary tree and a right binary tree (size is the number of edges). Therefore, we know that

$$B = \underbrace{\mathcal{E}}_{\text{empty tree}} + \underbrace{Z \times B \times B}_{\text{the rest binary trees}}$$

This yields us that

$$B(x) = 1 + xB(x)^2$$

Solving for $B(x)$ we obtain that

$$B(x) = \frac{1-\sqrt{1-4x}}{2x} \qquad \text{or} \qquad B(x) = \frac{1+\sqrt{1-4x}}{2x}$$

However, one of them is combinatorially irrelevant to us, so how can we determine which one of them is the one we care about? We can simply expand it out and find out that the one on the left is the on we wanted. So there are $[x^n]B(x) = \frac{1}{n+1}\binom{2n}{n}$ binary trees of size n.

Example 1.18

Let T be the class of all rooted planar trees such that it is a root vertex followed by a sequence of rooted planar tree. Hence we have

$$T = Z \times SEQ(T)$$

Hence we have

$$T(x) = \frac{x}{1-T(x)} \quad \Rightarrow \quad T(x) = \frac{1-\sqrt{1-4x}}{2}$$

so the number of planar trees is $[x^n]T(x) = \frac{1}{n}\binom{2n-2}{n-1}$.

Example 1.19

A Dyck path of size n is a sequence of "up steps" ($\nearrow$) and "down steps" ($\searrow$) that starts at the origin and ends at some point $(2n, 0)$ and never goes below the x-axis.

Note 1.3

The size of a dyck path is = the number of up steps.

By considering the first time we return to the x-axis, we have a unique decomposition

$$D = \mathcal{E} + Z_{\nearrow} \times D\mathcal{E}_{\searrow} \times D \quad \Rightarrow \quad D(x) = 1 + xD(x)^2$$

The reason we have $\mathcal{E}_{\searrow}$ is because only "up steps" contributes to the size of the path.

Example 1.20

Find the number of compositions of size n that have exactly k "parts" (i.e., are k-tuples). Let P be the positive integers, and A is the specified class of compositions, then $A = P^k$:

$$A = P^k = \frac{x^k}{(1-x)^k}$$

Thus there are $[x^n]A(x)$ such compositions. If $k > n$, this is 0. Otherwise, there are

$$[x^n]\frac{x^k}{(1-x)^k} = (-1)^{n-k}\binom{-k}{n-k} = \binom{n-1}{n-k}$$

Example 1.21

How many compositions have an even number of parts? How many have an odd number of parts? Let E be the class of compositions with even number of parts, and let P be the class of positive integers. We have

$$E(x) = SEQ_{even}(P)(x) = \frac{1}{1-P(x)^2} = \frac{1}{1-\left(\frac{x}{1-x}\right)^2} = \frac{1-2x+x^2}{1-2x} = 1 + \frac{x^2}{1-2x}$$

Hence

$$[x^n]E(x) = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{if } n = 1 \\ 2^{n-2} & \text{if } n \geq 2 \end{cases}$$

From here we can directly conclude that there are $2^{n-1} - 2^{n-2} = 2^{n-2}$ compositions of size $n \geq 2$ with an odd number of parts.

Lecture 10 - Wednesday, September 24

We do not always want to solve algebraic equations to get coefficients.

1.4.2 LIFT

Theorem 1.3: Lagrange Implicit Function Theorem/ LIFT

let D be an integral domain contains $\mathbb{Q}$ (or, for example, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[y]$). If $G(u)$ is a formal power series in $D[[u]]$ such that $[u^0]G(u)$ is invertible, then there exists a unique element $R \in D[[z]]$ with $[z^0]R(z) = 0$ such that

$$z = \frac{R(z)}{G(R(z))}$$

Furthermore, if $F(u)$ is any formal power series in $D[[u]]$, then

$$[z^n]F(R(z)) = \frac{1}{n}[u^{n-1}]F'(u)G(u)^n$$

for all $n \geq 1$.

Note 1.4

The most important case is when $F(u) = u$, and we have

$$[z^n]R(z) = \frac{1}{n}[u^{n-1}]G(u)^n$$

Example 1.22

Recall that a planar rooted tree is a vertex followed by a sequence of nonempty planar rooted trees. If T is the class of rooted planar tree, then

$$T = Z \times SEQ(T)$$

$$T(z) = \frac{z}{1 - T(z)} \implies z = \frac{T(z)}{G(T(z))}$$

where $G(u) = (1-u)^{-1}$. Hence

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

Example 1.23

Fix a positive integer r. Find the number of rooted planar trees where every vertex has either 0 or exactly r children. If T is the combinatorial class of such trees, then

$$T = Z \times (\mathcal{E} + T^r)$$

$$T(z) = z(1 + T(z)^r) \implies z = \frac{T(z)}{G(T(z))}$$

where $G(u) = 1 + u^r$. Hence

$$[z^n]T(z) = \frac{1}{n}[u^{n-1}]G(u)^n = \frac{1}{n}[u^{n-1}](1+u^r)^n = \frac{1}{n} = \begin{cases} 0 & r \nmid n-1 \\ \frac{1}{n}\binom{n}{(n-1)/r} & r \mid n-1 \end{cases}$$

Example 1.24

For 5-ary tree, we had

$$T(x) = 1 + xT(x)^5$$

The problem with this is that there is an object of size 0. To connect this, let $S(x) = T(x) - 1$, so

$$S(x) = x(S(x)+1)^5 \implies x = \frac{S(x)}{G(S(x))}$$

where $G(u) = (1+u)^5$. Hence if $n \geq 1$, LIFT implies that

$$[x^n]T(x) = [x^n]S(x) = \frac{1}{n}[u^{n-1}](1+u)^{5n} = \frac{1}{n}\binom{5n}{n-1}$$

Example 1.25

The Lambda W-function $W(z)$ is defined by

$$W(z)e^{W(z)} = z \implies z = \frac{W(z)}{G(W(z))}$$

where $G(u) = e^{-u}$. Hence for $n \geq 1$,

$$[z^n]W(z) = \frac{1}{n}[u^{n-1}]e^{-nu} = \frac{1}{n} \cdot \frac{(-n)^{n-1}}{(n-1)!}$$

which yields us that

$$W(z) = \sum_{n \geq 1} \frac{(-n)^{n-1}}{n!} z^n$$

Proof of LIFT, Theorem 1.3. You can prove LIFT using tools in complex analysis (contour integrals, residues, etc.) The proofs are short and nice, but they only apply in certain circumstances. There are several formal proofs, and there are also combinatorial proofs.

One formal proof uses formal analogs of the tools from complex analysis. See more at the following website: https://enumeration.ca/toolbox/lift/. □

1.5 Exercises

Some exercises can be found on https://enumeration.ca/. Shout out to Stephen Melczer.

1.5.1 Combinatorial Proof Exercises

Exercise 1.3

Give bijective proofs of the following identity. For all $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} \binom{n}{k} k = n2^{n-1}$$

Proof. We observe that LHS =

$$\sum_{k=0}^{n} \binom{n}{k} k = \sum_{k=1}^{n} \binom{n}{k} \binom{k}{1}$$

and RHS =

$$n2^{n-1} = \sum_{k=0}^{n-1} \binom{n}{1} \binom{n-1}{k} = \sum_{k=1}^{n} \binom{n}{1} \binom{n-1}{k-1}$$

i.e., choosing a group of size k and a leader from the group is the same as choosing the leader first and then fill the group with $k-1$ more people. □

Exercise 1.4

Give a combinatorial proof for the following identity:

$$\binom{n}{k}^2 = \sum_{i=0}^{k} \binom{n}{i} \binom{n-i}{k-i} \binom{n-k}{k-i}, \qquad 0 \leq k \leq n$$

Proof. The LHS counts the number of ways of choosing two groups of people out of n, denoted as group A and group B. For the RHS, $\binom{n}{i}$ is the number of ways choosing people in $A \cap B$, $\binom{n-i}{k-i}$ is the number of ways choosing people in $A - B$, and $\binom{n-k}{k-i}$ is the number of ways choosing people in $B - A$. □

Exercise 1.5

Give a combinatorial proof for the following identity:

$$\binom{2a+b+1}{b} = \sum_{i=0}^{b} \binom{a+i}{i} \binom{a+b-i}{i}$$

Proof. The extra one splits the $2a$ into two parts of size a, and then we are having b bars trying to partition them into $b+1$ parts. The one is essential because it distinguishes the different ways of partitionining two subparts as counted on the RHS. □

Exercise 1.6

Prove that

$$\sum_{m=k}^{n-1} \binom{m}{k} = \binom{n}{k+1} \quad \text{for all } 0 \leq k < n$$

Proof. RHS is simply counting the number of ways of picking $k+1$ things to form a subset of $[n]$. For the LHS, it describes another way of counting: we can first select the $(k+1)$-th largest element. Let's say this element is at position $m+1$, where m ranges from k (at least k elements before it to form a group of $k+1$) to $n-1$ (this is the maximum index it can take while still leaving room to have chosen k elements before it). Once we fix this $(k+1)$-th largest element at position $m+1$, we need to choose k elements from the first m elements. This can be done in $\binom{m}{k}$ ways. □

1.5.2 Combanotorial Construction Exercises

Exercise 1.7

Find the number of binary strings of length n such that every block of 0s is followed by an even number of 1s.

Proof. The regular expression recognizing all such binary strings is given by

$$\texttt{1}^*\texttt{(00}^*\texttt{(11)(11)}^*\texttt{)}^*\texttt{0}^*$$

and hence if B is the class of all such binary strings, then

$$B = SEQ(Z_1) \cdot SEQ(Z_0 \cdot SEQ(Z_0) \cdot Z_1^2 \cdot SEQ(Z_1^2)) \cdot SEQ(Z_0)$$

as desired. □

Exercise 1.8

Prove that the generating function $B_r(z)$ for the class of binary strings with blocks of size at most r is

$$B_r(x) = \frac{1 - z^{r+1}}{1 - 2z + z^{r+1}}$$

Proof. The regular expression recognizing all such binary strings is given by

$$(\varepsilon \cup 1 \cup \cdots \cup 1^r)((0 \cup \cdots \cup 0^r)(1 \cup \cdots \cup 1^r))^*(\varepsilon \cup 0 \cup \cdots \cup 0^r)$$

and hence if B is the class of all such binary strings, then

$$B(x) = \left(\frac{z^{r+1} - 1}{z - 1}\right)\left(\frac{z^{r+1} - z}{z - 1}\right)$$

as desired. □

2 Class with Parameters

Lecture 11 - Friday, September 26

Why did we take formal power series in $D[[x]]$ with D an integral domain? We can make D a ring of formal power series. For instance,

$$\mathbb{Q}[[x]][[y]] = D[[y]] \quad \text{where } D = \mathbb{Q}[[x]]$$

where $\mathbb{Q}[[x]][[y]] = \{\sum_{n\geq 0} a_n(x)y^n : a_n(x) \in \mathbb{Q}[[x]]\}$. Similarly, we have $\mathbb{Q}[[y]][[x]] = \{\sum_{n\geq 0} b_n(y)x^n : b_n(y) \in \mathbb{Q}[[y]]\}$. We can say $\mathbb{Q}[[x]][[y]]$ "is the same" as $\mathbb{Q}[[y]][[x]]$. In fact, its the same as

$$\mathbb{Q}[[x, y]] = \left\{ \sum_{i,j\geq 0} a_{ij} x^i y^j \right\}$$

This holds if $\mathbb{Q}$ is replaced by any integral domain, thus we can define $\mathbb{Q}[[z_1, \ldots, z_d]]$ recursively.

Note 2.1

For Laurent Series, the order of the variables does matter. For instance,

$$\frac{1}{x+y} = \frac{1}{y} \cdot \frac{1}{1+x/y} = \frac{1}{y} \sum_{n\geq 0} \left(-\frac{x}{y}\right)^n = \sum_{n\geq 0} (-1)^n y^{-n-1} x^n \in \mathbb{Q}((y))((x))$$

but is not in $\mathbb{Q}((x))((y))$.

Comment 2.1

Moral: Be very careful with the order of variables for Laurent Series.

Here are some notation conventions in this course:

- We write $\underline{z} = (z_1, \ldots, z_d)$;
- We write $\underline{z}^{\underline{i}} = z_1^{i_1} \cdots z_d^{i_d}$;

Therefore, we can write the following in a more compact form

$$\sum_{i_1,\ldots,i_d\geq 0} a_{i1}, \ldots, a_{id} z_1^{i_1} \cdots z_d^{i_d} = \sum_{\underline{i}\in\mathbb{N}^d} a_{\underline{i}} \underline{z}^{\underline{i}}$$

Comment 2.2

An important subring of $D((z))$ is the *ring of Laurent polynomials*: $\mathbb{Q}[\underline{z}, \underline{z}^{-1}]$, all Laurent series with a finite number of non-zero coefficients. The nice thing about it is that the order of the variables does not matter.

Definition 2.1: Parameter Function

Let $(C, |\bullet|)$ be a combinatorial class. A **parameter function** is any function $p : C \to \mathbb{Z}^d$.

Definition 2.2: Multivariate Generating Function

The multivariate generating function of the class with parameters $(C, |\bullet|, p)$ is the formal power series

$$C(\underline{u}, z) = \sum_{\sigma \in C} \underline{u}^{p(\sigma)} \cdot z^{|\sigma|} = \sum_{n \geq 0} \left(\sum_{i \in \mathbb{Z}^d} f_{\underline{i},n} \underline{u}^{\underline{i}} \right) z^n \in \mathbb{Q}[\underline{u}, \overline{u}][[z]]$$

where $f_{\underline{i},n}$ is the number of objects in $\sigma \in C$ with $p(\sigma) = \underline{i}$ and $|\sigma| = n$.

Example 2.1

If B is the class of binary strings (where $|\sigma| = len(\sigma)$), and $p(\sigma) = \#$ of zeros in σ, then

$$B(u, z) = \sum_{n \geq 0} \left(\sum_{k \geq 0} \binom{n}{k} u^k \right) z^n = \sum_{n \geq 0} (1+u)^n z^n = \sum_{n \geq 0} [(1+u)z]^n = \frac{1}{1-(1+u)z}$$

which exists only if we view z as the variable instead of u. Because each coefficient of z is a (Laurent) polynomial in u, we can set $u = 1$ to get $B(1, z) = 1/(1-2z)$, which is the generating function of all binary strings.

Lecture 12 - Monday, September 29

Example 2.2

Let T be the class of planar binary trees (with size = # of vertices). Let $p(z) = \#$ of leaves in the tree, so

$$T(u, x) = 1 + ux + (2u)x^2 + (4u + u^2)x^3 + \cdots$$

Note 2.2

Note that $C(\underline{1}, x) = C(x)$ is the regular generating function for the class $(C, |\bullet|)$. Also note that if $C(\underline{u}, x)$ is a polynomial in u (with no negative powers), then

$$C(0, x) = \textit{ generating function for objects with parameter value 0}$$

Note 2.3

If $C(\underline{u}, x)$ has no negative power of $\underline{u}$ and $C(\underline{u}, x)$ is rational, then the generating function $C(0, x)$ where the parameter values are all 0 is also rational.

Example 2.3

This serves as an example to the note above. Let D = walks on $\nearrow = (1,1)$ and $\searrow = (1,-1)$ that start at $(0,0)$ with $|w| = \#$ of steps in w. Let $p(w)$ = ending height (y-coordinate). One can show that

$$D(u,x) = \frac{1}{1-(u+1/u)\,x}$$

If $R(x)$ is the generating function for the walks ending with height 0 (end on the x-axis), then

$$R(x) = \sum_{n\geq 0} \binom{2n}{n} x^n = (1-4n)^{-1/2}$$

which is indeed not rational.

2.1 Combanotorial Construction with Parameters

Suppose that we have two combinatorial classes with parameter $(A, |\bullet|_A, p(A))$ and $(B, |\bullet|_B, p_B)$.

Definition 2.3: Inherited

We say that a parameter is **inherited** with respect to a construction if it behaves "nicely" under that construction.

1. If $C = A + B$, then $p_C : C \to \mathbb{Z}^d$ is inherited with respect to sum if

$$p_C(\sigma) = \begin{cases} p_A(\sigma) & \sigma \in A \\ p_B(\sigma) & \sigma \in B \end{cases}$$

2. If $C = A \times B$, then $p_C : C \to \mathbb{Z}^d$ is inherited with respect to product if

$$p_C((\alpha,\beta)) = p_A(\alpha) + p_B(\beta) \qquad \forall\, (\alpha,\beta) \in C$$

3. If A has no object of size 0, and $C = SEQ(A)$, then p_C is inherited with respect to SEQ if

$$p_C((\alpha_1,\ldots,\alpha_\ell)) = p_A(\alpha_1) + \cdots + p_A(\alpha_\ell)$$

We will say that a parameter is inherited if it is inherited with respect to some product (and SEQ).

