

SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Generating Functions and Applications

av

Arthur Shagulian

2014 - No 29

Generating Functions and Applications

Arthur Shagulian

Självständigt arbete i matematik 15 högskolepoäng, Grundnivå

Handledare: Paul Vaderlind

2014

Abstract

A generating function is a formal power series that contains information about a sequence of numbers. Applications of generating functions are many. They are used in a broad field of study and are powerful tools used in different type of computational problems. In this paper we shall be mainly concerned about two applications: i) *Exact Covering Sequence* (ECS): which refers to a finite sequence of residue classes in which every non-negative integer is covered by one and only one congruent; by using generating functions, cyclotomic polynomials and Möbius inversion formula, we shall show whether any given set of residue classes can be an ECS. ii) Calculation of the number of *Square Roots of a given Permutation*.: Here we are going to use cyclic index of the symmetric group to create an exponential generating function which shall provide us with the number of permutations of a given set with possible square roots.

Acknowledgement

I would like to express my gratitude to Ph.D. Paul Vaderlind for suggesting the topic of this bachelor thesis, and his guidance throughout the preparation of it.

I would also like to thank Professor Rikard Bøgvad for a thorough reading of the manuscript and providing me with several invaluable comments and corrections.

Contents

1	Introduction	2
2	General Properties of Generating Functions	4
	2.1 General Idea	4
	2.2 Formal Power Series	5
	2.3 Ordinary Generating Functions	5
	2.4 Exponential Generating Functions	8
	2.5 Formal Dirichlet Series and Zeta Function	10
3	Exact Covering Sequence	13
	3.1 Congruences	13
	3.2 Roots of Unity and Cyclotomic Polynomials	14
	3.3 Exact Covering Sequence	16
4	Square Roots of Permutations	19
	4.1 Permutations	19
	4.2 The Cyclic Index of the Symmetric Group	20
	4.3 Square Roots	22
5	A Short Summary and Further Horizon	28

0.1 Introduction

The concept of discrete mathematics has its origin in India, where they knew how to find the number of the permutation of a set with n elements, and the formula for the subsets of a given cardinality in a set of n elements. Discrete Mathematics consists of several sub-areas such as: set theory, number theory, probability, combinatorics. Combinatorial mathematics, as we know it today, was for the first time introduced by *Blaise Pascal*, *Abraham de Moivre* and *Leonhard Euler*, between 17th and 18th centuries. One of the most remarkable parts of combinatorial mathematics is the topic generating functions. The concept has shown to be a truly useful tool for solving mathematical problems. Generating functions are like magic boxes that are able to transform problems concerning sequence of numbers into the world of functions.

There are many type of generating functions, including ordinary and exponential generating functions, Bell series, Lambert series and Dirichlet series. The field, in which the generating functions are being used is broad with many applications. They could be used for finding averages, counting polyominoes and proving congruences among combinatorial numbers, just to name a few. The applications that We shall talk about in this paper are *exact covering sequence* and *square roots of permutations*. We shall begin our work with some general ideas followed by quick review of formal power series. Next we move to generating functions where we start by ordinary and exponential generating functions and gradually dig deeper into *formal Dirichlet series*, *Möbius function and inversion formula* and *zeta function*.

A *covering sequence* $\{(a_i, b_i)\}$, $i = 1, 2, \dots, k$, is a set of finite residue classes $n \equiv a_i \pmod{b_i}$ - with the relation $n = a_i + tb_i$, $t \in \mathbb{Z}$ -, whose union covers all positive integers. In an *exact covering sequence*, every positive integer is covered by one and only congruent. The question that rises here is: How can we know if a complete residue system is an exact covering sequence? For a collection of pairs (a_i, b_i) , $i = 1, 2, \dots, k$ to be exact covering sequence, it is necessary that the property $\sum_j 1/b_j = 1$ holds. But in order to have a better understanding, we shall create the polynomial

$$\psi_s(z) = \sum_{j:s|b_j} z^{a_j}/b_j,$$

and show that it is divisible by the cyclotomic polynomial

$$\Phi_s(z) = \prod_{\substack{1 \leq k \leq s \\ k:(k,s)=1}} (z - e^{2\pi ik/s}) \quad \text{where } s = 1, 2, 3, \dots$$

Not all permutations have square roots, for instance, the permutations $\sigma = (1, 2)$, can not be expressed as $\tau^2 = \sigma$. Then we ask the question: How many of the permutation of a given set S_n have square roots? And we shall come to the conclusion that, whether a permutation σ has or not square roots depends on the number of the specific type of cycles it is composed of. To prove this and find the permutations with desired cycle types we shall use *cyclic index of the symmetric group* - which is another useful application of generating functions - along with Taylor expansion of *hyperbolic cosine function* to create the necessary generating function

$$\sum_{n \geq 0} f(n, 2) \frac{x^n}{n!} = e^{x_1 t} \cosh(x_2 t^2 / 2) e^{x_3 t^3 / 3} \cosh(x_4 t^4 / 4) e^{x_5 t^5 / 5} \dots$$

which will provide us with the number of permutations of n letters that have square roots.

0.2 General Properties of Generating Functions

As the title suggests this section will be dedicated to generating functions and some of their properties. To have a better understanding for generating functions it is essential to have a good grasp of the power series and some of the properties it has. We will be dividing this section into five subsections, which shall cover ordinary and exponential generating functions followed by Dirichlet series and zeta function. Let us now start with some general ideas.

0.2.1 General Idea

A convenient way of representing the sequence of numbers $2, 4, 6, 8, 10, \dots$ would be to use the formula $a_n = 2(n + 1)$ for $n = 0, 1, 2, \dots$. Finding a formula for a given sequence of numbers is not always as simple as it seems, for example, the sequence of numbers $\{a_n\}_{n \geq 0} = 2, 3, 5, 7, 11, 13, 17, 19, \dots$ where a_n represents the n th prime number, has shown to be an impossible task.

Generating functions contain information about sequence of numbers in a compact form, and they are of great help for solving problems in combinatorial mathematics. For example, the function $g(x) = (2 + x)^4$, generates the sequence of numbers $16, 32, 24, 8, 1, 0, 0, 0, \dots$. To see this, we expand $g(x)$ and get $(2 + x)^4 = 16 + 32x + 24x^2 + 8x^3 + x^4$, in which we can clearly see that the coefficients of $g(x)$ represent the sequence of numbers mentioned above.

For a given function, it is straight forward to find the sequence of numbers it generates. But what if, we have a sequence of numbers, or even the formula that generates that sequence of numbers and want to find that very function that generates it. Suddenly we feel that it gets trickier.

Just to give you a taste of the matter, let us take a look at Fibonacci numbers F_0, F_1, F_2, \dots and the recurrence relation

$$F_{n+1} = F_n + F_{n-1} \quad (n \geq 1; F_0 = 0; F_1 = 1),$$

that produces them. $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \dots$ are the first thirteen numbers in the Fibonacci sequence and you can easily continue and get an exact non-complicated result.

Now, just to get a hint of what a generatingfunctionologist could strive for, we unveil the function,

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

which is the generating function for Fibonacci numbers. The n :th Fibonacci number F_n is the coefficient of x^n in the expansion of $F(x)$.