Example 2.4: Non-example

Let B be the class of binary trees, let $p_B(\tau)$ = height of τ (i.e., the maximum length path from the root to a leaf). We know that

$$B = \mathcal{E} + Z \times B^2$$

then we have

$$p(\tau) = 1 + \max\{\, p(\tau_1),\, p(\tau_2)\,\}$$

where τ_1 and τ_2 are the two subtrees of τ. Notice that this parameter is not inherited.

Lemma 2.1

If p_C is inherited and

- $C = A + B$, then $C(\underline{u}, x) = A(\underline{u}, x) + B(\underline{u}, x)$;
- $C = A \times B$, then $C(\underline{u}, x) = A(\underline{u}, x)B(\underline{u}, x)$;
- $C = SEQ(A)$, then $C(\underline{u}, x) = 1/(1 - A(\underline{u}, x))$.

To use these constructions, we need some "parameterized base caes". We introduce the classes $\mu_1, \ldots, \mu_d$ where μ_k has size 0 and $p(\mu_k) = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 appears on the k^{th} spot. These are **marking classes**. Similarly, we also have the classes μ_k^{-1}, who has k^{th} parameter value of -1 and every thing else zero.

Example 2.5

If B is the class of binary strings, and $p : B \to \mathbb{N}^2$ defined as $p(\sigma) = (\#\, 0's, \#\, 1's)$. Then p is inherited and we can write

$$B = SEQ(\underbrace{\mu_1 \times Z_0}_{GF\ u_1 x} + \underbrace{\mu_2 \times Z_1}_{GF\ u_2 x})$$

and hence

$$B(\underline{u}, x) = \frac{1}{1 - (u_1 x + u_2 x)}$$

Comment 2.3

If $d = 1$ (i.e., dimension of parameter is only 1), then we usually just write μ.

Lecture 13 - Wednesday, October 01

In class midterm today.

Lecture 14 - Friday, October 03

Example 2.6

Let B be the class of binary strings and $p(\sigma)$ = number of zeros in σ. Then

$$B = SEQ(Z_0 \times \mu + Z_1) \quad \Longrightarrow \quad B(u,x) = \frac{1}{1-(ux+x)}$$

Example 2.7

Let W be the class of paths starting at $(0,0)$ and have steps $\nearrow = (1,1)$ and $\searrow = (1,-1)$. Let $p(w)$ = ending height of w. Then

$$W = SEQ(Z_{\nearrow} \times \mu + Z_{\searrow} \times \mu^{-1}) \quad \Longrightarrow \quad W(u,x) = \frac{1}{1-(ux+x/u)}$$

Example 2.8

Let T be the class of (rooted planar) binary trees, so

$$T = \mathcal{E} + Z \times T^2$$

We want $p(t)$ = number of leaves in T. However, in the above specification of these trees, it is hard to tell whether we are looking ar a leaf or not. Hence we want something different that are easier to deal with, so we do the following: Let N be the class of binary trees that are non-empty, so we have

$$N = Z \times \mu + Z \times N \times \mathcal{E} + Z \times \mathcal{E} \times N + Z \times N \times N$$

This yields us

$$N(u,x) = ux + 2xN(u,x) + xN(u,x)^2$$

which is sovled to be

$$N(u,x) = \frac{1-2x-\sqrt{1-4x+(1-u)4x^2}}{2x}$$

2.1.1 Formal Partial Derivative and Expected Value (when $d=1$)

Definition 2.4: Formal Partial Derivative

The **formal partial derivative** of $F(u,x) = \sum_{n\geq 0}\left(\sum_{k\in\mathbb{Z}} f_{k,n}u^k\right)x^n$ is

$$F_u(u,x) = \sum_{n\geq 0}\left(\sum_{k\in\mathbb{Z}} k\cdot f_{k,n}u^{k-1}\right)x^n$$

Definition 2.5: Expected Value

The **expected value** of $p : C \to \mathbb{Z}$ on the object of size n is

$$\mathbb{E}_n(p) = \sum_{k \in \mathbb{Z}} \left(k \cdot [\texttt{Probability that } p(\sigma) = k \texttt{ when } |\sigma| = n] \right)$$

Note 2.4

We have

$$\mathbb{E}_n(p) = \sum_{k \in \mathbb{Z}} \frac{k \cdot C_{k,n}}{C_n} \tag{1}$$

Proposition 2.1

For any $n \in \mathbb{N}$, we have

$$\mathbb{E}_n(p) = \frac{[x^n]C_u(1,x)}{[x^n]C(1,x)}$$

Proof. Definition check. □

Comment 2.4

Because our definition of formal partial derivative matches the usual derivative for functions from Calculus, the derivatives behave like they would in Calculus.

Example 2.9

Let B be the class of binary strings and $p(\sigma) =$ number of zeros in σ. We just saw that

$$B(u,x) = \frac{1}{1-(1+u)x}$$

Now we have

$$B_u(u,x) = \frac{x}{[1-(1+u)x]^2} \quad \Longrightarrow \quad B_u(1,x) = \frac{x}{(1-2x)^2}$$

The Negative Binomial Theorem implies that if $n \geq 1$,

$$[x^n]\frac{x}{(1-2x)^2} = 2^{n-1}\binom{n}{n-1} = n \cdot 2^{n-1}$$

and so for $n \geq 1$, $E_n[p] = n2^{n-1}/2^n = n/2z$.

Example 2.10

Let C be the class of integer composition and $p(\sigma)$ = the number of ones in σ. Hence

$$C = SEQ(Z + Z^2 \times SEQ(Z))$$

and

$$C(u,x) = \frac{1}{1 - \left(ux + \frac{x^2}{1-x}\right)} = \frac{1-x}{(1-x)(1-ux) - x^2}$$

Recall that we have already seen that if $n \geq 1$, then $[x^n]C(1,x) = 2^{n-1}$. For the numerator to compute the expected value, we have

$$C_u(1,x) = \left[\frac{(1-x)^2 x}{[(1-x)(1-ux) - x^2]^2}\right]\Big|_{u=1} = \frac{(1-x)^2 x}{(1-2x)^2}$$

and for $n \geq 3$, we have

$$\begin{aligned}
[x^n]C_u(1,x) &= [x^{n-1}](1-2x)^{-2} - 2[x^{n-2}](1-2x)^{-2} + [x^{n-3}](1-2x)^{-2} \\
&= n \cdot 2^{n-1} + 2^{n-1} \cdot (n-1) + 2^{n-3} \cdot (n-2) \\
&= 2^{n-2} + 2^{n-3} \cdot n
\end{aligned}$$

Now, we can compute that

$$\mathbb{E}_n(p) = \frac{2^{n-2} + 2^{n-3} \cdot n}{2^{n-1}} = \frac{2+n}{4} \left(\approx \frac{n}{4}\right)$$

When $n = 1$ or $n = 2$, the expected values are both 1.

Lecture 15 - Monday, October 06

Proposition 2.2

Here are some nice facts:

$$[x^n]\frac{\mathrm{d}}{\mathrm{d}u}C(u,x) = \frac{\mathrm{d}}{\mathrm{d}u}[x^n]C(u,x)$$

$$[x^n]\left(A(u,x)\big|_{u=1}\right) = ([x^n]A(u,x))\big|_{u=1}$$

Exercise 2.1

Find the average value of leaves among the binary tres of size n.

Solution. Let N be the class of non-empty binary trees. Recall that we have

$$N(u,x) = ux + 2xN(u,x) + xN(u,x)^2$$

$$\implies x = \frac{N(u,x)}{G(N(u,x))}$$

where $G(t) = u + 2t + t^2$.

Comment 2.5

Thinking of $N(u,x)$ in $\mathbb{Q}[u][[x]]$ and $G(t)$ in $\mathbb{Q}[u][t]$.

LIFT 1.3 implies that

$$\begin{aligned}
[x^n]N_u(1,x) = [x^n]\frac{\mathrm{d}}{\mathrm{d}u}N(u,x)\big|_{u=1} &= \frac{\mathrm{d}}{\mathrm{d}u}\left([x^n]N(u,x)\right)\big|_{u=1} \\
&= \frac{\mathrm{d}}{\mathrm{d}u}\left[\frac{1}{n}[x^n]\left(u+2t+t^2\right)^n\right]\big|_{u=1} \\
&= [t^{n-1}](u+2t+t^2)^{n-1}\big|_{u=1} \\
&= [t^{n-1}](1+2t+t^2)^{n-1} \\
&= [t^{n-1}](1+t)^{2n-2} = \binom{2n-2}{n-1} \quad \text{if } n \geq 1
\end{aligned}$$

We have seem that there are $[x^n]N(1,x) = \dfrac{1}{n+1}\dbinom{2n}{n}$ binary trees on n vertices, so if $n \geq 1$,

$$\mathbb{E}_n[p] = \frac{\binom{2n-2}{n-1}}{\frac{1}{n+1}\binom{2n}{n}} = \frac{n(n+1)}{2(2n-1)} \approx \frac{n}{4}$$

by proposition 2.1, as desired. □

2.1.2 Variance

Definition 2.6: Variance

We define **variance** to be

$$\mathrm{Var}_n[p] = \mathbb{E}_n[p^2] - \mathbb{E}_n[p]^2$$

Proposition 2.3

We have

$$\mathrm{Var}_n[p] = \frac{[x^n]\left(C_{uu}(1,x) + C_u(1,x)\right)}{[x^n]C(1,x)} - \left[\frac{[x^n]C_u(1,x)}{[x^n]C(1,x)}\right]^2$$

Proposition 2.4

If $\mathbb{E}_n[p] \neq 0$ for all n sufficiently large, and

$$\frac{\mathrm{Var}_n[p]}{\mathbb{E}_n[p]^2} \to 0 \quad \text{as} \quad n \to \infty$$

Then for any fixed $\varepsilon > 0$, the probability that a random object $\sigma \in C$ of size n satisfies

$$(1-\varepsilon)\mathbb{E}_n[p] \leq p(\sigma) \leq (1+\varepsilon)\mathbb{E}_n[p]$$

goes to 1 as $n \to \infty$.

2.2 q-Analogues

Idea: take an identity that we have a combinatorial proof for, track a parameter, and get an identity involving polynomials.

Question 2.1.

What things have appeared in our combinatorial proofs?

Answer. We have seen powers (2^n), binomial coefficients (involving factorials), and sums, etc. $\square$

Comment 2.6

We wish to generalize these to polynomials tracking parameters.

2.2.1 q-Factorials

$n!$ counts the number of permutations. We will make a q-analogue involving permutations and a statistic.

Definition 2.7: Inversion

Let $\pi = \pi_1\pi_2\cdots\pi_n$ be a permutation of $[n] = \{1, \ldots, n\}$. An **inversion** in π is a pair (i, j) with $1 \le i < j \le n$ such that $\pi_i > \pi_j$. We let $\mathrm{inv}(\pi)$ be the number of inversions of π.

Example 2.11

Consider 13846725, it has the inversion number of value 11.

Definition 2.8: $[k]_q$

For $k \in \mathbb{N}$, we define

$$[k]_q = 1 + q + q^2 + \cdots + q^{k-1}$$

and $[0]_q = 1$.

Definition 2.9: q-factorial

The **q-factorial** of $n \in \mathbb{N}$ is

$$[n]!_q = [n]_q \cdot [n-1]_q \cdots [0]_q$$

Note 2.5

We note that

$$([n]!_q)_{q=1} = n!$$

$$[k]_q = \frac{1-q^k}{1-q}$$

2.2.2 q-Factorial Theorem

Theorem 2.1: q-Factorial Theorem

If S_n = set of permutations of size n, then

$$\sum_{\pi \in S_n} q^{\mathrm{inv}(\pi)} = [n]!_q$$

Proof. We build $\omega \in S_n$ from $u \in S_{n-1}$ by adding n into the 1-line notation for u in any of the n spots. We claim that the number of possible inv's for the new permutation are $\mathrm{inv}(u), \ldots, \mathrm{inv}(u) + n - 1$. This is indeed true because the number of extra inversions is just the number of values to the right of n. Therefore, we have

$$\sum_{\omega \in S_n} q^{\mathrm{inv}(\omega)} = [n]_q \sum_{u \in S_{n-1}} q^{\mathrm{inv}(u)} = [n]_q!$$

as desired. □

Lecture 16 - Wednesday, October 08

Comment 2.7

If $f : A \to B$ is a bijection between finite sets A and B, and p is a function on A, then

$$\sum_{\alpha \in A} p(\alpha) = \sum_{\beta \in B} q(\beta)$$

where $q(\beta)$ denotes $p(\alpha)$ for the unique $\alpha \in A$ with $f(\alpha) = \beta$.

Exercise 2.2

Show that $|S_n| = n!$.

Proof. Here we give a bijective proof. This holds when $n = 0$ so we assume $n \geq 0$. Define

$$P_n = [n] \times [n-1] \cdots [1]$$

so $|P_n| = n!$. Let $I : S_n \to P_n$ be the map that takes a permutation $\pi = \pi_1\pi_2 \ldots \pi_n$ and returns the tuple $(1 + r_1, \ldots, 1 + r_n)$ where r_i = the number of inversions starting at position i. This is clearly well-defined because at any position k, the number of inversions starting at k can be at most $n - k$. Let $J : P_n \to S_n$ be the map takes $(s_1, \ldots, s_n) \in P_n$ and returns $\pi = \pi_1 \ldots \pi_n$ built inductively by setting π_i to be the i^{th} smallest number in the remaining $[n]$ (remaining in the sense that there is no repetition in a permutation).

The part that shows I and J are inverses is left as an exercise. □

2.2.3 q-Binomials

Fix $n, k \in \mathbb{N}$ with $0 \leq k \leq n$, we define

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]!_q}{[k]!_q [n-k]!_q}$$

Example 2.12

As an example, we have

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{[4]!_q}{[2]!_q[2]!_q} = \frac{(1+q+q^2+q^3)(1+q+q^2(1+q))}{(1+q)(1+q)} = q^4+q^3+2q^2+q+1$$

We will sometimes show how we can get the result quickly in sage.

If $\{s_1, \ldots, s_k\} \subseteq [n]$, we define

$$\text{sum}(\{s_1, \ldots, s_k\}) = \sum s_i$$

Theorem 2.2: q-Binomial Theorem

For $n \in \mathbb{N}$, we have

$$\prod_{k=1}^{n}(1+q^k z) = \sum_{S \subseteq [n]} q^{\text{sum}(S)} z^{|S|} = \sum_{k=0}^{n} q^{k(k+1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q z^k$$

Proof. We first prove the first equality. Fix n, let B_n be the class of subsets of $[n]$ counted by size and sum. Then

$$\begin{aligned} B_n &= (\mathcal{E} + \mu \cdot z_1) \times (\mathcal{E} + \mu^2 \cdot z_2) \cdots (\mathcal{E} + \mu^n \cdot z_n) \\ \implies \quad \sum_{S \subseteq [n]} q^{\text{sum}(S)} z^{|S|} &= B_n(u, z) = (1+uz)(1+u^2 z)\cdots(1+u^n z) \end{aligned}$$

Now we prove the second equality, which needs a bit more effort. For $0 \leq k \leq n$, let $B_n(k)$ be the subsets of n with k elements. so $|B_n(k)| = \binom{n}{k}$. Observe that

$$[n]!_q = [k]!_q [n-k]!_q \begin{bmatrix} n \\ k \end{bmatrix}_q$$

Define $\varphi_{n,k} : S_n \to B_n(k) \times S_k \times S_{n-k}$ in the following way: Given $a_1, \ldots, a_m$ distinct positive integers, let $P(a_1, \ldots, a_m)$ be the permutation obtained by replacing each a_i with its relative order.

Lecture 17 - Friday, October 10

For instance, $P(3, 19, 5, 10, 20) = 14235$.

We define

$$\varphi_{n,k}(\sigma_1\sigma_2\ldots\sigma_n) = \Big(\{\sigma_1, \ldots, \sigma_k\}, P(\sigma_1, \ldots, \sigma_k), P(\sigma_{k+1}, \ldots, \sigma_n)\Big)$$

Exercise 2.3

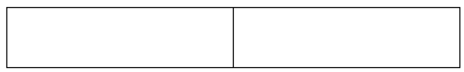
Prove that this is a bijection.

Exercise 2.4

If $\varphi_{n,k} = (\alpha, \beta, \gamma)$, then

$$\mathrm{inv}(\sigma) = \left(\mathrm{sum}(\alpha)\frac{k(k+1)}{2}\right) + \mathrm{inv}(\beta) + \mathrm{inv}(\gamma)$$

Here is the idea:



Let

$$\begin{aligned} E_1 &= \text{ inversions } (i,j) \text{ where } i < j \leq k \\ E_2 &= \text{ inversions } (i,j) \text{ where } k+1 \leq i < j \\ E_3 &= \text{ inversions } (i,j) \text{ where } i < k < j \end{aligned}$$

and thus $|E_1| = \mathrm{inv}(\beta)$, $|E_2| = \mathrm{inv}(\gamma)$, so it suffices to show that $|E_3| = \mathrm{sum}(\alpha) - k(k+1)/2$. We know that an inversion in E_3 corresponds to numbers $(a, z) \in [n]$ where $a \in \{\sigma_1, \ldots, \sigma_k\} = \alpha$ and $z \in [n] \setminus \alpha$ and $a > z$. Let S_i be the i^{th} smallest element of α, then

- S_i is the number of elements in $[n]$ that are $\leq S_i$;
- i is the number of elements in α that are $\leq S_i$.

and hence $S_i - i$ is the number of elements in $[n] - \alpha$ that are $\leq S_i$. Now, $|E_3| = (S_1 - 1) + (S_2 - 2) + \cdots + (S_k - k) = \mathrm{sum}(\alpha) - k(k+1)/2$, as desired.

Now we can finish our proof. We now have

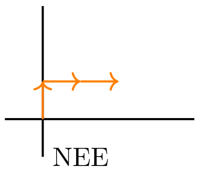
$$\begin{aligned} [n]!_q &= \sum_{\sigma \in S_n} q^{\mathrm{inv}(\sigma)} \\ &= \sum_{(\alpha,\beta,\gamma) \in B_n(k) \times S_k \times S_{n-k}} q^{\mathrm{sum}(\alpha) - k(k+1)/2 + \mathrm{inv}(\beta) + \mathrm{inv}(\gamma)} \\ &= q^{-k(k+1)/2} \left(\sum_{\alpha \in B_n(k)} q^{\mathrm{sum}(\alpha)} \right) \left(\sum_{\beta \in S_k} q^{\mathrm{inv}(\beta)} \right) \left(\sum_{\gamma \in S_{n-k}} q^{\mathrm{inv}(\gamma)} \right) \\ &= q^{-k(k+1)/2} \left(\sum_{\alpha \in B_n(k)} q^{\mathrm{sum}(\alpha)} \right) [k]!_q [n-k]!_q \end{aligned}$$

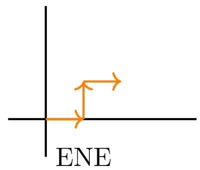
$$\implies \sum_{\alpha \in B_n(k)} q^{\mathrm{sum}(\alpha)} = \sum_{k=0}^{n} q^{k(k+1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q z^k$$

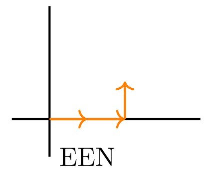
□

2.2.4 q-Lattice Paths

Let $L(a, b)$ for $a, b \in \mathbb{N}$ be lattice paths from $(0, 0)$ to (a, b) consisting of $E = (1, 0)$ and $N = (0, 1)$ steps. Here are some examples







It is easy to observe that $|L(a, b)| = \binom{a+b}{a}$. We define

$$\text{area}(P) = \text{ number of boxes under } P \text{ and above the } x\text{-axis}$$

Example 2.13

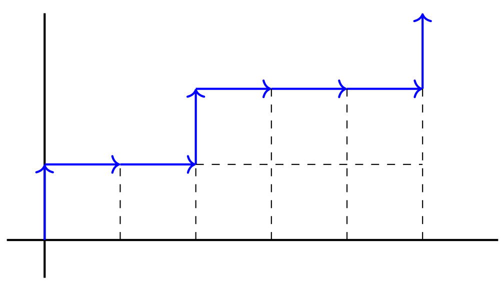
In the above three graphs, they have are of 2, 1, and zero respectively.

Theorem 2.3: q-Lattice Path Theorem

For any $a, b \in \mathbb{N}$,

$$\sum_{P \in L(a,b)} q^{\text{area}(P)} = \begin{bmatrix} a+b \\ a \end{bmatrix}_q$$

Proof. Let $f : L(a, b) \to B_{a+b}(a)$ be the function that maps a path P to the indices of its East steps. Suppose $f(P) = \{s_1, \ldots, s_a\}$ where the s_i are in increasing order. Here is an example



Notice that the number of boxes of P in the column whose top is the s_1^{th} step equals the number of North steps before the column. Observe that there are i East steps before s_i, and there are s_i total steps up to s_i, so $s_i - i$ is the number of North steps up to s_i. Thus

$$\text{area}(P) = \text{sum}(f(P)) - \sum_{i=1}^{a} i = \text{sum}(f(P)) - \frac{a(a+1)}{2}$$

As a result,

$$\sum_{P \in L(a,b)} q^{\text{area}(P)} = \sum_{S \in B_{a+b}(a)} q^{\text{sum}(f(S)) - a(a+1)/2} = \begin{bmatrix} a+b \\ a \end{bmatrix}_q \cdot q^{a(a+1)/2} \cdot q^{-a(a+1)/2}$$
$$= \begin{bmatrix} a+b \\ a \end{bmatrix}_q$$

as desired. $\square$

2.2.5 Use them as our tools

Example 2.14

Prove that
$$\begin{bmatrix} 2n \\ n \end{bmatrix}_q = \sum_{k=0}^{n} q^{k^2} \begin{bmatrix} n \\ k \end{bmatrix}_q^2 \quad \text{for any } n \in \mathbb{N}$$

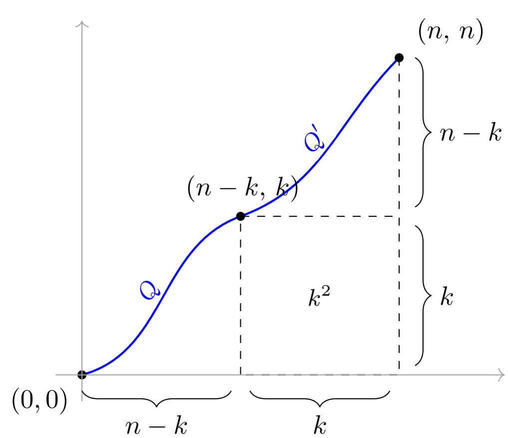
Proof. Setting $q = 1$ yields us
$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$$

We can prove this combinatorially using lattice paths: $|L(n,n)| = \binom{2n}{n}$. Decomposing an element P of $L(n,n)$ as a walk $P_1 \dots P_n$ defined by its first n steps followed by $P_{n+1} \dots P_n$ gives a bijection

$$f : L(n,n) \to \bigcup_{k=0}^{n} L(n-k,k) \times L(k,n-k)$$

and so
$$\binom{2n}{n} = |L(n,n)| = \sum_{k=0}^{n} |L(n-k,k)| \cdot |L(k,n-k)|$$
$$= \sum_{k=0}^{n} \binom{n}{n-k} \binom{n}{k}$$

If $f(P) = (Q, Q')$, then $\text{area}(P) = \text{area}(Q) + \text{area}(Q') + k^2$.



Now we are done, because

$$\begin{bmatrix} 2n \\ n \end{bmatrix}_q = \sum_{P \in L(n,n)} q^{\text{area}(P)} = \sum_{k=0}^{n} \sum_{Q \in L(n-k,k), Q' \in L(k,n-k)} q^{\text{area}(Q)+\text{area}(Q')+k^2}$$
$$= \sum_{k=0}^{n} q^{k^2} \begin{bmatrix} n \\ k \end{bmatrix}_q^2$$

as desired. □

Lecture 18 - Monday, October 20

Yapping about Sage again ...

2.3 Integer Partitions

Definition 2.10: Integer Partition

An **integer partition** of size n is a tuple of positive integers $(p_1, p_2, \ldots, p_r)$ with

$$p_1 + p_2 + \cdots + p_r = n \quad \text{and} \quad q_1 \geq q_2 \geq \cdots \geq q_r$$

Example 2.15

As an example, $3 = 2 + 1 = 1 + 1 + 1$.

If we have a partition $\lambda = (\lambda_1, \ldots, \lambda_r)$, then we write

$$|\lambda| = n(\lambda) = \lambda_1 + \lambda_2 + \cdots + \lambda_r$$
$$\kappa(\lambda) = r$$

Let Y be the class of (integer) partition.

Note 2.6

There is no nice formula for $P_n = |Y_n| = \#$ of partitions of size n, but we can still do a lot of interesting stuffs.

2.3.1 Tool 1, Generating Function

Theorem 2.4

The generating function for partitions is

$$\Phi(x) = \sum_{\lambda \in Y} x^{n(\lambda)} = \prod_{k \geq 1} \left(\frac{1}{1 - x^k} \right)$$

Proof. Think of a partition as a sequence of 1s, followed by a sequence of 2s, and so on. Then

$$\begin{aligned}\Phi(x) &= (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^3 + x^6 + \cdots)\cdots \\ &= \prod_{k\geq 1}\left(\frac{1}{1-x}\right)\end{aligned}$$

as desired. □

Theorem 2.5

The bivariate generating function enumerating partitions by size and number of parts is

$$\Phi(u,x) = \sum_{\lambda\in Y} u^{\kappa(\lambda)}x^{n(\lambda)} = \prod_{k\geq 0}\left(\frac{1}{1-ux^k}\right)$$

Proof. The idea is that

$$\Phi(u,x) = (1 + ux + u^2x^2 + \cdots)(1 + ux^2 + u^2x^4 + \cdots)(1 + ux^3 + u^2x^6 + \cdots)\cdots$$

yeah. □

2.3.2 Partition Generating Function Theorem

Lecture 19 - Wednesday, October 22

Theorem 2.6

For each $k \geq 1$, let M_k be a subset of $\mathbb{N}$. The bivariate generating function $\Phi(u,x)$, tracking size and number of parts, for the subclass of partitions where the number of parts equal to k lies in M_k for all k is

$$\Phi(u,x) = \prod_{k\geq 1}\left(\sum_{j\in M_k}(ux^k)^j\right)$$

Example 2.16

As an example, let $M_k = \mathbb{N}$ for all k, then

$$\Phi(u,x) = \prod_{k\geq 1}\left(\sum_{j\geq 0}(ux^k)^j\right) = \prod_{k\geq 1}\frac{1}{1-ux^k}$$

Note 2.7

Note that if we take $u = 1$, then we get the generating function just tracking size.

Example 2.17

The univariate generating function for partitions where every part is even is derived by tracking

$$M_k = \begin{cases} \mathbb{N} & k \text{ is even} \\ \{0\} & k \text{ is odd} \end{cases}$$

so that

$$\Phi(u,x) = \prod_{k\geq 1}\left(\sum_{j\geq 0}(x^{2k})^j\right) = \prod_{k\geq 1}\frac{1}{1-ux^{2k}}$$

Proof for Theorem 2.6. Let

$$\begin{aligned} Y_M &= \{\text{ class of partitions }\} \\ S_M &= \{\text{ sequence } \mathbf{r} = (r_1, r_2, \ldots) \text{ whith only a finite number of non-zero terms where } r_j \in M_j \text{ for all } j\ \} \end{aligned}$$

Define $f : Y_M \to S_M$ by $f(\lambda) = \mathbf{r}$ where r_j = number of times j appears in λ. Our claim is that f is a bijection. Thus,

$$\begin{aligned} \Phi(u,x) = \sum_{\lambda\in Y_M} u^{\kappa(\lambda)}x^{n(\lambda)} &= \sum_{\mathbf{r}\in S_M} u^{r_1+r_2+\cdots}x^{1\cdot r_1+2\cdot r_2+\cdots} \\ &= \left(\sum_{r_1\in M_1}(ux)^{r_1}\right)\left(\sum_{r_2\in M_2}(ux^2)^{r_2}\right)\cdots \\ &- \prod_{k\geq 1}\left(\sum_{j\in M_k}(ux^k)^j\right) \end{aligned}$$

ermmmm. □

Example 2.18

Show that for $n \geq 0$, the number of partitions of n with odd parts equals the number of partitions of n with distinct parts.

Proof. The Partition GF Theorem 2.6 implies that the generating function for partitions with distinct parts is

$$\begin{aligned} \prod_{k\geq 1}(1+x^k) &= \prod_{k\geq 1}(1+x^k)\cdot\left(\frac{1-x^k}{1-x^k}\right) \\ &= \frac{\prod_{k\geq 1}(1+x^{2k})}{\prod_{k\geq 1}(1+x^k)} \\ &= \prod_{k\geq 1}\left(\frac{1}{1-x^{2k-1}}\right) \end{aligned}$$

wwwww. □

2.3.3 Partition Diagrams

It can be useful to reperesent a partition graphically.

Definition 2.11: Ferrer's Diagram

If $\lambda = (\lambda_1, \ldots, \lambda_r)$, its Ferrer's diagram consists of r rows with the i^{th} row having λ_i dots.

Definition 2.12: Young Diagram

If $\lambda = (\lambda_1, \ldots, \lambda_r)$, its Ferrer's diagram consists of r rows with the i^{th} row having λ_i boxes.

We notice that there is a correspondance:

Partition	Diagram
size	number of dots
number of parts	number of rows
largest part	number of columns

Definition 2.13: Conjugate Partition

If $\lambda = (\lambda_1, \ldots, \lambda_r)$ is a partition of n with largest part $\lambda_1 = \ell$, then its **conjugate partition** is the partition $\lambda' = (\lambda'_1, \ldots, \lambda'_\ell)$ of n with λ'_j = number of indices $i \in \{1, \ldots, \ell\}$ such that $\lambda_i \geq j$.

Note 2.8

It is just view the Ferrer's diagram flipped over $y = -x$ (swapping rows and columns). Why is this?

Note 2.9

The map $\lambda \mapsto \lambda'$ is a bijection and is its own inverse.

Definition 2.14: Self-conjugate

A partition is called **self-conjugate** if $\lambda = \lambda'$.

Lemma 2.2

For any $n \geq 0$, and positive integer k, the number of partitions of size n with k parts equals the number of partitions of size n with maximum part k.

Proof. Easy just by looking at the diagram. □

Durfee Square

Definition 2.15: Durfee Length

If λ is a partition, then its **Durfee length** $d(\lambda)$ is the number of indices i such that $\lambda_i \geq i$.

Definition 2.16: Durfee Square

Durfee square is the largest square makde up of dots in the Ferrer's diagram.

Comment 2.8

Observe that the Durfee length is the side length of the Durfee square.

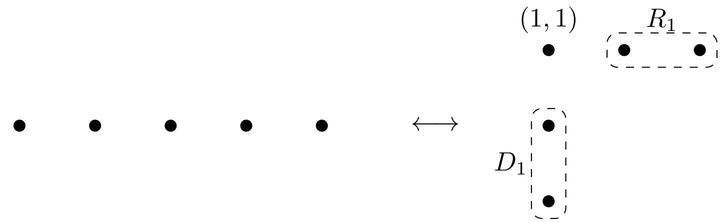
Proposition 2.5

Let S be the class of self-conjugate partitions (i.e., $\lambda \in S$ satisfies $\lambda = \lambda'$), then

$$\sum_{\lambda \in S} u^{d(\lambda)} x^{n(\lambda)} = \prod_{k \geq 1} \left(1 + ux^{2k-1}\right)$$

Lecture 20 - Friday, October 24

Proof sketch. Let O be the class of partitions with odd distinct parts. It is sufficient to find a bijection $f : S \to O$ that preserves size and sends Durfee length to the number of parts. The idea is: A row with an odd number of does in O can be "folded":



Formally, given $\lambda \in S$, let R_j be the points in λ to the right of (j, j), and D_j be the points in λ below (j, j). Because λ is self-conjugate, we have $|R_j| = |D_j|$. Define $f : S \to O$ by $f(\lambda) = (\mu_1, \ldots, \mu_{d(\lambda)})$ where $\mu_j = |R_j| + |D_j| + 1$. □

Exercise 2.5

Show that f defined above is a bijection.

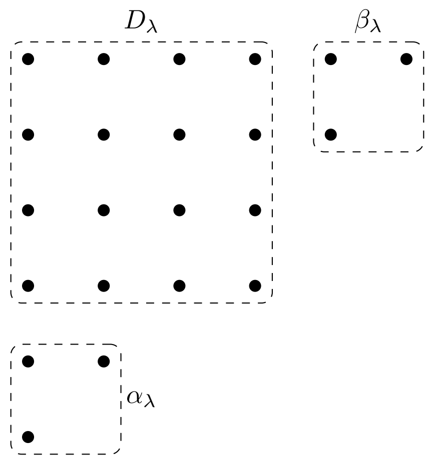
2.3.4 Euler's Identity

Theorem 2.7: Euler's Identity

We have

$$\prod_{j\geq 1} \frac{1}{1-yx^j} = \sum_{d\geq 0} \frac{x^{d^z} y^d}{\prod_{i=1}^{d}(1-yx^i)(1-x^i)}$$

Proof sketch. LHS is the generating function for partitions enumerated by size and number of parts $(u = y)$.