0.2.2 Formal Power Series

When a_n is a sequence of numbers, we call

$$\sum_{n=0}^{\infty} a_n = a_0 + a_1 + a_2 + a_3 + \dots,$$

for a *series*. In other words a *series* is the sum of a sequence of numbers. Infinite sequence can't always be summed. We can clearly see, that the sequence $1, 2, 3, \dots$ can't be summed to anything that would make sense. There are anyway many infinite sequences that give us some elegant results when we sum them. For instance $\sum_{n=1}^{\infty} 1/n^2 = 1 + 1/2^2 + 1/3^2 + \dots = \pi^2/6$.

A sequence of numbers can also be partially summed, but what we are mostly interested in a series is when it reaches the limit of the partial summation. And what we are really interested in is that: what happens to a series when it reaches the limit?

Definition 0.2.1. A series $\sum_n a_n$ is called **convergent** if the limit $\lim_{n \rightarrow \infty} S_n$ exists, where

$$S_n = \sum_{k=0}^n a_k.$$

Otherwise, we say that the series is **divergent**.

A very useful series is the *geometrical series* which converges for $|x| < 1$ and diverges for every other value of x .

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1 - x}, \quad \text{where } |x| < 1.$$

0.2.3 Ordinary Generating Functions

Definition 0.2.2. For the finite sequence of numbers $a_0, a_1, a_2, a_3, \dots$ the series

$$f(x) = \sum_{n=0}^{\infty} a_n x^n,$$

is called the generating function of that sequence of numbers.

A very simple example is the sequence $1, 1, 1, 1, 1, 1, \dots$ and the function generating it is the geometric series $1 + x + x^2 + x^3 + x^4 + \dots = 1/(1 - x)$. To generalize this idea, we can argue that the sequence a, ab, ab^2, ab^3, \dots is generated by the function $a + abx + ab^2x^2 + ab^3x^3 + \dots = a/(1 - bx)$.

Next (simple) example would be the sequence $1, 2, 3, 4, \dots$ which has the generating function $1 + 2x + 3x^2 + 4x^3 + \dots$. Now, if we would look closely we could see that,

$$\begin{aligned} 1 + 2x + 3x^2 + 4x^3 + \dots &= \frac{d}{dx}(1 + x + x^2 + x^3 + \dots) = \frac{d}{dx} \frac{1}{1 - x} \\ &= \frac{1}{(1 - x)^2} = \sum_{n \geq 0} (n + 1)x^n. \end{aligned}$$

Unfortunately we can't use the same method entirely to calculate the sequence $1, 4, 9, 16, 25, 36, 49, \dots$ so we need to tweak it a little,

$$\begin{aligned} 1 + 4x + 9x^2 + 16x^3 + \dots &= 1 + 2^2x + 3^2x^2 + 4^2x^3 + \dots \\ &= \frac{d}{dx}(x + 2x^2 + 3x^3 + 4x^4 + \dots) \\ &= \frac{d}{dx} \sum_{n \geq 0} (n + 1)x^{n+1} \\ &= \sum_{n \geq 0} (n + 1)^2x^n. \end{aligned}$$

Let us now take a look at Fibonacci numbers F_0, F_1, F_2, \dots and find out what generates it. In other words, we need to find an exact formula for the function $F(x) = \sum_{n \geq 0} F_n x^n$, which generates the Fibonacci sequence. We know that Fibonacci numbers can be expressed by recurrence formula

$$F_{n+1} = F_n + F_{n-1}, \quad (n \geq 1, F_0 = 0, F_1 = 1) \quad (0.2.3.1)$$

and it gives us the sequence $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \dots$. Now we multiply the sequence with x^n and sum it over $n \geq 1$

$$\begin{aligned} \sum_{n \geq 1} F_{n+1}x^n &= \sum_{n \geq 1} F_n x^n + \sum_{n \geq 1} F_{n-1}x^n \Rightarrow \\ \Rightarrow \frac{F(x) - x}{x} &= F(x) + xF(x) \Rightarrow F(x) = \frac{x}{1 - x - x^2}. \end{aligned}$$

To expand $\frac{x}{1 - x - x^2}$ in partial fraction, we begin first with factorization of the expression,

$$1 - x - x^2 = (1 - xr_+)(1 - xr_-), \quad \text{where } (r_{\pm} = \frac{1 \pm \sqrt{5}}{2}) \Rightarrow$$

$$\frac{x}{1-x-x^2} = \frac{x}{(1-xr_+)(1-xr_-)}.$$

Using partial fraction method we obtain

$$\begin{aligned} \frac{x}{1-x-x^2} &= \frac{1}{r_+ - r_-} \left(\frac{1}{(1-xr_+)} - \frac{1}{(1-xr_-)} \right) \\ &= \frac{1}{\sqrt{5}} \left(\sum_{j \geq 0} r_+^j x^j - \sum_{j \geq 0} r_-^j x^j \right) \\ &= \frac{1}{\sqrt{5}} \left(\sum_{j \geq 0} r_+^j - r_-^j \right) x^j, \end{aligned}$$

so it becomes clear now that the coefficient of x^n for the n :th Fibonacci number is

$$F_n = \frac{1}{\sqrt{5}} \left(\sum_{j \geq 0} r_+^j - r_-^j \right), \text{ where } (r_{\pm} = \frac{1 \pm \sqrt{5}}{2}), \text{ and } n = 0, 1, 2, \dots$$

Throughout this paper you will see the symbol $f \overset{ogf}{\longleftrightarrow} \{a_n\}_0^\infty$ which means that the power series f is the *ordinary power series generating function* or for short *ogf* of the sequence $\{a_n\}_0^\infty$.

If $f \overset{ogf}{\longleftrightarrow} \{a_n\}_0^\infty$ then we have the following rules:

- For integer $m > 0$

$$\{a_{n+m}\}_0^\infty \overset{ogf}{\longleftrightarrow} \frac{f - a_0 - \dots - a_{m-1}x^{m-1}}{x^m}.$$

- For integer $k > 0$

$$\{n^k a_n\}_0^\infty \overset{ogf}{\longleftrightarrow} \left(x \frac{d}{dx}\right)^k f,$$

or, if P is a polynomial, then

$$P\left(x \frac{d}{dx}\right) f \overset{ogf}{\longleftrightarrow} \{P(n)a_n\}_0^\infty.$$

- For $g \overset{ogf}{\longleftrightarrow} \{b_n\}_0^\infty$

$$fg \overset{ogf}{\longleftrightarrow} \left\{ \sum_{r+s=n} a_r b_s \right\}_{n=0}^\infty.$$

This can be applied for more than two series. Let $h \xleftrightarrow{ogf} \{c_t\}_0^\infty$ then,

$$fgh \xleftrightarrow{ogf} \left\{ \sum_{r+s+t=n} a_r b_s c_t \right\}_{n=0}^\infty.$$

- This rule is a direct consequence of the previous rule and is about finding the k th root of a power series. Let integer $k > 0$

$$f^k \xleftrightarrow{ogf} \left\{ \sum_{n_1+n_2+\dots+n_k=n} a_{n_1} a_{n_2} a_{n_3} \dots a_{n_k} \right\}_{n=0}^\infty.$$

- This rule is about the result we get when multiplying power series f by $1/(1-x)$

$$\begin{aligned} \frac{f}{1-x} &= (a_0 + a_1x + a_2x^2 + \dots)(1 + x + x^2 + \dots) \\ &= a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + \dots \\ &= \sum_{n=0}^\infty x^n \left(\sum_{k=0}^n a_k \right), \end{aligned}$$

in other words, for $n \geq 0$

$$\frac{f}{1-x} \xleftrightarrow{ogf} \left\{ \sum_{k=0}^n a_k \right\}.$$

0.2.4 Exponential Generating Functions

Definition 0.2.3. Let $a_0, a_1, a_2, a_3, \dots$ be a sequence of real numbers. Then, the function

$$f(x) = a_0 + a_1 \frac{x}{1!} + a_2 \frac{x^2}{2!} + a_3 \frac{x^3}{3!} + \dots = \sum_{i=0}^\infty a_i \frac{x^i}{i!},$$

is an exponential generating function of that sequence.