We can decompose a partition λ into:

$$\begin{aligned} D_\lambda &= \text{ Durfee square} \\ \alpha_\lambda &= \text{ dots under } D_\lambda && \longleftarrow \text{ partition} \\ \beta_\lambda &= \text{ dots to the right of } D_\lambda && \longleftarrow \text{ partition} \end{aligned}$$

α_λ is a partition with parts of size $\leq d(\lambda)$, and β_λ is a partition with $\leq d(\lambda)$ parts. Number of parts in λ is $d(\lambda) = \#$ parts in α_λ.

This decomposition implies a bijection from

$$Y \longleftarrow \text{ disjoint union } \bigcup_{d\geq 0} \{d\} \times A_d \times B_d$$

where A_d denotes $\leq d$ parts and B_d denotes parts of size $\leq d$. $\square$

2.4 Exercises

2.4.1 Parameters and Multivariate GFs

Exercise 2.6

Find the average number of summands among all compositions of size n.

Exercise 2.7

Find the bivariate generating function for binary strings with no consecutive zeroes enumerated by size and number of zeroes.

Proof. We have the following regular expression:

$$(01 \smile 1)^*(0 \smile \varepsilon)$$

□

2.4.2 q-Analogue

Exercise 2.8

Give a combinatorial proof involving lattice paths that, for all $a, b, n \in \mathbb{N}$ with $0 \leq a \leq b$,

$$\binom{b+n+1}{n} = \sum_{j=0}^{n} \binom{a+j}{j} \binom{(b-a)+(n-j)}{n-j}.$$

Proof. Identifying a lattice path from $(0,0)$ to $(b+1,n)$ by its edge from $x=a$ to $x=a+1$. □

Exercise 2.9

Prove a q-analogue of the identity in the above exercise (i.e., an identity where the binomial coefficients are replaced by q-binomial coefficients, potentially after multiplying by an extra power of q).

Proof. I think we can show that

$$\begin{bmatrix} b+n-1 \\ n \end{bmatrix}_q = \sum_{j=0}^{n} q^j \begin{bmatrix} a+j \\ j \end{bmatrix}_q \begin{bmatrix} (b-a)+(n-j) \\ n-j \end{bmatrix}_q$$

□

Exercise 2.10

Prove that

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q,$$

for all $n, k \in \mathbb{N}$ with $k \leq n$.

Proof. Split the lattice paths to two cases depend on the first step. On the RHS, the first expression correspond to the case of up step, while the second correspond to the case of right step. □

2.4.3 Integer Partitions

Exercise 2.11

Write down an expression for the bivariate generating function enumerating the following classes of partitions with respect to size and number of parts.

(a) Partitions in which even parts occur at most twice.

(b) Partitions in which the parts of size at most 20 must be distinct.

(c) Partitions in which the multiplicity of a part j is either 0 or has the same parity as j.

(d) Partitions in which every part is either divisible by 3 or even.

Proof. We have

$$(a) \qquad \prod_{k\geq 1 \text{ odd}} \frac{1}{1-uz^k} \cdot \prod_{k\geq 2 \text{ even}} (1+uz^j+u^2z^{2j})$$

$$(b) \qquad \prod_{k=1}^{20}(1+ux^k) \cdot \prod_{k\geq 21} \frac{1}{1-ux^k}$$

$$(c) \qquad \prod_{k \text{ odd}} \left(1+\frac{ux^k}{1-(ux^k)^2}\right) \prod_{k \text{ even}} \left(\frac{1}{1-(ux^k)^2}\right)$$

$$(d) \qquad \frac{\prod_{k\geq 1} \frac{1}{1-ux^{2k}} \cdot \prod_{k\geq 1} \frac{1}{1-ux^{3k}}}{\prod_{k\geq 1} \frac{1}{1-ux^{6k}}}$$

□

Exercise 2.12

Let $\mathcal{A}$ be the class of partitions in which each part may occur $0, 1, 4,$ or 5 times, and let $\mathcal{B}$ be the class of partitions which have no parts congruent to $2 \pmod 4$ and in which parts divisible by 4 occur at most once each. Prove that for all n the number of partitions in $\mathcal{A}$ of size n equals the number of partitions in $\mathcal{B}$ of size n by showing that their generating functions are equal.

Proof. We have

$$\begin{aligned} A(x) &= \prod_{k\geq 1}(1+z+z^{4k}+z^{5k}) \\ &= \prod_{k\geq 1}(1+z)(1+z^{4k}) \end{aligned}$$

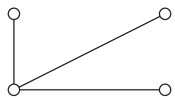
We can show that $B(x)$ is the same thing. □

3 Labelled Enumeration

In many contexts, it is natural to label atoms. A combinatorial object of size n is labelled by giving each atom a distinct number from $[n]$.

Example 3.1: s

Let $G = \{\text{graph}\}$. Consider the graph



If we were to label all the nodes using elements in $[4]$, we really only have 4 differnet labellings for the above graph, shown below:

A combinatorial class is labelled by labelling each of its objects, where each object is repeated with each non-equivalent labelling.

Example 3.2

We have $SEQ(Z) = \{\varepsilon, \bullet, \bullet\bullet, \bullet\bullet\bullet, \ldots\}$, so the labelled version is

$$\{\varepsilon, 1, 12, 21, 123, 132, 213, 231, 312, 321, \ldots\}$$

which is the class of permutations.

Definition 3.1: Exponential Generating Function

The **exponential generating function** of a sequence (c_n) is the formal power series

$$C(x) = \sum_{n \geq 0} \frac{c_n}{n!} x^n$$

Definition 3.2: Ordinary Generating Function

The **ordinary generating function** is $\sum_{n \geq 0} c_n x^n$.

Lecture 21 - Monday, October 27

3.1 Labelled Construction

As for unlabelled objects, we can build labelled classes recursively. One major takeaway from this section is that the exponential generating functions of labelled classes behave the same as the ordinary generating functions of unlabelled classes under our basic constructions.

We have the following base cases:

- Labelled Atomic Class $Z = \{\boxed{1}\}$;
- Labelled Neutral Class $\mathcal{E} = \{1 \text{ object of size } 0\}$;

Construction:

- **Laballed Sum:** If A and B are laballed classes, then their sum $C = A + B$ is the class formed by their disjoint union.

Lemma 3.1

We have $C(x) = A(x) + B(x)$.

Proof. Disjoint union implies that

$$
\begin{aligned}
C(x) = \sum_{n \geq 0} \frac{c_n}{n!} x^n &= \sum_{n \geq 0} \frac{(a_n + b_n)}{n!} x^n \\
&= \sum_{n \geq 0} \frac{a_n}{n!} x^n + \sum_{n \geq 0} \frac{b_n}{n!} x^n \\
&= A(x) + B(x)
\end{aligned}
$$

□

- **Labelled Product:** We want $A \times B$ to consist of elements (α, β) with $\alpha \in A$ and $\beta \in B$.

Note 3.1

The problem is that we will get duplicate labels. We see below how we resolve the problem.

Definition 3.3: Consistant Relabelling

A **consistant relabelling** of a labelled pair (α, β) of size $|\alpha| + |\beta|$ is an assignment of $\{1, 2, \ldots, |\alpha| + |\beta|\}$ to be the atoms in α and β such that each number is used exactly once, and

- the new labels on atoms in α are in the same relative order as the original labels on the atoms in α;
- the same for atoms in β.

We let $\alpha * \beta$ be the set of all consistant labellings of (α, β).

Example 3.3

We have

$$\boxed{1} * \boxed{1}\boxed{2}\boxed{3} = \left\{ (\boxed{1}, \boxed{1}\boxed{2}\boxed{3}), (\boxed{2}, \boxed{1}\boxed{3}\boxed{3}), (\boxed{3}, \boxed{1}\boxed{2}\boxed{4}), (\boxed{4}, \boxed{1}\boxed{2}\boxed{3}) \right\}$$

The labelled product $C = A \times B$ of labelled classes A and B is the class whose objects form the union $\bigcup_{\substack{\alpha \in A \\ \beta \in B}} (\alpha * \beta)$, with size $|(\alpha, \beta)| = |\alpha|_A + |\beta|_B$.

Lemma 3.2

If $C = A \times B$, then $C(x) = A(x)B(x)$.

Proof. Fix n. For any $0 \leq k \leq n$, there are a_k objects in A of size k and b_{n-k} objects in B of size $n-k$. Observe that a consistant relabelling of (α, β) with size n is uniquely defined by picking k numbers in $\{1, \dots, n\}$ to assign to the atoms in α, so there are $\binom{n}{k}$ consistant relabellings. Because we consistant relabellings in our construction for C, so

$$\begin{aligned} C(x) = \sum_{n \geq 0} \frac{c_n}{n!} x^n &= \sum_{n \geq 0} \left[\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \right] \frac{x^n}{n!} \\ &= \sum_{n \geq 0} \left[\sum_{k=0}^{n} \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!} \right] x^n = A(x)B(x) \end{aligned}$$

□

- **Labelled Power and Sequence:**
  - Let $A^k = \underbrace{A \times \cdots \times A}_{k \text{ times}}$, then $A^k(x) = A(x)^k$;
  - Let $SEQ(A) = \mathcal{E} + A + A^2 + \cdots$ and suppose A has no object of size 0, then $C = SEQ(A)$ implies $C(x) = \dfrac{1}{1 - A(x)}$.
- **Labelled Set**: Let A be a labelled combanitorial class. For any positive integer k, the class $SET_k(A)$ consists of the objects in A^k where two tuples are considered the same if they are equal up to a permutation.

Example 3.4

In $SET_3(A)$, the following objects are equivalenet:

$$(a_1, a_2, a_3) \equiv (a_1, a_3, a_2) \equiv (a_2, a_1, a_3) \equiv (a_2, a_3, a_1) \equiv (a_3, a_1, a_2) \equiv (a_3, a_2, a_1)$$

If $C = SET_k(A)$, then, since there are $k!$ permutations for a k-tuple, and no a_i and a_j with $i \neq j$ can be equal because of their labels, we have

$$C(x) = \frac{A(x)^k}{k!}$$

when A has no objects of size 0, then we define

$$SET(A) = \mathcal{E} + SET_1(A) + SET_2(A) + \cdots$$

and we have the following result:

Lemma 3.3

If A has no object of size 0 and $C = SET(A)$, then

$$C(x) = \sum_{k \geq 0} \frac{A(x)^k}{k!} = e^{A(x)}$$

Comment 3.1

We can have SET in the unlabelled case as well, but in that scenario, if $C = SET(A)$, then

$$C(x) = \exp\left(\sum_{k \geq 1} \frac{(-1)^{k-1}}{k} A(x^k)\right)$$

- **Labelled Cycle:** Let A be a labelled combanitorial class. For any positive integer k, the class $CYC_k(A)$ consists of the objects in A^k where two tuples are considered equal if they are equal up to a *cyclic shift*. We define
$$CYC(A) = CYC_1(A) + CYC_2(A) + \cdots$$

Lemma 3.4

If A has no object of size 0 and $C = CYC(A)$, then

$$C(x) = \sum_{k \geq 1} \frac{A(x)^k}{k} = \log\left(\frac{1}{1 - A(x)}\right)$$

3.1.1 Labelled Construction Examples

Question 3.1.

Why is $\exp\left(\log\left(\frac{1}{1-x}\right)\right) = \frac{1}{1-x}$?

Answer. As labelled classes, these are the generating functions for

$$SET(CYC(Z)) \qquad \text{and} \qquad SEQ(Z)$$

respectively. A permutation can be viewed as a set of disjoint cycles (for instance, (12)(3)), this is known as the cycle decomposition theorem from Pmath347. ☐

Lecture 22 - Wednesday, October 29

Example 3.5

In a planar rooted tree, the order of the children matter. A non-planar rooted labelled tree of size n is a rooted tree on n vertices whose vertices are labelled with $\{1, \ldots, n\}$ where the order of a vertex's children does not matter. If T is the labelled class of such trees, then

$$T = Z \times SET(T)$$

where Z represents the root, and $SET(T)$ represents the unordered set of trees. Therefore,

$$T(x) = xe^{T(x)} \implies x = \frac{T(x)}{G(T(x))} \quad \text{with} G(t) = e^t$$

By LIFT 1.3, the number of such trees is

$$n! \cdot [x^n]T(x) = \frac{n!}{n}[t^{n-1}]G(t)^n = (n-1)![t^{n-1}]e^{nt} = n^{n-1}$$

To get unrooted trees, we note that there are n ways to root an unrooted tree, so there are n^{n-2} unrooted non-planar labelled trees of size n.

3.1.2 Restricted Construction

Just like in the unlabelled case, we write

$$SEQ_{property} \qquad SET_{property} \qquad CYC_{property}$$

for restricted classes.

Example 3.6

We may write $SET_{\leq r}(A)$ to be the sets with at most r objects, so the generating function would be

$$\sum_{k=0}^{r} \frac{A(x)^k}{k!}$$

Similarly, $SET_{>r}(A)$ has the generating function

$$e^{A(x)} - \sum_{k=0}^{r} \frac{A(x)^k}{k!}$$

Exercise 3.1

Show taht if $C = SET_{even}(A)$, then

$$C(x) = \cosh(A(x))$$

recall that $\cosh(x) = (e^x + e^{-x})/2$.

Exercise 3.2

Show taht if $C = CYC_{even}(A)$, then

$$C(x) = -\frac{1}{2}\log\left(1 - A(x)^2\right)$$

Exercise 3.3

Show taht if $C = CYC_{odd}(A)$, then

$$C(x) = \log\sqrt{\frac{1 + A(x)}{1 - A(x)}}$$

3.1.3 Restricted Permutations

Definition 3.4: Fixed Point

A **fixed point** of a permutation is a cycle of length 1.

Definition 3.5: Derangement

A **derangement** is a permutation with no fixed point.

Question 3.2.

What is the EGF for the class of derangements?

Answer. If D is this class, then

$$D = SET(CYC_{\geq 2}(Z)) \implies D(x) = \exp\left[\log\left(\frac{1}{1-x}\right) - \frac{x}{1}\right]$$
$$= e^{-x} \cdot e^{\log\left(\frac{1}{1-x}\right)}$$

as desired. □

Comment 3.2

From now on, unless specified, we will use the usual rules of the exponential and logarithm, i.e., we have the following properties:

1. $e^{A \cdot B} = e^A \cdot e^B$;
2. $\log(AB) = \log(A) + \log(B)$;
3. $c \log(A) = \log(A^c)$ for some constant c;
4. log and exp are inverses of each other.

Note 3.2

Note that the probability that a permutation is a derangement is

$$\frac{\#\text{ of derangements of size } n}{\#\text{ of permutations of size } n}$$

Also note that in exp, there is already a $n!$ at the bottom of the corresponding coefficient, so the probability that a permutation of size n is a derangement is

$$\begin{aligned}[x^n]D(x) &= [x^n]\frac{e^{-x}}{1-x} \\ &= \sum_{k=0}^{n} \frac{(-1)^k}{k!}\end{aligned}$$

As $n \to \infty$, this probability approaches e^{-1}.

Question 3.3.

What if our permutations of cycles of length $> r$?

Answer. Our class A would be

$$A = SET(CYC_{>r}(Z))$$

Since $CYC_{>r}(Z) = \log\left(\frac{1}{1-x}\right) - \sum_{k=1}^{r} \frac{x^k}{k!}$. Hence

$$A(x) = \frac{\exp\left(-x - \frac{x^2}{2} - \cdots - \frac{x^r}{r!}\right)}{1-x}$$

We are able to show that as $n \to \infty$, the probability that you have all cycls of size at least $r+1$ approaches $e^{-1-1/2-\cdots-1/r}$. □

Question 3.4.

What if there are no cycles of length r?

Answer. We simply have $A = SET(CYC_{\neq r}(Z))$, and have

$$A(x) = \exp\left[\log\left(\frac{1}{1-x}\right)\frac{x^r}{r!}\right]$$

as desired. □

3.1.4 Set Partitions

Definition 3.6: Set Partition

A set partition of size n is a decomposition of $\{1, \ldots, n\}$ into disjoint union of non-empty sets called **blocks**.

Question 3.5.

What is the EGF for the class of set partitions?

Answer. Let C be this class, so

$$C = SET(\underbrace{SET_{\geq 1}(Z)}_{blocks}) \implies C(x) = e^{e^z - 1}$$

□

Lecture 23 - Friday, October 31

Exercise 3.4

Fix a positive integer r, how many set partitions of size n are there with r blocks.

Answer. If $S^{(r)}$ is the class of set partitions with r blocks, then

$$S^{(r)} = SET_{=r}(SET_{\geq 1}(Z)) \implies S^{(r)}(x) = \frac{(e^x - 1)^r}{r!}$$

If $\left\{ n \atop r \right\}$ is the number of set partitions with r blocks of size n, then

$$\begin{aligned} \left\{ n \atop r \right\} &= [x^n]\frac{(e^x-1)^r}{r!} \cdot n! \\ &= \frac{n!}{r!}[x^n]\sum_{j \geq 0}\binom{r}{j}(-1)^{r-j}e^{xj} \\ &= \frac{1}{r!}\sum_{j=0}^{r}\binom{r}{j}(-1)^{r-j} \cdot j^n \end{aligned}$$

which is known as the Stirling numbers of the second kind. □

3.2 Functional Graphs

A mapping of size n is a function $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$. There are n^n mappings of size n. We can interpret mappings with restriction using labelled enumeartion.

Comment 3.3

The key idea is to view a mapping as a directed graph on vertex set $[n]$ with an edge $x \to y$ if $f(x) = y$.

The class of functional graphs constructed by this process can be expressed in class of rooted trees.

Theorem 3.1: Map Enumeration Theorem

Let M be the class of mappings, let K be the class of connected functional graphs and T is the class of rooted labelled trees. Then

$$M = SET(K) \qquad \text{and} \qquad K = CYC(T)$$

Thus, we have

$$M(x) = \frac{1}{1 - T(x)}$$

where $T(x)$ satisfies $T(x) = x\exp(T(x))$.

Proof. The fact that $M = SET(K)$ follows from the definition of K and the fact that a general graph is a set of connected components.

Because a mapping has a unique output for every input, every node in a functional graph has outdegree 1. Thus, every connected functional graph has exactly one cycle.

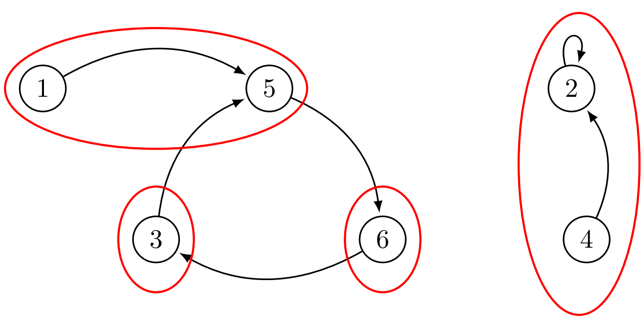
Coming into the cycle at any vertex is a (possibly empty) connected cycle-free graph, which is a tree. Thus, $K = CYC(T)$. The labelled trees are rooted as the vertices on the cycle are special, so they become the roots. See below for an example. □

Example 3.7

Suppose we have $f : [6] \to [6]$ defined as:

x	1	2	3	4	5	6
f(x)	5	2	5	2	6	3

which as a functional graph depicted below:



which is the same as:

$$\left\{\left[\text{①}\!-\!\text{⑤}\,,\ \text{③}\,,\ \text{⑥}\right],\left[\text{④}\!-\!\text{②}\right]\right\}$$

Example 3.8

An **idempotent** mapping f is a map such that $f(f(x)) = f(x)$ for all x. Find the EGF for the class I of idempotent mappings.

Answer. The class of functional graphs corresponding to idempotent mappings consist of connected components that are *stars*: a (potentially empty) set of single vertices pointed at a loop. If X is the class of star graphs, then $X = Z \times SET(Z)$, and $I = SET(X)$. Hence $I(x) = \exp(xe^x)$. □

Proposition 3.1

We have

$$\sum_{k\geq 0} \binom{n-1}{k-1} k!\, n^{-k} = 1$$

Proof. We will prove that there are $m_n = n^n \sum_{k\geq 0} \binom{n-1}{k-1} k!\, n^{-k}$ mappings of size n. Since $x = \dfrac{T(x)}{G(T(x))}$ where $G(u) = e^u$, by setting $F(u) = u^k$ in LIFT (1.3), we have

$$\begin{aligned}
[x^n]T(x)^k &= \frac{k}{n}[u^{n-k}]e^{un} \\
&= \frac{k}{n} \cdot \frac{n^{n-k}}{(n-k)!}
\end{aligned}$$

Thus, we have

$$\begin{aligned}
m_n = n! \cdot [x^n]M(x) = n! \cdot [x^n]\frac{1}{1-T(x)} \\
&= n! \cdot [x^n]\sum_{k\geq 0} T(x)^k \\
&= n! \cdot \sum_{k\geq 0} \frac{k}{n} \cdot \frac{n^{n-k}}{(n-k)!} = n^n \cdot \sum_{k\geq 0} n^{-k} \cdot n! \cdot \binom{n-1}{k-1}
\end{aligned}$$

as desired. □

Lecture 24 - Monday, November 03

3.3 Labelled Parameters

The (labelled) bivariate generating function of a labelled class C with respect to a parameter $p : C \to \mathbb{Z}$ is

$$C(u,x) = \sum_{\sigma \in C} u^{p(u)} \frac{x^{|\sigma|}}{|\sigma|!} = \sum_{n \geq 0} \left(\sum_{k \in \mathbb{Z}} c_{k,n} u^k \right) \frac{x^n}{n!}$$

where $c_{k,n}$ is the number of objects in C with size n and parameter value k.

Note 3.3

Some sources call this a **semi-exponent generating function**.

Again, we can often derive labelled EGSs using a parameterized neutral class/ marking class μ (size of 0 and parameter value of 1). We introduce μ into labelled specifications to mark changes in parameter.

Example 3.9

The labelled specification

$$P = SET(CYC(Z))$$

encodes the class of permutations as a set of disjoint cycles. Thus, the marked specification

$$P = SET(\mu \times CYC(Z))$$

keeps track of the number of cycles in the permutation. Hence, we have

$$P(u,x) = e^{u \log\left(\frac{1}{1-x}\right)} = (1-x)^{-u}$$

Similar to the unlabelled case, we have

$$\frac{d}{du} C(u,x)|_{u=1} = C_u(1,x) = \sum_{\substack{n \geq 0 \\ k \in \mathbb{Z}}} \frac{k \cdot c_{x,n}}{n!} x^n$$

Furthermore,

$$\frac{[x^n]C_u(1,x)}{[x^n]C(1,x)} = \frac{\sum_{k \in \mathbb{Z}} \frac{k \cdot C_{k,n}}{n!}}{C_n/n!} = \sum_{k \in \mathbb{Z}} k \cdot \frac{C_{k,n}}{C_n} = \mathbb{E}_n[p]$$

Comment 3.4

From now on, we assume the usual calculus rules for derivatives of exp/ log.

Example 3.10

Find the average number of cycles among the permutations of size n.

Answer. We saw that $P(u,x) = (1-x)^{-u} = e^{u\log\left(\frac{1}{1-x}\right)}$, so

$$P_u(u,x) = e^{u\log\left(\frac{1}{1-x}\right)} \cdot \log\left(\frac{1}{1-x}\right) \implies P_u(1,x) = \frac{1}{1-x}\log\left(\frac{1}{1-x}\right)$$

Since

$$\log\frac{1}{1-x} = \sum_{k\geq 1}\frac{x^k}{k} \implies [x^n]\frac{1}{1-x}\log\left(\frac{1}{1-x}\right) = \sum_{i=1}^{k}\frac{1}{i}$$

and $[x^n]C(1,x) = [x^n]\frac{1}{1-x} = 1$. We can now conclude that the average length of a cycle among the permutations of size n is

$$\boxed{\sum_{k=1}^{n}\frac{1}{k} = H_n} \approx \log n$$

as desired. □

Example 3.11

Let T be the class of non-planar rooted labelled trees, so

$$T = Z \times SET(T)$$

The Z in this specification corresponds to the root of the tree, so

$$R = Z \times SET(\mu \times T)$$

encodes the clabelled class R where size and root degree are tracked. Thus, $R(u,x) = xe^{uT(x)}$ where $T(x) = xe^{T(x)}$. Therefore,

$$\frac{d}{du}R(u,x)\bigg|_{u=1} = xT(x)e^{uT(x)}\bigg|_{u=1} = xT(x)e^{T(x)} = T(x)^2$$

The general form of LIFT implies

$$\begin{aligned}[x^n]R_u(1,x) &= [x^n]T(x)^2 \\ &= \frac{2}{n}[t^{n-2}]e^{nt} = \frac{2}{n}\cdot\frac{n^{n-2}}{(n-2)!}\end{aligned}$$

Since there are $[x^n]R(1,x) = [x^n]T(1,x) = \frac{n^{n-1}}{n!}$ trees, the average root degree among the trees in T of size n is $2(n-1)/n$ for $n \geq 1$.

Example 3.12

The n^{th} Bell number B_n is defined by the EGF

$$e^{e^x-1} = \sum \frac{B_n}{n!} x^n$$

Recall that the LHS is the EGF for the class of set partitions (see Section 3.1.4), so B_n counts the set partitions of size n. Thus,

$$B_n = \sum_{r=1}^{n} \left\{ \begin{matrix} n \\ r \end{matrix} \right\}$$

where $\left\{ \begin{smallmatrix} n \\ r \end{smallmatrix} \right\}$ is the Stirling number of the second kind (see exercise 3.4), which is the number of partitions of size n with r blocks.

Question 3.6.

What is the average number of blocks? We will find this in terms of B_n. See below.

If S is the class of set partitions, then

$$S = SET(SET_{\geq 1}(Z))$$

so marking blocks yields us $S = SET(\mu \times SET_{\geq 1}(Z))$. Thus,

$$S(u, x) = e^{u(e^x-1)}$$

$$\frac{d}{du} S(u,x)\Big|_{u=1} = e^{u(e^x-1)} \cdot (e^x - 1)\Big|_{u=1} = e^x \cdot e^{e^x-1} - e^{e^x-1}$$

Then $[x^n]S(1,x) = B_n/n!$ implies that

$$[x^n]e^x \cdot e^{e^x-1} = [x^n]\frac{d}{dx}S(1,x) = \frac{B_{n+1}}{n!}$$

So the average number of blocks is

$$\frac{[x^n]e^x e^{e^x-1} - [x^n]e^{e^x-1}}{[x^n]e^{e^x-1}} = \boxed{\frac{B_{n+1}}{B_n} - 1}$$

The **saddle point method** can be used to show that this $\approx \frac{n}{\log n}$ as n approaches ∞.

Lecture 25 - Wednesday, November 05

Midterm 2 Review today.

4 Asymptotics

Lecture 26 - Friday, November 07

Most of the times, exact counting is too hard to do, so a lot of the times we would instead compute the asymptotics of the objects. In other words, we approximate a complicated sequence by a "simpler" one.

Definition 4.1: Asymptotic

Let f_n, g_n be positive sequences (so $f_n > 0$, $g_n > 0$ for all n). We write $f_n \sim g_n$ if $\lim_{n\to\infty} \dfrac{f_n}{g_n} = 1$. We say that f_n is **asymptotic** to g_n.

Definition 4.2: Big-O

We write $f_n = O(g_n)$ if there exists $c > 0$ and $N \in \mathbb{N}$ such that

$$f_n \leq c \cdot g_n \qquad \forall n > N$$

Note 4.1

We write $f_n = g_n + O(h_n)$ if $f_n - g_n = O(h_n)$. What?

Comment 4.1

The reason why we used $=$ sign intead of treating $O(g_n)$ as a set is because we want to be able to use algebra on them afterwards.

Definition 4.3: Small-o

We write $f_n = o(g_n)$ if $\lim_{n\to\infty} \dfrac{f_n}{g_n} = 0$.

Note 4.2

These definitions only depend on the "eventual behaviour" of f_n and g_n, so these definitions make sense if f_n and g_n are eventually positive.

Lemma 4.1

Let f_n, g_n, a_n, b_n be eventually positive sequences, then

- If $f_n = O(g_n)$ and $a_n = O(b_n)$, then $f_n + a_n = O(g_n + b_n)$, and $f_n a_n = O(g_n b_n)$;
- If $f_n = o(g_n)$ and $a_n = o(b_n)$, then $f_n + a_n = o(g_n + b_n)$, and $f_n a_n = o(g_n b_n)$;

Proof. We will only prove the first bit of the lemma. We know that there exists $c_1, N_1, c_2, N_2 > 0$ such that

$$f_n \le c_1 \cdot g_n \qquad \forall n > N_1$$
$$a_n \le c_2 \cdot b_n \qquad \forall n > N_2$$

so we know that $f_n + a_n \le c_3 \cdot (g_n + b_n)$ for all $n > N_3$ where $c_3 = \max\{c_1, c_2\}$ and $N_3 = \max\{N_1, N_2\}$. ☐

Lemma 4.2

Let f_n, g_n, a_n, b_n be eventually positive sequences, then

1. $f_n = g_n(1 + o(1))$ (which is equivalent to saying $f_n = g_n + o(g_n)$) if and only if $f_n \sim g_n$.
2. If $f_n = a_n + b_n$, with $a_n \sim g_n$ and $b_n = o(g_n)$, then $f_n \sim g_n$.

Proof. For part 1, by definition, we have

$$\begin{aligned} f_n \sim g_n \quad &\iff \quad \frac{f_n}{g_n} \to 1 \text{ as } n \to \infty \\ &\iff \quad \frac{f_n}{g_n} = 1 + c_n \text{ for some sequence } c_n \to 0 \text{ as } n \to \infty \\ &\iff \quad \frac{f_n}{g_n} = 1 + o(1) \end{aligned}$$

For part 2, we have

$$\lim_{n\to\infty} \frac{f_n}{g_n} = \lim_{n\to\infty} \frac{a_n + b_n}{g_n} = 1 + 0$$

as desired. ☐

4.1 Asymptotic Hierarchy

Name	**General Member**	**Example**
constant	$f_n = A$ for $A > 0$	$f_n = 1$
log-power	$f_n = (\log n)^B$ for some $B > 0$	$f_n = \sqrt{\log n}$
power of n	$f_n = n^C$ for some $C > 0$	$f_n = n^{1/3}$
exponent	$f_n = D^n$ for some $D > 1$	$f_n = 2^n$
n^n power	$f_n = n^{En}$ for some $E > 0$	$f_n = n^{2n}$

Lemma 4.3

Any sequence in one row of this table is small-o of any sequence in the next row.

Proof. Basic limit laws and L'Hôpital's Rule. ☐

Name	General Member	Example
negative n^n power	$f_n = n^{en}$ for some $e < 0$	$f_n = n^{-2n}$
decreasing exponent	$f_n = d^n$ for some $0 < d < 1$	$f_n = (1/2)^n$
negative power of n	$f_n = n^c$ for some $C < 0$	$f_n = n^{-1/3}$
negative log-power	$f_n = (\log n)^b$ for some $b < 0$	$f_n = (\log n)^{-1/2}$
constant	$f_n = a$ for $a > 0$	$f_n = 1$

Corollary 4.1

We can still show that any sequence in one row of this table is small-o of any sequence in the next row.

4.2 Asymptotic Through Calculus

Taylor Series are very useful for asymptotics.

Example 4.1

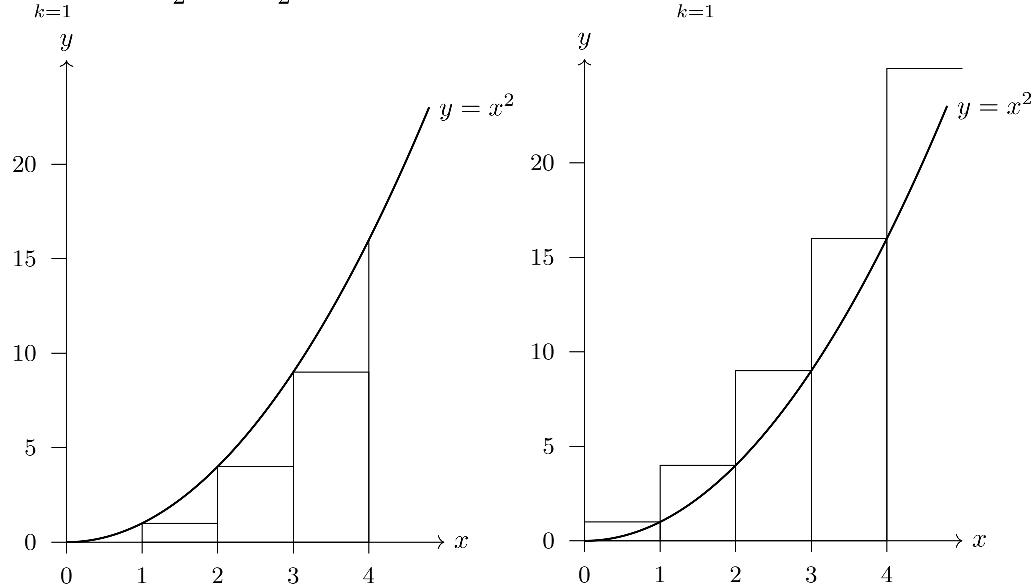
We know that $\dfrac{1}{1-x} = \sum_{k \geq 0} x^k$ for $|x| < 1$, so for $n > 1$,

$$\frac{1}{1-1/n} = \sum_{k \geq 0} \left(\frac{1}{n}\right)^k = 1 + \frac{1}{n} + \frac{1}{n^2} + \frac{1}{n^3} + O\left(\frac{1}{n^3}\right)$$

We can approximate series with integrals.