Let $(1+x)^n = \binom{n}{0}x^0 + \binom{n}{1}x^1 + \binom{n}{2}x^2 + \dots + \binom{n}{n}x^n$. This means that equation $(1+x)^n$ is the (ordinary) generating function of the sequence $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n}, 0, 0, 0, \dots$. We also know that,

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{P(n, k)}{k!}, \quad \text{where } P(n, k) = \frac{n!}{(n-k)!},$$

$$(1+x)^n = P(n,0)\frac{x^0}{0!} + P(n,1)\frac{x^1}{1!} + P(n,2)\frac{x^2}{2!} + \dots + P(n,n)\frac{x^n}{n!},$$

in which, we can clearly see that $(1+x)^n$, aside from being the ordinary generating function for the sequence $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n}, 0, 0, 0, \dots$, is the exponential generating function for $P(n,0), P(n,1), \dots, P(n,n), 0, 0, 0, \dots$. If we also take a look at the Maclaurin series for the natural exponential function

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \dots,$$

we will see that it is the exponential generating function for the sequence $1, 1, 1, 1, 1, 1, \dots$ and at the same time, the ordinary generating function for the sequence $1, 1/2!, 1/3!, 1/4!, 1/5!, 1/6!, 1/7!, \dots$.

The name of the *exponential generating function* comes from the fact that the exponential generating function of the sequence $\{1, 1, 1, 1, \dots\}$ is

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

We are now going to investigate how the rules from the previous section, which were applied to *ordinary generating functions*, are going to work for *exponential generating functions*. We shall use the same symbols except the letters *ogf*, which will be replaced with *egf*, short for *exponential generating function*.

- If $f \xleftrightarrow{egf} \{a_n\}_0^\infty$, then $f' \xleftrightarrow{egf} \{a_{n+1}\}_0^\infty$. To see this, we differentiate f ,

$$f' = \sum_{n=1}^{\infty} n a_n \frac{x^{n-1}}{n!} = \sum_{n=1}^{\infty} a_n \frac{x^{n-1}}{(n-1)!} = \sum_{n=0}^{\infty} a_{n+1} \frac{x^n}{n!}.$$

For $k \geq 0$ we generalize the rule to,

$$\{a_{n+k}\}_0^\infty \xleftrightarrow{egf} \left(\frac{d}{dx}\right)^k f.$$

- This rule is the same as the one for the ordinary generating functions. If $f \xleftrightarrow{egf} \{a_n\}_0^\infty$, and P is a polynomial, then

$$P\left(x \frac{d}{dx}\right) f \xleftrightarrow{egf} \{P(n)a_n\}_0^\infty.$$

- This rule is about multiplying two generating functions. Let $f \xleftrightarrow{egf} \{a_n\}_0^\infty$ and $h \xleftrightarrow{egf} \{c_n\}_0^\infty$, then

$$fh = \left\{ \sum_{r=0}^{\infty} a_r \frac{x^r}{r!} \right\} \left\{ \sum_{t=0}^{\infty} c_t \frac{x^t}{t!} \right\} = \sum_{r,t \geq 0} a_r c_t \frac{x^r x^t}{s!t!} = \sum_{n=0}^{\infty} x^n \left\{ \sum_{r+t=n} \frac{a_r c_t}{s!t!} \right\}.$$

We multiply the last expression with $n!/n!$ and get

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} \left\{ \sum_{r+t=n} \frac{n! a_r c_t}{r!t!} \right\} \Rightarrow fh \xleftrightarrow{egf} \sum_r \binom{n}{r} a_r c_{n-r},$$

hence, fh is the generating function for the sequence $\left\{ \sum_{r+t=n} \binom{n}{r} a_r c_{n-r} \right\}_0^\infty$ and more generally

$$fgh \dots \xleftrightarrow{egf} \left\{ \sum_{r+s+t+\dots=n} \frac{n! a_r b_s c_t \dots}{r!s!t! \dots} \right\}_0^\infty,$$

and in the case, where we seek the coefficients of a multinomial,

$$f^k \xleftrightarrow{egf} \left\{ \sum_{r_1+r_2+r_3+\dots=n} \binom{n!}{r_1!r_2!r_3! \dots} a_{r_1} a_{r_2} a_{r_3} \dots \right\}_0^\infty$$

is the function to turn to.

0.2.5 Formal Dirichlet Series and Zeta Function

Definition 0.2.4. A formal power series of the form

$$f(x) = \sum_{n=1}^{\infty} \frac{a_n}{n^x} = a_1 + \frac{a_2}{2^x} + \frac{a_3}{3^x} + \frac{a_4}{4^x} + \dots$$

is called *Dirichlet series generating function*, which generates the sequence $\{a_n\}_1^\infty$ and will be denoted by

$$f(x) \xleftrightarrow{Dir} \{a_n\}_1^\infty.$$

In the cases of *ogf* and *egf* we are familiar with the function that generates the sequence $\{1\}_1^\infty$, namely $1/(1-x) \xleftrightarrow{ogf} \{1\}_1^\infty$ and $e^x \xleftrightarrow{egf} \{1\}_1^\infty$. The question that we ask now is: what function generates $\{1\}_1^\infty$ in our present

case, the formal Dirichlit series? And the answer is, the *Riemann zeta function*

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x} = 1 + 2^{-x} + 3^{-x} + 4^{-x} + \dots,$$

one of the most important functions in analysis.