Example 4.2

The series $\sum_{k=1}^{n} k = \dfrac{n(n+1)}{2} \sim \dfrac{n^2}{2}$. What can we say about $S_n \coloneqq \sum_{k=1}^{n} k^2$?



We know that

$$\frac{n^3}{3} = \int_0^n x^2 \, dt \;\leq\; \sum_{k=1}^{n} k^2 \;\leq\; \int_0^{n+1} x^2 \, dt = \frac{n^3}{3} + o(n^3)$$

so we can conclude that $S_n = o(n^3)$.

Lecture 27 - Monday, November 10

Example 4.3

More generally, we can show that for any positive rational number r, we have

$$\sum_{k=1}^{n} k^r \sim \frac{n^{r+1}}{r+1}$$

Theorem 4.1

Let $a < b$ be integers and let $f(x)$ be a continuous function on $[a-1, b+1]$,

(a) If f is increasing on $[a-1, b+1]$, then

$$\int_{a-1}^{b} f(x) \, dx \;\leq\; \sum_{k=a}^{b} f(k) \;\leq\; \int_{a}^{b+1} f(x) \, dx$$

(b) If f is decreasing on $[a-1, b+1]$, then

$$\int_{a-1}^{b} f(x) \, dx \;\geq\; \sum_{k=a}^{b} f(k) \;\geq\; \int_{a}^{b+1} f(x) \, dx$$

Proof. The proof is left as an exercise, the intuition is shown in example 4.2 (i.e., we can always overapproximate and underapproximate to get a upper and lower bound). □

Corollary 4.2

Let $a < b$ be integers and $f(x)$ be a continuous function on $I \coloneqq [a-1, b+1]$. If f is either increasing on I or decreasing on I, and $|f(x)| \leq M$ on I, then

$$\left| \sum_{k=a}^{b} f(k) - \int_a^b f(x) \, dx \right| \;\leq\; M$$

Proof. The upper and lower bounds in our Theorem differ by the integral of $f(x)$ over an intervals of length 1. Since f is continuous, if J is an interval of length 1, then

$$\left| \int_J f(x) \, dx \right| \leq \text{length}(J) \cdot \max_{x^\star \in J} |f(x^\star)| \leq M$$

so we are done. □

Example 4.4

Let $\alpha > 0$. Since $f(x) = x^\alpha$ has $f'(x) = \alpha x^{\alpha-1} > 0$ for all $x > 0$ and f is increasing for $x > 0$, so our corollary implies that

$$\sum_{k=1}^{n} k^\alpha = \frac{n^{\alpha+1}}{\alpha+1} + O(n^\alpha)$$

since $|x^\alpha| \le (n+1)^\alpha$ on $[0, n+1]$.

Example 4.5

Recall that $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Let $f(x) = 1/x$. Since f is decreasing on $(0, \infty)$, we see that

$$H_n \ge \int_1^{n+1} \frac{dx}{x} = \log(n+1)$$

Because $f(x)$ is not defined at $x = 0$, we take out the first term and bound

$$H_n - 1 = \sum_{k=2}^{n} \frac{1}{k} \le \int_1^{n} \frac{dx}{x} = \log n$$

Thus

$$\log n \le \log(n+1) \le H_n \le \log n + 1$$

4.2.1 Quicksort

A sorting algorithm is an algorithm that takes a list of numbers and sorts them.

Comment 4.2

We assume that no number repeat for the sake of simplicity. This is equivalent to assuming that we have a permutation.

We care about how many comparisons the algorithm takes (on average among the parameter of size n).

Here is the Quicksort algorithm:

Input: A permutation π
Output: Sorted permutation
Pick a random element of π;
Go through π, move everything smaller to the left of the pivot and else to the right;
Recurse on the left and right sides of the pivot.

Algorithm 1: Quicksort

We will show that the average number of comparisons performed by Quicksort on a permutation of size n is $\le 2(n+1)\log(n+1) = O(n \log n)$.

Lecture 28 - Wednesday, November 12

In class Midterm again today.

Lecture 29 - Friday, November 14

Note 4.3

Easy to see that the worst case happens when we happen to always pick either the lowerest or the largest number in the permutation, which yields

$$(n-1)+(n-2)+\cdots+2+1=\frac{n(n-1)}{2}$$

comparisons in total. On the other hand, the best case is when we always pick the median, which gives us roughly $n\log_2 n$ comparisons.

Let c_n be the average number of comparisions quicksort does on elements in S_n. Then we have $c_0=c_1=0$ and for $n>1$,

$$\begin{aligned}
c_n &= \frac{1}{n}\sum_{k=1}^{n}\Big[(n-1)+c_{k-1}+c_{n-k}\Big] \\
&= (n-1)+\frac{1}{n}\left[\sum_{k=1}^{n}c_{k-1}+\sum_{k=1}^{n}c_{n-k}\right] \\
&= (n-1)+\frac{2}{n}\sum_{k=1}^{n}c_k \\
\implies \quad nc_n &= n(n-1)+2\sum_{k=1}^{n-1}c_k \\
\implies \quad (n-1)c_{n-1} &= (n-1)(n-2)+2\sum_{k=1}^{n-2}c_k
\end{aligned}$$

Subtracting the two equations, we obtain

$$nc_n=(n+1)c_{n-1}+2(n-1)$$

Thus, we have

$$\begin{aligned}
\frac{c_n}{n+1} &= \frac{c_{n-1}}{n}+\frac{2}{n+1}-\frac{2}{n(n+1)} \\
&\le \frac{c_{n-1}}{n}+\frac{2}{n+1} \\
&\le \frac{c_{n-2}}{n+1}+\frac{2}{n+1}+\frac{2}{n}=\frac{c_1}{2}+\sum_{k=2}^{n}\frac{2}{k+1}\le\sum_{k=2}^{n}\frac{2}{k+1}
\end{aligned}$$

Our asymptotic results imply that

$$\sum_{k=2}^{n}\frac{1}{k+1}\le\int_1^n\frac{dx}{1+x}=\log(n+1)-\log(2)$$

and so $c_n \le 2(n+1)\log(n+1) = O(n \log n)$.

Obtaining "tight" asymptotics: How to we get a tight asymptotic?

1. Start with
$$nc_n = (n+1)c_{n-2} + 2(n-1)$$
2. Multiply by x^n and sum over $n \ge 1$.
3. Derive the ODE
$$(1-x)^3 C'(x) - 2(1-x)^2 C(x) - 2x = 0$$
with $c(0) = 0$.
4. Solving the ODE to prove that
$$C(x) = \frac{-2\log(1-x)}{(1-x)^2} - \frac{2x}{(1-x)^2}$$
5. Prove that
$$[x^n]\frac{-\log(1-x)}{(1-x)^2} = (n+1)H_n - n$$
6. Conclude that $c_n = 2(n+1)H_n - 4n \sim 2n\log n \approx (1.39)n\log_2 n$.

Comment 4.3

This implies that on average, Quicksort is only $\approx 39\%$ worse than the best case.

4.3 Asymptotics of Rational GFs

4.3.1 C-Finite Sequences

Definition 4.4: C-Finite Sequence

A **C-finite sequence** (f_n) is a sequence that satisfies a linear recurrence of the form

$$f_n + c_1 f_{n-1} + \cdots + c_r f_{n-r} = 0 \qquad (*)$$

for all $n \ge N \ge r$ where each $c_1, \ldots, c_r \in \mathbb{Q}$.

We say r is the order of the recurrence. The sequence (f_n) is defined by (*) and its intial conditions $f_1, f_2, \ldots, f_N$.

Example 4.6: Fibonacci

For Fibonacci sequence, we have $f_0 = f_1 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for $n \ge 0$.

Theorem 4.2

(f_n) satisfies (*) if and only if $F(x) = \sum_{n\geq 0} f_n x^n$ satisfies $F(x) = \dfrac{G(x)}{H(x)}$ where

$$H(x) = 1 + c_1 x + \cdots + c_r x^r$$
$$G(x) = g_0 + g_1 x + \cdots + g_{N-1} x^{N-1}$$

where $g_k = f_k + c_1 f_{n-1} + \cdots + c_r f_{n-r}$ for $0 \leq k \leq N-1$.

Lecture 30 - Monday, November 17

Proof. Define $c_0 = 1$ and let $H(x) = c_0 + c_1 x + \cdots + c_r x^r$. Then

$$H(x)F(x) = \left(\sum_{k=0}^{r} c_k x^k\right)\left(\sum_{k\geq 0} f_k x^k\right) = \sum_{n\geq 0}\left(\sum_{k=0}^{r} c_k f_{n-k}\right) x^n$$

Thus, $[x^n]H(x)F(x)$ is a polynomial in x of degree $N-1$ if and only if (*) holds for all $n \geq N$. □

Example 4.7: Fibonacci

Let $f_0 = f_1 = 1$ and $f_n - f_{n-1} - f_{n-2} = 0$ for all $n \geq 2$, so

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

Example 4.8: Conway Look-and-Say Sequence

The sequence (https://oeis.org/A005150) is given by

$$(\ell_n) = 1, 11, 21, 1211, 111221, \ldots$$

Let d_n be the number of digits in ℓ_n, whose first few terms are

$$d_n = 1, 2, 2, 4, 6, \ldots$$

Conway proved that (d_n) is C-finite, and

$$D(x) = \frac{G(x)}{H(x)} = \frac{1 + x + \cdots + 18x^{77} - 12x^{78}}{1 - x + \cdots - 9x^{71} + 6x^{72}}$$

Lemma 4.4

If (f_n) and (g_n) are C-finite, then $(f_n + g_n)$ and $(\sum_{k=0}^{n} f_k g_{n-k})$ are also C-finite.

Fact: If $P(x) \in \mathbb{Q}[x]$ of degree d, then it has d roots in $\mathbb{C}$. We can always write

$$P(x) = c(x-\lambda_1)^{d_1}(x-\lambda_2)^{d_2}\cdots(x-\lambda_s)^{d_s}$$

for positive integers $d_1, \ldots, d_s$ and distinct roots $\lambda_1, \ldots, \lambda_s$. We call d_s the **multiplicity** of root $x = \lambda_i$. A root of multiplicity 1 is a **simple root**.

Lemma 4.5

The multiplicity of the root λ_i is the smallest positive integer k such that

$$p(\lambda_i) = p'(\lambda_i) = \cdots = p^{(k-1)}(\lambda_i) = 0$$

and $p^{(k)}(\lambda_i) \neq 0$.

Proof. Product rule. □

Fact (Partial Fraction Decomposition): Suppose $F(x) = G(x)/H(x)$ where $\deg(G) = \deg(H)$, and $H(x) = C(x-\lambda_1)^{d_1}\cdots(x-\lambda_s)^{d_s}$ with the λ_is are distinct and non-zero. Then there exists $c_i^{(j)} \in \mathbb{C}$ such that

$$F(x) = \sum_{i=1}^{s}\sum_{j=1}^{d_i} \frac{c_i^{(j)}}{(1-x/\lambda_i)^j}$$

4.3.2 C-Finite Coefficient Theorem

Theorem 4.3: C-Finite Coefficient Theorem

Suppose (f_n) is a C-finite sequence with rational generating function

$$F(x) = R(x) + \frac{G(x)}{H(x)}, \qquad \deg(G) < \deg(H) \text{ and } H(0) = 1$$

If $\lambda_1, \ldots, \lambda_s$ form the distinct roots of H with multiplicities $d_1, \ldots, d_s$, then

$$f_n = P_1(n)\cdot\lambda_1^{-n} + \cdots + P_s(n)\cdot\lambda_s^{-n} \qquad \forall n > \deg(R)$$

where $P_j(n)$ are polynomials in n of degree at most $d_j - 1$.

Proof. Let $n > \deg(R)$, so $f_n = [x^n]F(x) = [x^n]G(x)/H(x)$. A partial fraction decomposition implies that

$$\frac{G(x)}{H(x)} = \Lambda_1(x) + \cdots + \Lambda_s(x)$$

where $\Lambda_i(x) = \frac{c_i^{(1)}}{1-x/\lambda_i} + \cdots + \frac{c_i^{(d_i)}}{(1-x/\lambda_i)^{d_i}}$ for constants c_i^j. Since $\lambda_i \neq 0$, the Negative Binomial Theorem implies

$$[x^n](1-x/\lambda_i)^{-m} = \lambda^{-n}\binom{m+n-1}{m-1} = \lambda^{-n}\cdot(\text{polynomial in } n \text{ of degree } m-1)$$

Thus, $[x^n]\Lambda_i(x) = P_i(n) \cdot \lambda_i^{-n}$ for a polynomial $P_i(n)$ of degree at most $d_i - 1$. $\square$

Lecture 31 - Wednesday, November 19

Corollary 4.3

If (f_n) satisfies $f_n + c_1 f_{n-1} + \cdots + c_r f_{n-r} = 0$ for all $n \geq r$, then $f_n = P_1(n)\lambda_1^{-n} + \cdots + P_s(n)\lambda_s^{-n}$ where the λ_is are the roots of the characteristic polynomial $H(x) = 1 + c_1 x + \cdots + c_r x^r$ and $P_i(n)$ is a polynomial of degree at most 1 less than the multiplicity of λ_i.

Example 4.9

Find a closed form for the sequence (f_n) that satisfies

$$f_{n+3} = 3f_{n+1} - 2f_n \qquad \forall n \geq 0$$

and $f_0 = f_1 = 4$ and $f_2 = 13$.

Answer. Since the characteristic polynomial $H(x) = 1 - 3x^2 + 2x^3$ has the factorization $H(x) = (1-x)^2(1+2x)$, the C-finite coefficient theorem (4.3) implies that there exists $A, B, C \in \mathbb{C}$ such that

$$f_n = (An + B) \cdot 1^{-n} + C \cdot \left(-\frac{1}{2}\right)^{-n}$$

Substituting $n = 0, 1$, and 2 gives

$$\begin{aligned}
(n=0) \quad & 4 = f_0 && = B + C \\
(n=1) \quad & 4 = f_1 && = A + B - 2C \\
(n=2) \quad & 13 = f_2 && = 2A + B + C
\end{aligned}$$

Solving the system of equations gives us $(A, B, C) = (3, 3, 1)$ and so $f_n = 3(n+1) + (-2)^n$. $\square$

4.4 Asymptotics of C-Finite Sequences

Can we find a "simple" g_n such that $f_n \sim g_n$ where f_n is C-finite? Not all terms in the C-finite coefficient theorem 4.3 contribute to dominant asymptotics.

Lemma 4.6

Assume the hypothesis of the C-finite coefficient theorem. If λ_k is a simple root of H and $G(\lambda_k) \neq 0$, then the polynomial $P_k(n)$ is

$$P_k(n) = \frac{-G(\lambda_k)}{\lambda_k H'(\lambda_k)}$$

Proof. Since λ_k is a simple root, we can write $H(x) = (x - \lambda_k) \cdot I(x)$, where $I(\lambda_k) \neq 0$. Thus,

$$H'(x) = I(x) + (x - \lambda_k) \cdot I'(x) \quad \Longrightarrow \quad H'(\lambda_k) = I(\lambda_k)$$

Partial fractions implies that we can write

$$\frac{G(x)}{H(x)} = \frac{G(x)}{(x-\lambda_k)I(x)} = \frac{C}{x-\lambda_k} + \frac{J(x)}{I(x)}$$

for some constant C and polynomial $J(x)$. Clearing the denominators gives

$$G(x) = C \cdot I(x) + (x-\lambda_k) \cdot J(x)$$

Setting $x = \lambda_k$ yields us $G(\lambda_k) = C \cdot I(\lambda_k)$, and thus $C = \dfrac{G(\lambda_k)}{I(\lambda_k)} = \dfrac{G(\lambda_k)}{H'(\lambda_k)}$. Then, using the polynomial $\Lambda_k(x)$ from the proof of the C-finite coefficient theorem 4.3,

$$[x^n]\Lambda_k(x) = [x^n]\frac{C}{x-\lambda_k} = \frac{C}{-\lambda_k}[x^n]\frac{1}{1-x/\lambda_k} = \frac{C}{-\lambda_k} \cdot (\lambda_k)^{-n} = \frac{-G(\lambda_k)}{\lambda_k H'(\lambda_k)} \cdot (\lambda_k)^{-n}$$

as desired. □

Lemma 4.7

Assume the hypothesis of the C-finite coefficient theorem. If λ_k is a root with multiplicity m of $H(x)$ and $G(\lambda_k) \neq 0$, then the polynomial $P_k(n)$ satisfies

$$P_k(n) = \frac{m(-1)^m G(\lambda_k)}{\lambda_k^m H^{(m)}(\lambda_k)} n^{m-1} + O(n^{m-2})$$

Proof. Suppose $H(x) = (x-\lambda)^m I(x)$ and thus $H^{(m)}(\lambda_k) = m! I(\lambda_k) \neq 0$. PFD gives us

$$F(x) = \frac{C}{(x-\lambda_k)^m} + \frac{J(x)}{I(x)(x-\lambda_k)^{m-1}}$$

and thus

$$C = \frac{G(\lambda_k)}{I(\lambda_k)} = \frac{m! \cdot G(\lambda_k)}{H^{(m)}(\lambda_k)}$$

Then we use Negative Binomial theorem on $\dfrac{C}{(x-\lambda_k)^m}$ □

Corollary 4.4

Assume the hypothesis of the C-finite coefficient theorem and that G and H are coprime. If $|\lambda_1| < |\lambda_k|$ for all $k = 2, \dots, s$, then

$$f_n = P_1(n) \cdot \lambda_1^{-n} + \underbrace{O(w^{-n} n^{\alpha-1})}_{\text{exponentially smaller error}}$$

where $w = \min_{2 \le k \le s} |\lambda_k| > |\lambda_1|$ and α is the largest multiplicity of a root of H with modulus w.