Next, we would like to know what sequence is generated by $f(x)g(x)$, where $f(x) \xleftrightarrow{Dir} \{a_n\}_1^{\infty}$ and $g(x) \xleftrightarrow{Dir} \{b_n\}_1^{\infty}$.

$$\begin{aligned} f(x)g(x) &= (a_1 + a_2 2^{-x} + a_3 3^{-x} + \dots)(b_1 + b_2 2^{-x} + b_3 3^{-x} + \dots) \\ &= (a_1 b_1) + (a_1 b_2 + a_2 b_1) 2^{-x} + (a_1 b_3 + a_3 b_1) 3^{-x} \\ &\quad + (a_1 b_4 + a_2 b_2 + a_4 b_1) 4^{-x} + \dots \end{aligned}$$

and it becomes clear that if $f(x) \xleftrightarrow{Dir} \{a_n\}_1^{\infty}$ and $g(x) \xleftrightarrow{Dir} \{b_n\}_1^{\infty}$, then

$$f(x)g(x) \xleftrightarrow{Dir} \left\{ \sum_{d|n} a_d b_{n/d} \right\}_{n=1}^{\infty}. \quad (0.2.5.1)$$

Back to the zeta function, where $\zeta(x) \xleftrightarrow{Dir} \{1\}_1^{\infty}$, we can obtain $d(n)$, which is the number of the divisors of n , by finding the sequence that is generated by ζ^2 ,

$$\zeta(x) \xleftrightarrow{Dir} \left\{ \sum_{d|n} 1 \right\}_{n=1}^{\infty}, \quad \text{thus, } \zeta^2 \xleftrightarrow{Dir} \sum_{d|n} 1 = d(n).$$

Definition 0.2.5. An arithmetic function f is called a *multiplicative number theoretic function*, if $f(n_1 n_2 n_3 \dots) = f(n_1) f(n_2) f(n_3) \dots$ for all integers $n_i \geq 1$ where $\gcd(n_i, n_j) = 1$ and $i \neq j$.

And since every positive integer can be uniquely express as a product of prime numbers, $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$, the multiplicative number-theoretic function can be expressed by $f(n) = f(p_1^{a_1}) f(p_2^{a_2}) f(p_3^{a_3}) \dots f(p_k^{a_k})$.

An example of a multiplicative function would be $d(n)$, the number of divisors of n . For instance

$$4 = d(6) = d(2 \cdot 3) = d(2)d(3) = 2 \cdot 2 = 4.$$

We are now going to take a look at an identity - and it uses -, that multiplicative number-theoretic function satisfies.

Theorem 0.2.1. *Let f be a formal multiplicative number-theoretic function. Then we have the formal identity*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^x} = \prod_p \{1 + f(p)p^{-x} + f(p^2)p^{-2x} + f(p^3)p^{-3x} + \dots\}. \quad (0.2.5.2)$$

And if we take the multiplicative function $f(n) = 1$ for all n , then we obtain $\zeta(x) = \prod_p \{1 + p^{-x} + p^{-2x} + p^{-3x} + \dots\} = 1/(\prod_p \{1 - p^{-x}\})$ which is the fundamental factorization of zeta function.

Definition 0.2.6. Let $n = \prod_{i=1}^k p_i^{a_i}$ be a positive integer, where p_i is a prime and $a_i \geq 0$. Then,

$$\mu(n) = \begin{cases} +1, & \text{if } 0 \leq a_i \leq 1 \text{ and } |p_i| \text{ is even;} \\ -1, & \text{if } 0 \leq a_i \leq 1 \text{ and } |p_i| \text{ is odd;} \\ 0, & \text{if } 2 \leq a_i, \end{cases}$$

is the *Möbius function*.

Our next move is to find the reciprocal of the zeta function. We begin by replacing $f(n)$ in (2.5.2) with the Möbius function $\mu(n)$ and get the following result.

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^x} = \prod_p \{1 - p^{-x}\}, \quad (0.2.5.3)$$

which implies that

$$\frac{1}{\zeta(x)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^x}, \quad \text{or equally, } \frac{1}{\zeta(x)} \xleftrightarrow{Dir} \{\mu(n)\}_1^{\infty},$$

And to see the magic of this process at work, let us have two sequences $\{a_n\}_1^{\infty}$ and $\{b_n\}_1^{\infty}$ with the relation $a_n = \sum_{d|n} b_d$ where n is a positive integer. What we would like to achieve now, is to invert this relation, and solve it for b_n in terms of a_n .

Since $f(x) \xleftrightarrow{Dir} \{a_n\}_1^{\infty}$ and $g(x) \xleftrightarrow{Dir} \{b_n\}_1^{\infty}$, by (2.5.1) it becomes obvious that $\sum_{d|n} b_d \xleftrightarrow{Dir} g(x)\zeta(x)$. Knowing this, we can write the equality $f(x) = g(x)\zeta(x)$, which implies that $g(x) = f(x)/\zeta(x)$, and by (2.5.1), $f(x)/\zeta(x) \xleftrightarrow{Dir} \sum_{d|n} \mu(n/d)a_d$. Thus,

$$b_n = \sum_{d|n} \mu\left(\frac{n}{d}\right)a_d, \quad n = 1, 2, 3, \dots \quad (0.2.5.4)$$

0.3 Exact Covering Sequence

Finding a set of congruences which could represent or cover a whole sequence of numbers is indeed very fascinating. Our main goal in this section is to focus on *exact covering sequences*, and we are going to use generating functions, which are excellent tools in finding out whether a covering sequence is exact or not.

0.3.1 Congruences

Definition 0.3.1. Let b be a positive integer. If n and a are integers, we say that n is congruent to a modulo b if $b|(n - a)$ and denote it

$$n \equiv a \pmod{b}.$$

This is called *residue class* with *modulo* n or an *arithmetic sequence* with *common difference* b .

Theorem 0.3.1. If n and a are positive integers, then

$$n \equiv a \pmod{b}$$

if and only if there is an integer t for which $n = a + bt$.

Definition 0.3.2. A *covering system* (also called complete residue system) is a finite system of congruences

$$n \equiv a_i \pmod{b_i}, \quad 1 < i < t,$$

if every integer n satisfies at least one of the congruences.

For instance, every possible integer is covered by the congruent system $A = \{(1, 2), (0, 3), (0, 4), (2, 4)\}$, where each pair $(a_i, b_i) \in A$ represent the congruence relation $n \equiv a_i \pmod{b_i}$, $(i = 1, 2, 3, 4)$.

Definition 0.3.3. An *exact covering system* is a covering system, in which each integer is covered by one and only one congruence relation.

Since the integer $n = 12$ can be covered with both $(0, 3)$ and $(0, 4)$, the covering system $A = \{(1, 2), (0, 3), (0, 4), (2, 4)\}$ is not an "exact" one. But, by removing $(0, 3)$, it can easily become an exact covering system.

0.3.2 Roots of Unity and Cyclotomic Polynomials

Roots of Unity

The roots of the polynomial $x^n = 1$ are called the *roots of unity* and they form a group under multiplication. There are precisely n roots of unity when solving the polynomial $x^n - 1$. We are going to describe each root as ζ_n^k , $1 \leq k \leq n$, expressing them as k th powers of a fix primitive root ζ_n . These roots are complex numbers and have the form

$$\begin{aligned}\zeta_n^k &= (\zeta_n)^k = \left(\exp\left(\frac{2\pi i}{n}\right) \right)^k \\ &= \left(\cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right) \right)^k = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right).\end{aligned}$$

For a $1 \leq d \leq n$ such as $d|n$ we have

$$\zeta_n^d = \exp\left(\frac{2\pi i}{n/d}\right) = \zeta_{n/d}.$$

As mentioned above, the roots of unity form a group under multiplication. In other words, if $\zeta_n^{k_1}$ and $\zeta_n^{k_2}$, then $\zeta_n^{k_1} \zeta_n^{k_2} = \zeta_n^{k_1+k_2}$, where $1 \leq k_1 + k_2 \leq n$ is also a root. Or more generally expressed

$$x^n - 1 = \prod_{1 \leq k \leq n} (x - \zeta_n^k).$$

An n th root of unity ζ is called *primitive* if $\zeta^m \neq 1$ for all $m < n$. The primitive roots of unity are

$$\zeta_n^k, \quad \text{where } \gcd(k, n) = 1.$$

Now, if we have $\gcd(k, n) = m$, where the integer $m > 1$, and we denote $k/m = t$ and $n/m = s$ we can obtain

$$\zeta_n^k = \zeta_n^{mt} = \zeta_{n/m}^t = \zeta_s^t,$$

and since $\gcd(s, t) = 1$, the ζ_n^k is a primitive s th root of unity.

We are now going to group the factors of the $(x^n - 1)$, and the result is

$$x^n - 1 = \prod_{1 \leq k \leq n} (x - \zeta_n^k) = \prod_{s|n} \prod_{\substack{1 \leq k \leq s \\ \gcd(k, s) = 1}} (x - \zeta_s^k).$$

Cyclotomic Polynomials

Definition 0.3.4. The n th cyclotomic polynomial is a monic polynomial with all n th primitive roots of unity as its roots, and is denoted

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ k:(k,n)=1}} (x - \zeta_n^k).$$

The number of k 's is the degree of the cyclotomic polynomials $\Phi_n(x)$ and is denoted $\phi(n)$, and is called the *Euler Phi Function*. So, for $1 \leq k \leq n$,

$$\deg \Phi_n(x) = \phi(n) = |\{1 \leq k \leq n : \gcd(k, n) = 1\}|.$$

Definition 0.3.5. Let ζ be a n th root of unity. The *order* of ζ , denoted $\text{ord}(\zeta)$, is the smallest integer $k > 0$ that satisfies $\zeta^k = 1$.

Theorem 0.3.2. Let n be a positive integer, then

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{0.3.2.1}$$

Proof. We know that the roots of the polynomial $x^n - 1$ are the n th roots of unity. And if ζ is an n th root of unity with $d = \text{ord}(\zeta)$, then ζ is a primitive root of unity and therefore a root of $\Phi_d(x)$. And since $d|n$, ζ is a root of $\prod_{d|n} \Phi_d(x)$. But, both $x^n - 1$ and $\prod_{d|n} \Phi_d(x)$ are monic and thus, the equality holds. \square

The first twelve cyclotomic polynomials are as follows

$$\begin{array}{ll} \Phi_1(x) = x - 1 & \Phi_7(x) = x^6 + x^5 + \dots + 1 \\ \Phi_2(x) = x + 1 & \Phi_8(x) = x^4 + 1 \\ \Phi_3(x) = x^2 + x + 1 & \Phi_9(x) = x^6 + x^3 + 1 \\ \Phi_4(x) = x^2 + 1 & \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1 \\ \Phi_5(x) = x^4 + x^3 + \dots + 1 & \Phi_{11}(x) = x^{10} + x^9 + \dots + 1 \\ \Phi_6(x) = x^2 - x + 1 & \Phi_{12}(x) = x^4 - x^2 + 1 \end{array}$$

Now, with help of Möbius inversion formula, we will obtain reasonably explicit formula for $\Phi_n(x)$. For $n = 1, 2, 3, \dots$, $\ln(\prod_{d|n} \Phi_d(x)) = \ln(x^n - 1)$, which implies that $\sum_{d|n} \ln(\Phi_d(x)) = \ln(x^n - 1)$. And by (2.5.4), we will have $\ln(\Phi_n(x)) = \sum_{d|n} \mu(n/d) \ln(x^d - 1)$, and eventually arrive at

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \tag{0.3.2.2}$$

Just to see how this works, we will take a look at $\Phi_{18}(x)$, which according to our new formula is

$$\begin{aligned} & (x-1)^{\mu(18)}(x^2-1)^{\mu(9)}(x^3-1)^{\mu(6)}(x^6-1)^{\mu(3)}(x^9-1)^{\mu(2)}(x^{18}-1)^{\mu(1)} \\ &= (x-1)^0(x^2-1)^0(x^3-1)^1(x^6-1)^{-1}(x^9-1)^{-1}(x^{18}-1)^1 \\ &= (x^3-1)^1(x^{18}-1)^1/(x^6-1)^1(x^9-1)^1 \\ &= x^6 - x^3 + 1. \end{aligned}$$

0.3.3 Exact Covering Sequence

An *exact covering sequence* (ECS) is a set of ordered pairs (a_i, b_i) , $a_i \geq 0$ and $b_i \geq 1$ such as, for every $n \geq 0$ there is one and only one pair of (a_i, b_i) such that $n \equiv a_i \pmod{b_i}$. Our main goal in this subsection is to find out if a given sequence is an exact covering sequence and we are going to use the generating functions to achieve that goal.

Suppose that (a_i, b_i) , $(i = 1, 2, 3, \dots)$ is an exact covering sequence. Then every $n \geq 0$ can uniquely be written as $n = a_i + tb_i$ where $t \in \mathbb{Z}$. With these in mind, we can rewrite the geometric series

$$\sum_{n=0}^{\infty} x^n = \sum_{i=1}^k \sum_{t \geq 0} x^{a_i + tb_i} = \sum_{i=1}^k \frac{x^{a_i}}{1 - x^{b_i}}, \quad (0.3.3.1)$$

and obtain

$$\sum_{i=1}^k \frac{x^{a_i}}{1 - x^{b_i}} = \frac{1}{1 - x}. \quad (0.3.3.2)$$

Theorem 0.3.3. *For a sequence of pairs (a_i, b_i) , $(i = 1, 2, 3, \dots)$ to be an exact covering sequence, it must have the property (3.3.2).*

A conclusion that can be drawn from this is that, in a ECS, the property $\sum_j 1/b_j = 1$ must hold. To see this, we multiply both sides of (3.3.2) by $1 - x$ and let $x \rightarrow 1$. But we will gain a lot more by digging deeper in the subject.

Now let us begin by expanding the left hand side of (3.3.2)

$$\sum_{i=1}^k \frac{x^{a_i}}{1 - x^{b_i}} = \sum_{\omega: \omega^{B=1}} \frac{A(\omega)}{\omega - x}, \quad (0.3.3.3)$$

where $B = \text{lcm}\{b_i\}$, and

$$A(\omega) = \lim_{x \rightarrow \omega} (\omega - x) \sum_{i=1}^k \frac{x^{a_i}}{1 - x^{b_i}} = \sum_{i=1}^k \omega^{a_i} \lim_{x \rightarrow \omega} \frac{\omega - x}{1 - x^{b_i}}.$$