Corollary 4.5

Assume the hypothesis of the C-finite coefficient theorem and G and H are coprime. If $|\lambda_1| \leq |\lambda_k|$ for all $k = 2, \ldots, s$ and λ_1 has a strictly higher multiplicity than any other root with its modulus, then

$$f_n = \frac{m(-1)^m G(\lambda_1)}{\lambda_1^m H^{(m)}(\lambda_1)} \cdot n^{m-1} \cdot \lambda_1^{-n} + \underbrace{O(|\lambda_1|^{-n} n^{m-\alpha})}_{\text{polynomially smaller error}}$$

Example 4.10

If (f_n) = the number of integer partitions of n with parts of size ≤ 3, then

$$F(x) = \sum_{n \geq 0} f_n x^n = \frac{1}{(1-x)(1-x^2)(1-x^3)}$$

Since $H(x) \coloneqq (1-x)(1-x^2)(1-x^3) = (1-x)^3(1+x)(1+x+x^2)$, we see that H has a root $x = 1$ with multiplicity 3 and all other roots have modulus 1 but multiplicity less than 3. Then $H^{(3)}(1) = -36$, so

$$f_n = \frac{-3}{-36} \cdot n^2 + O(n) \sim \frac{n^2}{12}$$

Lecture 32 - Friday, November 21

Result 4.1

Here we summarize how we find asymptotics:

1. Find the roots for H that is the "closest to origin" (λ_i with minimim $|\lambda_i|$);
2. Among the roots with minimum modulus, find those with highest multiplicity.

4.4.1 Vivanti-Pringsheim Theorem

Theorem 4.4: Vivanti-Pringsheim Theorem

Suppose $F(x) = \frac{G(x)}{H(x)} = \sum_{n \geq 0} f_n x^n$ for G and H coprime polynomials. If

1. only a finite number of terms in (f_n) are negative; or
2. $f_n \geq 0 \ \ \forall n$

then one of the roots of H with minimal modulus is positive and real.

Proof Idea. If p is a root of H of minimal modulus, then

$$\lim_{x \to p^-} |F(x)| = \infty$$

Note that $|F(x)| = |\sum_{n \geq 0} f_n x^n| \leq \sum_{n \geq 0} f_n |x|^n = F(|x|)$. $\square$

Example 4.11: Look and Say Digit Sequence

Recall the look and say sequence (d_n), Conway proved that (d_n) is C-finite, and

$$D(x) = \frac{G(x)}{H(x)} = \frac{1 + x + \cdots + 18x^{77} - 12x^{78}}{1 - x + \cdots - 9x^{71} + 6x^{72}}$$

We know that there exists a positive root $p \geq 0$ of H with monimal modulus. We can even check that $p$is a simple root (no other roots of modulus p). Therefore, we can obtain that

$$d_n \sim \frac{-G(p)}{pH'(p)} \cdot p^{-n} \approx (2.04) \cdot (1.303)^n$$

4.4.2 Skolem's Problem

Consider the following problem:

$$[x^n]\left(\frac{1}{1-4x^2} + \frac{1}{1-x/2}\right) = \begin{cases} 2^n + 2^{-n} & 2 \mid n \\ 2^{-n} & 2 \nmid n \end{cases}$$

This goes to ∞ if $n \to \infty$ and n is even, and goes to 0 if $n \to \infty$ and n is odd. Here is the statement of the Skolem's Problem:

> `[Skolem's Problem]`: Is there any algorithm that takes a rational function with integer coefficient and decides if its Taylor expansion has a coefficient equal to 0. Equivalently speaking, it asks whether you can detect if a C-finite sequence has a 0 term.

Note 4.4

We note that if (f_n) is C-finite, then (f_n^2) is C-finite.

Open Problem (Positivity): Can we decide if coefficients are all positive?

Open Problem (Eventual Positivity): Can we decide if evantually all coefficients are positive?

Definition 4.5: ℕ-Rational Functions

ℕ-rational functions is a set of functions you get from operations listed below:

$$1, \quad z, \quad +, \quad \times, \quad f \mapsto \frac{1}{1-zf}$$

Equivalently, they are generating functions defined by $+$, $\times$, SEQ (with only atoms and neutrals – no recursions).

Comment 4.4

ℕ-rational functions are generating functions of regular languages, which is the same as the languages "recognized by finite automata".

Theorem 4.5: Berstel

If $F(x) = \frac{G(x)}{H(x)}$ is $\mathbb{N}$-rational and λ is a root of H with $|\lambda|$ minimal, then there exists a positive integer r such that $\lambda^r = |\lambda|^r$. In other words, all minimal modulus roots differ by "roots of unity".

Note 4.5

The above theorem implies that $\mathbb{N}$-rational functions have "periodic behaviour" in their series coefficients.

Theorem 4.6: Meta Theorem

All rational functions (with coefficients in $\mathbb{N}$) appearing in combinatorial problems are $\mathbb{N}$-rational.

4.4.3 Classify C-finite Sequences/ Rational Generating Functions

Example 4.12

Prove that $c_n = \dfrac{1}{n+1}\dbinom{2n}{n}$ is not C-finite.

Answer. The generating function $c(x) = \frac{1-\sqrt{1-4x}}{2x}$ is not rational. □

Example 4.13

Prove that $F(x) = \sum_{n\geq 1} \frac{x^n}{n^5}$ is irrational.

Note 4.6

We note that $F(1) = \sum_{n\geq 1} \frac{1}{n^5} = \zeta(5)$. The question about the rationality of $\zeta(5)$ is open for 250 years.

Answer. $f_n = n^{-5}$ is not C-finite. □

Example 4.14

Let $p_n = n^{th}$ prime number, then $p_n = n\log n + n\log n \log\log n + O(n)$. The $\log n$ term means that this sequence is not C-finite.

Lecture 33 - Monday, November 24

4.5 Analytic Combinatorics

In our study of C-finite sequences, we saw how properties of their rational generating functions as complex-valued functions (locations and multiplicities of the denominator roots) translated directly into asymptotic information. Using more advanced techniques from complex analysis, these observations can be greatly generalized.

4.5.1 Radius of Convergence and Exponential Growth

Let

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

be a power series, which we now consider *as a function* from the complex numbers to the complex numbers, for all values of z where the series converges. In order to characterize the values of z where $F(z)$ converges, we must first introduce some notation.

Definition 4.6: Subsequence

A subsequence of (f_n) is any sequence (f_{k_n}) with

$$0 \leq k_1 < k_2 < k_3 < \cdots$$

(informally, a subsequence is obtained by selecting some terms of (f_n) when running through the sequence). For instance, (f_n) is a subsequence of itself – other subsequences include the terms f_{2n} with even indices, and the terms with prime indices.

Definition 4.7: Limit Superior

The **limit superior** $\limsup_{n\to\infty} x_n$ of any sequence (x_n) with positive real terms is the supremum of all limits of all subsequences of (x_n).

Note 4.7

Unlike limits, which may not exist because sequences can oscillate between different values, limit superiors always exist (although they may equal infinity).

Example 4.15

If $f_n = 1$ when n is even and $f_n = 2 - 2^{-n}$ when n is odd, then the subsequences of f_n that converge have limits equal to 1 or 2, so the limit superior of f_n is 2.

The following result is usually presented in a first analysis course.

Theorem 4.7: Root Test

Let

$$\rho = \limsup_{n\to\infty} |a_n|^{1/n}$$

and define

$$R = \begin{cases} \dfrac{1}{\rho} & \text{if } 0 < \rho < \infty, \\ \infty & \text{if } \rho = 0, \\ 0 & \text{if } \rho = \infty. \end{cases}$$

Then $F(z)$ converges whenever $|z| < R$ and diverges if $|z| > R$.

Definition 4.8: Radius of Convergence

We call the value R computed with the root test the **radius of convergence** of $F(z)$.

Comment 4.5

The root test is closely related to the *ratio test*, which is commonly seen in a first calculus course.

Theorem 4.8: Ratio Test

If

$$\lim_{n\to\infty} \left| \frac{f_{n+1}}{f_n} \right|$$

exists then it equals the value ρ computed in the root test.

Example 4.16

- Since $\lim_{n\to\infty} (2^n)^{1/n} = 2$, the radius of convergence of

  $$\frac{1}{1-2z} = \sum_{n\geq 0} 2^n z^n$$

  is $1/2$.

- Since $\lim_{n\to\infty} \dfrac{(n+1)!}{n!} = \infty$, the radius of convergence of

  $$\sum_{n\geq 0} n!\, z^n$$

  is 0.

- Since $\lim_{n\to\infty} \frac{1/(n+1)}{1/n} = 1$, the radius of convergence of

$$-\log(1-z) = \sum_{n\geq 0} \frac{z^n}{n}$$

is 1.

- Since $\lim_{n\to\infty} \frac{1/(n+1)!}{1/n!} = 0$, the radius of convergence of

$$e^z = \sum_{n\geq 0} \frac{z^n}{n!}$$

is infinity.

We now restrict to the case of a series $F(z)$ with finite positive radius of convergence $R = 1/\rho$. In this case we can write

$$f_n = \rho^n \cdot \theta(n) + O(\alpha^n)$$

for some function θ that grows slower than any exponential function and $0 < \alpha < \rho$.

Definition 4.9: Exponential Growth and Subexponential Growth

We call $\rho(n)$ the exponential growth of (f_n) and $\theta(n)$ the subexponential growth of (f_n). Under our conditions, the exponential growth forms the most impactful part of the asymptotic behaviour of f_n.

4.5.2 Singularities

We have now linked the exponential growth of the sequence (f_n) to the radius of convergence of its generating function $F(z)$. In the examples above it was possible to determine the radius of convergence directly from a closed expression for (f_n), but what if such an expression is not known?

The key to analytic combinatorics is that the radius of convergence (and much more) can be deduced directly from the properties of $F(z)$ as a complex-valued function. In fact, we have already seen this in a special case.

Example 4.17

If

$$F(z) = \frac{G(z)}{H(z)}$$

is a rational function defined by the ratio of coprime polynomials G and H then the C-finite Coefficient Theorem implies that the exponential growth of (f_n) is the minimum value of $|w|^{-1}$ as w ranges over the roots of the denominator H.

Generalizing beyond the rational case requires defining the *singularities* of a complex function. Roughly, singularities are points where “something goes wrong” in a function, such as division by zero, putting zero into a root, or putting zero into a logarithm. A rigorous discussion of singularities requires discussing analytic continuation of complex functions, which we do not get into here.

Example 4.18

- The only singularity of $F(z) = 1/(1-2z)$ is $z = 1/2$.
- The singularities of $F(z) = 1/(1+z^2)$ are $z = i$ and $z = -i$.
- The EGF of permutations with no fixed points is

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

  which has its only singularity at $z = 1$.
- The Catalan generating function

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

  has a singularity at $z = 1/4$ (where there is a zero inside the square-root). Note that $z = 0$ might appear to be a singularity due to a division by zero, but the fact that the numerator of C also vanishes at $z = 0$ implies that this "apparent singularity" can be "removed".

Theorem 4.9: Cauchy

If $F(z) = \sum_{n\geq 0} f_n z^n$ has a finite positive radius of convergence R then R equals the minimum modulus of the singularities of F over the complex numbers.

Because we deal with generating functions, which have non-negative coefficients, we can be more specific about where to find singularities.

Theorem 4.10: Vivanti-Pringsheim Theorem

If $F(z) = \sum_{n\geq 0} f_n z^n$ and $f_n \geq 0$ for all n then the radius of convergence R of (f_n) is a minimal modulus singularity of $F(z)$.

Comment 4.6

Thus, the exponential growth of (f_n) can be deduced immediately from the first positive real singularity of $F(z)$.

Example 4.19

- If $F(z) = 1/(1-2z)$ then f_n has exponential growth 2^n.
- If $F(z) = e^{-z}/(1-z)$ then f_n has exponential growth $1^n = 1$.
- If $F(z) = \dfrac{1-\sqrt{1-4z}}{2z}$ then f_n has exponential growth 4^n. In fact, using our closed formula for the nth Catalan number and Stirling's approximation, it is possible to show that

  $$f_n \sim \frac{4^n}{\sqrt{n^3\pi}}$$

- Recall that the EGF of surjections is $F(z) = 1/(2 - e^z)$. Since $z = \log 2$ is the first (and only) positive real singularity of F, the exponential growth of f_n is

$$(\log 2)^{-n} = (1.442\ldots)^n$$

Note that F has an infinite number of singularities $\{\log 2 + k(2\pi i) : k \in \mathbb{Z}\}$ in the complex plane.

Definition 4.10: Dominant Singularity

The singularities of F closest to the origin are called its **dominant singularities**, as they are the ones that dictate the dominant asymptotic behaviour of its coefficient sequence.

4.5.3 Meromorphic Asymptotics

Definition 4.11: Analytic

We say that a complex function $F(z)$ is *analytic* at a point $z = a$ if its Taylor series

$$F(z) = \sum_{n \geq 0} \frac{F^{(n)}(a)}{n!}(z - a)^n$$

around $z = a$ exists and has a positive radius of convergence.

Comment 4.7

A singularity of F is roughly a point where F is not analytic, however as mentioned above a fully rigorous definition of singularities also requires the notion of analytic continuation.

Example 4.20

The functions e^z, $\sin(z)$, and $\cos(z)$, and all polynomials, are analytic in the entire complex plane.

Example 4.21

If $p(z)$ is analytic at $z = a$ and $p(a) \neq 0$ then $\sqrt{p(z)}$, $1/p(z)$, and $\log p(z)$ are analytic at $z = a$.

Example 4.22

If $f(z)$ and $g(z)$ are analytic at $z = a$ then $f(z)g(z)$ and $f(z) + g(z)$ are analytic at $z = a$.

A ratio of analytic functions behaves "like" a rational function near each of its singularities, which means that they have similar asymptotic behaviour. The following result follows from the Cauchy Residue Theorem in complex analysis.

Theorem 4.11: Meromorphic Asymptotic Theorem

Suppose that $F(z) = G(z)/H(z)$ is the ratio of complex functions G and H that are analytic in $|z| \leq B$ for some $B > 0$. If

- $H(z)$ has a single zero $z = w$ with $|z| < B$ and no zeroes with $|z| = B$, and
- both $H'(w) \neq 0$ and $G(w) \neq 0$,

then

$$[z^n]F(z) \;=\; w^{-n}\,\frac{-G(w)}{wH'(w)} \;+\; O(B^{-n})$$

Note 4.8

- When F is a rational function then this result matches the C-finite Asymptotic Theorem (where the denominator has a unique root of minimal modulus, with multiplicity one).
- It is possible to define the multiplicity of a zero of an analytic function using derivatives, and generalize the Meromorphic Asymptotic Theorem beyond simple zeroes.
- If H has a finite set of zeroes with $|z| < B$ and no zeroes with $|z| = B$ then asymptotics are obtained by adding up contributions from the zeroes with $|z| < B$.

Example 4.23

Find asymptotics for the number s_n of surjections of size n.

Answer. As recalled above the EGF for surjections is $F(z) = 1/(2-e^z)$. Both of the functions $G(z) = 1$ and $H(z) = 2 - e^z$ are analytic everywhere in the complex plane, and when $|z| \leq 1$ the only root of $H(z)$ is $z = \log 2$. Since $G(\log 2) = 1$ and $H'(\log 2) = -2^{\log 2} = -\log 2$ are non-zero, the Meromorphic Asymptotic Theorem implies

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

so that

$$s_n \sim \frac{n!}{2(\log 2)^{n+1}}.$$

□

Example 4.24

The labelled class $\mathcal{A}$ of *alignments* has the labelled specification $\mathcal{A} = \text{SEQ}(\text{CYC}(\mathcal{Z}))$. Find asymptotics for the number of alignments of size n.