Now, if $\omega^{b_i} \neq 1$, then $A(\omega) = 0$. Otherwise we will have the case where $\lim_{x \rightarrow \omega} (\omega - x)/(1 - x^{b_i}) = 0/0$ which leads us to L'Hôpital's rule. We can see that $d(\omega - x)/dx = -1$ and $d(1 - x^{b_i})/dx = -b_i x^{b_i-1}$ and have the limits $\lim_{x \rightarrow \omega} d(\omega - x)/dx = -1$ and $\lim_{x \rightarrow \omega} d(1 - x^{b_i})/dx = -b_i \omega^{b_i-1}$ which gives us

$$\begin{aligned} \sum_{i=1}^k \omega^{a_i} \lim_{x \rightarrow \omega} \frac{\omega - x}{1 - x^{b_i}} &= \sum_{i=1}^k \omega^{a_i} \frac{-1}{-b_i \omega^{b_i-1}} \\ &= \sum_{i=1}^k \frac{\omega^{a_i+1}}{b_i \omega^{b_i}} \\ &= \sum_{j: \omega^{b_j}=1} \frac{\omega^{a_j+1}}{b_j}, \end{aligned}$$

and by taking a quick glance at (3.3.2) we can see that in the case where a sequence covers *exactly* all the $A(\omega)$'s vanish except for $\omega = 1$, when $A(1) = 1$. Knowing this, we obtain

$$\sum_{j: \omega^{b_j}=1} \frac{\omega^{a_j}}{b_j} = \begin{cases} 1, & \text{if } \omega = 1 \\ 0 & \text{otherwise.} \end{cases} \quad (0.3.3.4)$$

We proceed by letting $\omega_m^r = \exp(2\pi i r/m)$, ($m > 0$ and $\gcd(r, m) = 1$), represent a primitive m th root of unity. Then we will have the form

$$\sum_{j: m|b_j} \frac{\omega^{a_j}}{b_j} = \begin{cases} 1, & \text{if } m = 1; \\ 0 & \text{otherwise,} \end{cases} \quad (0.3.3.5)$$

in the case when $\{(a_i, b_i)\}_{i=1}^k$ is ECS, we define polynomials that are associated with the sequence $\{(a_i, b_i)\}_{i=1}^k$ in the following way

$$\psi_m(z) = \sum_{j: m|b_j} \frac{z^{a_j}}{b_j}.$$

For a finite system of congruences to be an exact covering sequence, it is necessary that the polynomial ψ_m , for $m > 0$, to vanish at primitive m th roots of unity, and $\psi_1(z) = 1$. And every polynomial that vanishes at primitive m th roots of unity, must be divisible by the cyclotomic polynomial

$$\Phi_m(z) = \prod_{\substack{1 \leq r \leq m \\ r: (r, m)=1}} (z - \omega_m^r) \quad \text{where } m = 1, 2, 3, \dots$$

The first few cyclotomic polynomials are

$$\Phi_1(z) = z - 1, \quad \Phi_2(z) = z + 1, \quad \Phi_3(z) = z^2 + z + 1, \quad \Phi_4(z) = z^2 + 1, \dots$$

And now by combining these last pages, we obtain the following theorem

Theorem 0.3.4. *Let $a_i \geq 0$ and $b_i \geq 1$, then the set $\{(a_i, b_i)\}_{i=1}^k$ is an exact covering sequence if and only if $\sum_j 1/b_j = 1$, and for each $m > 1$, the polynomial $\psi_m(z)$, is divisible by the cyclotomic polynomial $\Phi_m(z)$.*

In his book *generatingfunctionology* [1], Herbert Wilf, gives us a good example of how the set of the pairs $(0, 4), (2, 4), (1, 4), (3, 4), (5, 12), (11, 12)$ can be proven to be an exact covering sequence. We shall prove the same thing with another set of congruences.

Example 0.3.1. We take the pairs $(1, 2), (0, 4), (2, 4)$. We can right away see that $\sum_j 1/b_j = 1/2 + 1/4 + 1/4 = 1$. Let us now check the divisibility conditions:

$$\begin{array}{lll} \psi_2(z) = z/2 + 1/4 + z^2/4 & \text{divisible by} & \Phi_2(z) = z + 1; \\ \psi_4(z) = 1/4 + z^2/4 & \text{divisible by} & \Phi_4(z) = z^2 + 1, \end{array}$$

therefore, by theorem 3.4, the set of congruences $\{(1, 2), (0, 4), (2, 4)\}$ is an exact covering sequence.

0.4 Square Roots of Permutations

In this section of our thesis, we shall mainly concentrate our work on the question: How many, out of the total permutations of a given set S_n have square roots? We shall also take it a little further by generalizing the idea in order to find the number of the permutations of a given set with k th roots.

0.4.1 Permutations

Definition 0.4.1. A permutation of a set A is a function $\varphi : A \rightarrow A$ that is both one to one and onto

Example 0.4.1. Let $A = \{1, 2, 3, 4, 5, 6\}$ be a set. Then $\sigma : 1 \rightarrow 3 \rightarrow 5 \rightarrow 2 \rightarrow 4 \rightarrow 6 \rightarrow 1$ is one of its permutations. Or in a more standard notation

$$\sigma = \begin{pmatrix} 1 & 3 & 5 & 2 & 4 & 6 \\ 3 & 5 & 2 & 4 & 6 & 1 \end{pmatrix} \quad (0.4.1.1)$$

A more compact way of writing (3.2.1) would be $(1\ 3\ 5\ 2\ 4\ 6\ 1)$ which is called *cycle-notation*, and since it starts and ends with the same element and goes through all of them, it says to have one **cycle**. And if we take a look at an other permutation, say

$$\tau = \begin{pmatrix} 1 & 3 & 2 & 5 & 4 & 6 \\ 3 & 1 & 5 & 4 & 2 & 6 \end{pmatrix} = (1\ 3)(2\ 5\ 4)(6),$$

we can see that it is a product of disjointed cycles, namely, $(1\ 3)$, $(2\ 5\ 4)$ and (6) .

A question rises: *How many permutations are there for a given set?* Let A be a set with n elements. The total amount of permutations the set A can have is $n!$. A quick example would be to take a look at $B = \{1, 2, 3\}$ and all its $3! = 6$ permutation which are $(1\ 2\ 3)$, $(1)(2)(3)$, $(1\ 2)(3)$, $(1)(2\ 3)$, $(1\ 3\ 2)$ and $(1\ 3)(2)$.

The multiplication of permutations is not commutative and when written in standard notation is always performed from right to left. For example, consider the permutations

$$\sigma = \begin{pmatrix} 1 & 3 & 5 & 2 & 4 & 6 \\ 3 & 5 & 2 & 4 & 6 & 1 \end{pmatrix}, \text{ and } \tau = \begin{pmatrix} 1 & 6 & 2 & 5 & 3 & 4 \\ 6 & 2 & 5 & 3 & 4 & 1 \end{pmatrix},$$

then,

$$\sigma\tau = (1)(2)(3)(4)(5)(6), \text{ and } \tau\sigma = (142)(3)(5)(6),$$

for example, $\sigma\tau(4) = \sigma(\tau(4)) = 3 \neq 2 = \tau(\sigma(4)) = \tau\sigma(4)$

0.4.2 The Cyclic Index of the Symmetric Group

In this subsection we are going to take a look at detailed information about the cycles of a permutation. Let us first take a look at *Stirling numbers of the first kind*.

Stirling Numbers of the First Kind, the *unsigned* Stirling numbers of the first kind, or Stirling cycle numbers, is the number of permutations of a set of n elements with precisely k cycles. The most common notation for Stirling numbers of first kind is $c(n, k)$.

Example 0.4.2. Let $A = \{1, 2, 3, 4\}$, then, $c_A(4, 2)$ is the number of the partitions of A into two cycles which are

$$(1)(2\ 4\ 3), \quad (1\ 2\ 3)(4), \quad (1\ 2\ 4)(3), \quad (1\ 4\ 2)(3), \quad (1\ 4)(2\ 3), \quad (1\ 3)(2\ 4), \\ (1)(2\ 3\ 4), \quad (1\ 3\ 2)(4), \quad (1\ 4\ 3)(2), \quad (1\ 3\ 4)(2), \quad (1\ 2)(3\ 4).$$

Now we are going to take this a little further and instead of considering only the numbers of the cycles of a permutation, we shall try to find the numbers of the cycles with respect to their lengths.

Let $\mathbf{a} = \{a_1, a_2, a_3, \dots\}$ be a sequence of positive integers. $n = a_1 + 2a_2 + 3a_3 + \dots$ being finite, represents the cycles of different length which the permutations of n letters can have. For instance, $a_3 = 5$ means that n has exactly 5 cycles of length 3. Let us call $\mathbf{a} = \mathbf{a}(\sigma)$ the *cycle type* of the permutation σ which tell us the number of cycles of different length that σ can take on. Now let $c(\mathbf{a}(\sigma))$ be the number of permutations of cycle type \mathbf{a} . Then we call

$$\phi_n(\mathbf{x}) = \sum_{\substack{a_1+2a_2+\dots=n \\ a_1 \geq 0, a_2 \geq 0, \dots}} c(\mathbf{a}) \mathbf{x}^{\mathbf{a}}, \quad (0.4.2.1)$$

the *cycle index of the symmetric group* S_n , where $\mathbf{x}^{\mathbf{a}} = \prod_{j=1}^n x_j^{a_j}$, is the *cycle index monomial* of the permutation σ . These monomials $\mathbf{x}^{\mathbf{a}}$, are just dummy variables and have the purpose of showing the cycle structure of a permutation.

We need to find the number of permutations of n letters with the cycle type $\mathbf{a} = \{a_1, a_2, a_3, \dots\}$, and the coefficient of $\mathbf{x}^{\mathbf{a}}$ in $\phi_n(\mathbf{x})$ will provide us with just that. We are going to find the generating function

$$C(\mathbf{x}, t) = \sum_{n=1}^{\infty} \phi_n(\mathbf{x}) \frac{t^n}{n!}.$$

We begin by finding an exact formula for $c(\mathbf{a})$.

Lemma 0.4.1. *Let m , a and k be integers. The number of the ways that we can choose ka elements from m distinct elements and arrange them into a cycles of length k is*

$$f(m, a, k) = \frac{m!}{(m - ka)! k^a a!}.$$

Proof. We begin by choosing a ka -tuple from the set with m letters, which can be done in $m!/(m - ka)!$ different ways. There are k ways where k letters can be arranged in a cycle retaining same permutational equality. And if we have a numbers of cycles of the length k , then there will be k^a arrangements with same permutational equality. We also know that there are $a!$ ways we can arrange a cycles in a row. Therefore, in $m!/(m - ka)!$, there are $k^a a!$ arrangements with same permutational equality. \square

So according to Lemma (4.1) if we have n elements and a sequence of non-negative integers $\mathbf{a} = \{a_1, a_2, a_3, \dots\}$ so that $n = a_1 + 2a_2 + 3a_3 + \dots$, then,

$$\begin{aligned} & f(n, a_1, 1) f(n - a_1, a_2, 2) f(n - a_1 - 2a_2, a_3, 3) \dots = \\ & = \left(\frac{n!}{(n - a_1)! 1^{a_1} a_1!} \right) \left(\frac{(n - a_1)!}{(n - a_1 - 2a_2)! 2^{a_2} a_2!} \right) \dots = \\ & = \frac{n!}{a_1! a_2! a_3! \dots 1^{a_1} 2^{a_2} 3^{a_3} \dots}, \end{aligned}$$

is the number of ways we can form the elements in n into a_1 cycles of length 1, a_2 cycles of length 2, ..., and so on and so forth.

Theorem 0.4.1. *Let $\mathbf{a} = \{a_1, a_2, a_3, \dots\}$ be a sequence of non-negative integers such that $\sum_j j a_j = n$. Then, the number of permutations of n elements with \mathbf{a} as the type of cycle is*

$$c(\mathbf{a}) = \frac{n!}{\prod_{j \geq 1} a_j! j^{a_j}}.$$

Continuing our search for the generating function, we calculate

$$\begin{aligned}
C(\mathbf{x}, t) &= \sum_{n \geq 0} \phi_n(\mathbf{x}) \frac{t^n}{n!} \\
&= \sum_{n \geq 0} t^n \sum_{\substack{a_1+2a_2+\dots=n \\ a_1 \geq 0, a_2 \geq 0, \dots}} \frac{x_1^{a_1} x_2^{a_2} x_3^{a_3} \dots}{a_1! a_2! a_3! \dots 1^{a_1} 2^{a_2} 3^{a_3} \dots} \\
&= \left(\sum_{a_1 \geq 0} \frac{(tx_1)^{a_1}}{1^{a_1} a_1!} \right) \left(\sum_{a_2 \geq 0} \frac{(t^2 x_2)^{a_2}}{2^{a_2} a_2!} \right) \left(\sum_{a_3 \geq 0} \frac{(t^3 x_3)^{a_3}}{3^{a_3} a_3!} \right) \dots \\
&= e^{tx_1} e^{t^2 x_2/2} e^{t^3 x_3/3} \dots \\
&= \exp \left(\sum_{j \geq 1} \frac{x_j t^j}{j} \right)
\end{aligned}$$

Theorem 0.4.2. *The coefficient of $t^n/n!$ in*

$$C(\mathbf{x}, t) = \exp \left(\sum_{j \geq 1} \frac{x_j t^j}{j} \right)$$

is the cycle index of S_n , which represents the number of permutations of n letters with all possible cycle index monomials. And the coefficient of $\mathbf{x}^{\mathbf{a}} t^n/n!$ is the number of permutations of n elements with cycle type \mathbf{a} .

0.4.3 Square Roots

Theorem 0.4.3. *A permutation σ has square roots if and only if the numbers of cycles of σ that have each even length are even numbers.*

Proof. we divide the cycles that a given permutation σ is composed of i four different groups.

- 1 Even numbers of cycles with each odd length.
- 2 Odd numbers of cycles with each odd length.
- 3 Even numbers of cycles with each even length.
- 4 Odd numbers of cycles with each even length.