Answer. This specification implies

$$A(z) = \frac{1}{1 + \log(1-z)},$$

which has singularities when $z = 1$ (0 in a logarithm) and $\log(1-z) = -1$ (divide by zero). The equation $\log(1-z) = -1$ has solution $z = 1 - e^{-1} = 0.632\ldots$ which is the only dominant singularity of $A(z)$. Applying the Meromorphic Asymptotic Theorem then gives

$$a_n = n![z^n]A(z) \sim \frac{n!}{e(1-e^{-1})^{n+1}}.$$

□

Exercise 4.1

Recall that the exponential generating function of alternating permutations is $T(z) = \tan(z)$. Use the Meromorphic Asymptotic Theorem to find asymptotics for the number of alternating permutations.

4.5.4 The Principles of Analytic Combinatorics

The two basic principles of analytic combinatorics are

> **First Principle of Analytic Combinatorics**: The locations of the singularities of a generating function determine the exponential growth of its coefficient sequence.
>
> **Second Principle of Analytic Combinatorics**: The type of the singularities of a generating function determine the sub-exponential growth of its coefficient sequence.

Note 4.9

The *type* of a singularity includes dividing by zero (and with what multiplicity), putting zero in a root, zero in a logarithm, etc.

Like the C-finite Coefficient Theorem, and Meromorphic Asymptotic Theorem, one "transfers" singular behaviour of $F(z)$ near its dominant singularities to dominant asymptotic behaviour.

4.6 Random Generation

Definition 4.12: Uniform Generation algorithm

A uniform generation algorithm for a combinatorial class C is a randomized algorithm that takes $n \in \mathbb{N}$ and returns an element in C of size n, where every element of C_n is returned with probability $1/c_n$.

Comment 4.8

We assume that we have access to a function `rand()` that returns a random real number in $[0, 1)$

We can use `rand` to generate a random integer in $\{0, \ldots, n\}$ by defining

$$\texttt{rand}(0\ldots n) = \lfloor (n+1) \cdot \texttt{rand}() \rfloor$$

Our goal is to generate random algorithms that are correct, efficient, *and* easy to understand. Below we discuss random generation using

- Direct algorithms
- Bijections
- Recursive sampling
- Boltzmann sampling (which is no longer uniform random generation)

4.6.1 Direct Algorithms

If the class is simple enough, we can directly implement a random generation algorithm.

Example 4.25

Find a uniform generation algorithm to compute a random binary string of length n. We directly generate binary digits one by one. In Sage code,

```
def rbin(n):
    # Every string appears with probability 1/2^n
    return [floor(2*RR.random_element(0,1)) for k in [1..n]]
```

where `RR.random_element(0,1)` returns a random real number in $(0, 1)$. For instance, running `rbin(10)` returns (on the run saved in the Sage notebook corresponding to this chapter) `[0, 1, 0, 1, 1, 0, 1, 0, 0, 0]`.

4.6.2 Bijections

If we can randomly generate objects in a class A, and know a bijection from A to another class B, then we can randomly generate objects in the class B using the bijection.

4.6.3 Random Sampling

How can we use combinatorial specifications to randomly generate elements?

As usual, we start with our base cases. In pseudocode,

```
def genε(n):
    if n = 0 return ε
    else return NULL

def genZ(n):
    if n = 1 return Z
    else return NULL
```

Combinatorial Sum Suppose $\mathcal{A} = \mathcal{B} + \mathcal{C}$ and we have uniform generation algorithms `genB(n)` and `genC(n)`. How do we build `genA(n)`? If $\alpha \in \mathcal{A}_n$ then

$$\mathbb{P}[\alpha \in \mathcal{B}_n] = \frac{b_n}{a_n} = \frac{b_n}{b_n + c_n}$$

so we define

```
def genBplusC(n):
    x = RR.random_element(0,1)
    if x < b(n)/(b(n) + c(n)) return genB(n)
    else return genC(n)
```

If $\alpha \in \mathcal{B}$ then it is returned with probability

$$\frac{b_n}{b_n + c_n} \cdot \frac{1}{b_n} = \frac{1}{b_n + c_n} = \frac{1}{a_n}$$

and a similar argument works when $\alpha \in \mathcal{C}$, so we have a uniform random generation algorithm.

Combinatorial Product Suppose $\mathcal{A} = \mathcal{B} \times \mathcal{C}$ and we have uniform generation algorithms `genB(n)` and `genC(n)`. How do we build `genA(n)`?

The probability that $\alpha \in \mathcal{A}_n$ is $\alpha = (\beta, \gamma)$ and $|\beta| = k$ is

$$\frac{b_k c_{n-k}}{a_n}$$

Thus, we first randomly generate the size that β should have, then generate objects of the appropriate size from $\mathcal{B}$ and $\mathcal{C}$.

```
def genBtimesC(n):
    x    = RR.random(0,1)
    k    = 0
    a(n) = sum(b(k)*c(n-k), k=0..n)
    s    = b(0)*c(n)/a(n)
    while x > s:
        k = k + 1
        s = s + b(k)*c(n-k)/a(n)
    return [genB(k), genC(n-k)]
```

The probability that $(\beta, \gamma) \in \mathcal{B}_k \times \mathcal{C}_{n-k}$ is returned is

$$\frac{b_k \cdot c_{n-k}}{a_n} \cdot \frac{1}{b_k} \cdot \frac{1}{c_{n-k}} = \frac{1}{a_n}$$

so we have a uniform random generation algorithm.

Sequence If $\mathcal{B}$ has no objects of size 0 then $\mathcal{A} = \text{SEQ}(\mathcal{B})$ is equivalent to

$$\mathcal{A} = \varepsilon + \mathcal{B} \times \mathcal{A}$$

so the sequence construction can be captured by sum and product using a *recursive* algorithm.

4.6.4 Boltzmann Sampling

Recursive sampling is powerful, but can be slow for complicated objects. Instead of saying we need an object of size n, we can look for an object of size (say) $[0.9n, 1.1n]$ and (in general) do better. The elegant framework for handling this is **Boltzmann sampling**.

Note 4.10

If $F(z) = \sum f_n z^n$ has radius of convergence R, then $F(p)$ converges to a complex number for $|p| < R$. We call the points $v \in (0, R)$ the *admissible values* of F.

Let $\mathcal{A}$ be a combinatorial class and v an admissible value for $A(x)$. A **Boltzmann model** at v assigns each $\alpha \in \mathcal{A}$ the probability

$$\mathbb{P}_v(\alpha) = \frac{v^{|\alpha|}}{A(v)}.$$

Note that

$$\sum_{\alpha \in \mathcal{A}} \mathbb{P}_v(\alpha) = \sum_{\alpha \in \mathcal{A}} \frac{v^{|\alpha|}}{A(v)} = \frac{A(v)}{A(v)} = 1.$$

and $\mathbb{P}_v(\alpha)$ depends only on $|\alpha|$. A **Boltzmann generation algorithm** with parameter v is a randomized algorithm that returns $\alpha \in \mathcal{A}$ with probability $\mathbb{P}_v(\alpha)$.

The value v is a parameter: we can "tune" it to get objects of roughly the size we want. The expected size of the Boltzmann algorithm with parameter v is

$$\sum_{\alpha \in \mathcal{A}} |\alpha| \mathbb{P}_v(\alpha) = \sum_{\alpha \in \mathcal{A}} \frac{|\alpha| v^{|\alpha|}}{A(v)} = \frac{vA'(v)}{A(v)},$$

so we typically solve $n = \dfrac{vA'(v)}{A(v)}$ for $v \in (0, R)$, if possible.

Example 4.26

For rooted binary trees with generating function

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

we have seen in past chapters that $R = 1/4$. The following table shows the probabilities of generating trees of size $n = 0, 1, 2, 3$ for different values of v approaching R. The expected sizes of the trees generated are approximately

- 0.14 if $v = 0.1$
- 0.62 if $v = 0.2$
- 24.5 if $v = 0.2499$

Comment 4.9

See more at https://enumeration.ca/asymptotics/random-generation/.

5 Final Exercises

5.1 LIFT

Exercise 5.1

Fix an integer $k \geq 2$. A k-ary rooted tree T has a root node $\odot$, and each node may have at most one child of each of k "types". (The case $k = 2$ gives BRTs, and the case $k = 3$ gives TRTs.)

(a) Show that the number of k-ary rooted trees with n nodes is $\frac{1}{n}\binom{kn}{n-1}$.

(b) Show that, as $n \to \infty$, the expected number of terminals among all k-ary rooted trees with n nodes is asymptotically $\big(1 - 1/k\big)^k n$.

Proof. (a) Let $T(z)$ be the OGF of k-ary rooted trees by number of nodes. A tree is a root (z) with, for each of the k types, either no child or a subtree:

$$T(z) = z\big(1 + T(z)\big)^k.$$

This is of the form $T = z\phi(T)$ with $\phi(t) = (1+t)^k$. By LIFT,

$$[z^n]T(z) = \frac{1}{n}[t^{n-1}]\phi(t)^n = \frac{1}{n}[t^{n-1}](1+t)^{kn} = \frac{1}{n}\binom{kn}{n-1}.$$

(b) Let $T(z,u)$ be the OGF where u marks terminals (leaves). A node is either terminal (no children, weight u) or has at least one child:

$$T(z,u) = z\Big(u + (1 + T(z,u))^k - 1\Big).$$

Again $T = z\phi(T,u)$ with $\phi(t,u) = u + (1+t)^k - 1$. By LIFT,

$$[z^n]T(z,u) = \frac{1}{n}[t^{n-1}]\big((1+t)^k - 1 + u\big)^n.$$

Write $T_n(u) = [z^n]T(z,u)$.

$$T_n(1) = \frac{1}{n}[t^{n-1}](1+t)^{kn} = \frac{1}{n}\binom{kn}{n-1},$$

$$T_n'(1) = \frac{1}{n}\frac{d}{du}[t^{n-1}]\big((1+t)^k - 1 + u\big)^n\Big|_{u=1} = \binom{k(n-1)}{n-1}.$$

Thus the expected number of terminals is

$$\mathbb{E}_n = \frac{T_n'(1)}{T_n(1)} = n\,\frac{\binom{k(n-1)}{n-1}}{\binom{kn}{n-1}} = n\prod_{j=1}^{k}\frac{(k-1)(n-1)+j}{k(n-1)+j}.$$

For fixed k and $n \to \infty$, each factor tends to $(k-1)/k$, hence

$$\mathbb{E}_n \sim \left(\frac{k-1}{k}\right)^k n = \left(1 - \frac{1}{k}\right)^k n.$$

as desired. $\square$

Exercise 5.2

If an SDLP (super-diagonal lattice path, also known as Dyck path) P touches the diagonal $x = y$ at points

$$(0,0) = (k_0, k_0),\ (k_1, k_1),\ \dots,\ (k_r, k_r) = (n, n),$$

then the sub-path of P between the points (k_{i-1}, k_{i-1}) and (k_i, k_i) is called the i-th block of P. Show that the expected number of blocks among all SDLPS to (n, n) is $3n/(n + 2)$.

Proof. Superdiagonal lattice paths from $(0, 0)$ to (n, n) are Dyck paths of semilength n, counted by the Catalan numbers

$$C_n = \frac{1}{n+1}\binom{2n}{n},$$

with generating function

$$C(z) = \sum_{n\geq 0} C_n z^n, \qquad C(z) = 1 + zC(z)^2.$$

Every Dyck path is a sequence of *primitive* Dyck paths (those touching the diagonal only at start and end). These primitives correspond exactly to the blocks. Let $P(z)$ be the OGF of primitive Dyck paths. Then

$$C(z) = \frac{1}{1 - P(z)} \quad \Rightarrow \quad P(z) = 1 - \frac{1}{C(z)}.$$

Mark each block with a variable u. The bivariate OGF is $C(z, u) = \frac{1}{1-uP(z)}$. Then $[z^n u^k]C(z, u)$ counts paths of semilength n with k blocks, and

$$\frac{\partial}{\partial u} C(z,u)\bigg|_{u=1} = \frac{P(z)}{(1 - P(z))^2} = P(z)C(z)^2 = \big(1 - \tfrac{1}{C(z)}\big)C(z)^2 = C(z)^2 - C(z).$$

Thus the total number of blocks over all paths of semilength n is

$$B_n = [z^n]\big(C(z)^2 - C(z)\big).$$

Using $C(z) = 1 + zC(z)^2$ gives $C(z)^2 = \dfrac{C(z) - 1}{z}$, so

$$C(z)^2 = \sum_{n\geq 0} C_{n+1} z^n,$$

hence $B_n = C_{n+1} - C_n$. Therefore the expected number of blocks among all SDLPs to (n, n) is

$$\mathbb{E}_n = \frac{B_n}{C_n} = \frac{C_{n+1} - C_n}{C_n} = \frac{C_{n+1}}{C_n} - 1.$$

Now

$$\frac{C_{n+1}}{C_n} = \frac{\frac{1}{n+2}\binom{2n+2}{n+1}}{\frac{1}{n+1}\binom{2n}{n}} = \frac{4n+2}{n+2},$$

so

$$\mathbb{E}_n = \frac{4n+2}{n+2} - 1 = \frac{3n}{n+2}.$$

□

5.2 q-Analogue

Exercise 5.3

Show that for $k, m, n \in \mathbb{N}$:

$$\begin{bmatrix} m+n \\ k \end{bmatrix}_q = \sum_{j=0}^{k} q^{(m-j)(k-j)} \begin{bmatrix} m \\ j \end{bmatrix}_q \begin{bmatrix} n \\ k-j \end{bmatrix}_q.$$

Exercise 5.4

(a) Let $0 \leq a \leq c \leq b$ be integers. Show that

$$\binom{a+b}{b} = \sum_{j=0}^{a} \binom{c}{c-j} \binom{a+b-c}{j+b-c}.$$

(b) State (without proof) a generalization of the formula in part (a) which involves q-binomial coefficients.

Exercise 5.5

Fix $n \in \mathbb{N}$ and $0 \leq k \leq n$, and let $q = p^c$ be a prime power. Let $\mathbb{F}_q$ denote the finite field with q elements. Show that the number of k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$ is $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

5.3 Integer Partitions

Exercise 5.6

Let $\mathrm{pe}(n)$ be the number of partitions of size n with an even number of parts, and let $\mathrm{po}(n)$ be the number of partitions of size n with an odd number of parts. Let $\mathrm{od}(n)$ be the number of partitions of size n which have odd and distinct parts. Show that for all $n \in \mathbb{N}$:

$$\mathrm{pe}(n) - \mathrm{po}(n) = (-1)^n \,\mathrm{od}(n).$$

Exercise 5.7

Show that

$$\prod_{i=1}^{\infty} (1 + x^{2i-1} y) = \sum_{d=0}^{\infty} \frac{x^{d^2} y^d}{(1-x^2)(1-x^4)\cdots(1-x^{2d})}.$$

5.4 Exponential Generating Functions

Exercise 5.8

Recall that a derangement is a permutation with no fixed points. Let $\mathcal{D}$ be the class of derangements. Derive the exponential generating function

$$D(x) = \frac{\exp(-x)}{1-x}.$$

Exercise 5.9

For a permutation $\sigma \in S_n$, let $c(\sigma)$ be the number of cycles of σ. What is the average value of $c(\sigma)$ among all $n!$ permutations in S_n?

Proof. Let P be the class of permutations labelling on cycles, so $P = SET(\mu \times CYC(z))$, and hence

$$P(u,z) = \exp\left(u \cdot \log\left(\frac{1}{1-z}\right)\right)$$

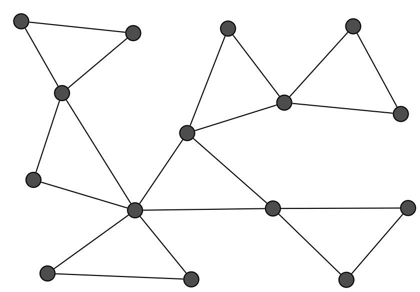
Therefore, we have

$$P_u(1,z) = \log\left(\frac{1}{1-z}\right) \cdot (1-z)^{-u}\Big|_{u=1}$$

The rest follows intuitively. □

Exercise 5.10

A *triangle-tree* is a connected graph in which every edge is in exactly one cycle, and this cycle has length three (see figure below).



Show that the number of triangle-trees with vertex-set N_n is 0 when n is even, and is

$$\frac{(2k)!(2k+1)^{k-1}}{k!\,2^k}$$

when $n = 2k+1$ is odd. (Hint: Describe the recursive structure of the class of rooted triangle-trees.)

Proof. Let T be the class, then

$$T = SET(SET_{=2}(z))$$

When extrac coefficient, remember to devide the result value by n because the specification is rooted, but the triangle trees are not. □

Exercise 5.11

Prove that the number p_n of permutations of $\{1, \ldots, 2n\}$ which have no cycles of length larger than n is

$$p_n = (2n)! \left(1 - \sum_{k=n+1}^{2n} \frac{1}{k} \right).$$

Index