Now if σ has a square root then there exists a permutation τ such that $\sigma = \tau^2$. Let us now take a look at the cycles of τ a see what happens when we square it.

$$\begin{array}{ll}
(a_1 b_1 a_2 b_2 \dots a_m b_m), & \xrightarrow{()^2} (a_1 a_2 \dots a_m)(b_1 b_2 \dots b_m), \\
(d_1 d_3 \dots d_m d_2 d_4 \dots d_{m-1}), & \xrightarrow{()^2} (d_1 d_2 d_3 \dots d_{m-1} d_m), \\
\text{no such cycle ,} & \xrightarrow{()^2} (c_1 c_2 \dots c_{m-1} c_m \dots c_{2m}).
\end{array}$$

This tells us that the only time a permutation can't have square roots is when it contains odd numbers of a cycle with each even length. In other words, a permutations that is composed of the first three group mentioned above has square roots. And since the numbers of the cycles with each odd length are arbitrary, we say that a permutation σ has square roots if and only if the numbers of cycles of σ that have each even length are even numbers

□

We need now to find the generating function of the sequence

$$\{f(1, 2), f(2, 2), f(3, 2), f(4, 2), \dots\}$$

where $f(n, 2)$ represents the number of the permutations of n elements that have square roots. As we have mentioned before, a cycle type vector, $\mathbf{a} = \{a_1, a_2, a_3, \dots\}$ of a permutation with square roots must have even numbers of even-indexed components, and the odd-indexed components are arbitrary. Now, according Theorem 4.2, number of the permutations of n elements with cycle type $\mathbf{a} = \{a_1, a_2, a_3, \dots\}$ can easily be obtained by calculating the coefficient of $\mathbf{x}^{\mathbf{a}} t^n / n!$ in the product

$$e^{tx_1} e^{t^2 x_2 / 2} e^{t^3 x_3 / 3} \dots$$

We start by dividing $C(\mathbf{x}, t)$ in two parts. The first part, $e^{tx_1} e^{t^3 x_3 / 3} \dots$, which contains only cycles with odd number of letters - and have been proved to have a square root regardless of the number of cycles - will remain untouched. The second part however, $e^{t^2 x_2 / 2} e^{t^4 x_4 / 4} \dots$, with cycles containing even number of elements must be rewritten. Here we only need to keep the even-indexed cycles that come in even numbers, and for achieving that, we will turn to hyperbolic cosine function. So instead of using the whole exponential series $e^{x_i t^i / i} = 1 + t^i x_i / i + t^{2i} x_i^2 / 2i^2 + t^{3i} x_i^3 / 6i^3 \dots$, where $i = 2, 4, 6, \dots$, we use

$$\cosh(x_i t^i / i) = \sum_{k=0}^{\infty} \frac{t^{2ki} x_i^{2k}}{i^{2k} (2k)!}, \quad i = 2, 4, 6, \dots$$

Then, by knowing $f(n, 2)$ is the number of permutations of n elements with square roots, we can construct a new generating function that will provide us with that very sequence of numbers we are looking for. This new generating function shall only contain the cycle index monomials of permutations that have square roots. And since it is the total number of those monomials for each n that is important, we can neglect all x_j by letting $x_j = 1$ for all j 's. Then we shall have

$$\begin{aligned}
\sum_{n \geq 0} f(n, 2) \frac{t^n}{n!} &= e^t \cosh(t^2/2) e^{t^3/3} \cosh(t^4/4) e^{t^5/5} \cosh(t^6/6) \dots \\
&= \exp\left(t + \frac{t^3}{3} + \frac{t^5}{5} + \dots\right) \prod_{m \geq 1} \cosh\left(\frac{t^{2m}}{2m}\right) \\
&= \exp\left(\frac{1}{2}(\log(1+t) - \log(1-t))\right) \prod_{m \geq 1} \cosh\left(\frac{t^{2m}}{2m}\right) \\
&= \exp\left(\log \sqrt{\frac{1+t}{1-t}}\right) \prod_{m \geq 1} \cosh\left(\frac{t^{2m}}{2m}\right) \\
&= \sqrt{\frac{1+t}{1-t}} \prod_{m \geq 1} \cosh\left(\frac{t^{2m}}{2m}\right) \\
&= 1 + t + \frac{t^2}{2!} + 3\frac{t^3}{3!} + 12\frac{t^4}{4!} + 60\frac{t^5}{5!} + 270\frac{t^6}{6!} + \dots
\end{aligned}$$

Therefore the sequence $\{f(n, 2)\}$ begins with 1, 1, 1, 3, 12, 60, 270, ...

Now that we have explained how to find the number of permutations with square roots, it would be good time to go a little further and try to generalize the idea and find a way which would lead us to the number of k th roots of a given permutation.

We let $f(n, k)$ be the number of permutation with n letters which has the j th roots, and we seek the exponential generating function for the sequence $\{f(n, k)\}_{n \geq 0}$. We start with some new notations. If p is a prime and k is an integer, then, by $e(p, k)$ we mean $\max\{j\}$, where $p^j | k$. Then, for each pair of positive integers m and k , we define $((m, k))$ as

$$((m, k)) = \prod_{p|m} p^{e(p, k)}.$$

Now to the main theorem which is the generalization of Theorem 4.3.

Theorem 0.4.4. *A permutation σ has k th roots if and only if for every m , where $m \in \mathbb{Z}^+$, the number of the cycles of σ with length m is a multiple of $((m, k))$.*

Proof. We let $\sigma = \tau^k$ be a permutation of a set with n letters. Suppose now, that σ has exactly ν_m cycles with the length m , for $m = 1, 2, 3, \dots$. Then we consider that there is a cycle of the length r in τ . In τ , this would contribute to $\gcd(r, k)$ cycles of length $r/\gcd(r, k)$ in σ . Therefore the ν_m cycles of length m in σ must come from cycles of length r in τ , where $r/\gcd(r, k) = m$. If we now take a look at the equation $r = \gcd(r, k)m$, we will see that r must be a multiple of $m((m, k))$. Thus, all the cycles of the length m in σ must come from cycles of lengths that are multiples of $m((m, k))$ in τ . Conversely, every such cycle in τ must contribute a multiple of $((m, k))$ m -cycles in σ . Therefore, the number of m -cycles in σ must be a multiple of $((m, k))$. □

Just to reduce the level of confusion, let us construct a k th root of a permutation σ that satisfies the condition. We start by fixing m and write $g = ((m, k))$. Then the number of cycles of σ with the length m is now a multiple of g , so we put them together into g cycles of length m . Now for each bundle, we construct a single new cycle of length mg by creating a cycle with mg empty places. Then, for $i, j = 1, 2, 3, \dots$, we simply place the i th element of the j th m -cycle in the $((i-1)g + j)$ th position of the new empty mg -cycle till all the elements are in their new positions. In this way we have constructed a k th root of σ .

To see even more clearly how this works, we are now going to give an example with a permutation that satisfies the condition.

Example 0.4.3. Let $\sigma = (1, 6)(5, 7)(2, 3, 8)(4, 9, 11)(10, 12, 13)$ be a given permutation. Our first step in the process would be to find out whether σ satisfies the requirements to have, say a 3rd root. Then, $\nu_2 = 2$ is a multiple of $((2, 3)) = 1$, and $\nu_3 = 3$ is a multiple of $((3, 3)) = 3$. Now we are going to construct a τ so that $\tau^3 = \sigma$. Here we have two groups of m -cycles, with $m = 2$, and $m = 3$. First we create different bundles of cycles with same m , the $\nu_m/((m, k))$ will tell us the number of the new cycles of the length $m((m, k))$, that each bundle will give rise to. If $\nu_m/((m, k))$ is the same as the number of the cycles of the bundle in question, then those cycles will remain the same in τ . In our case, $\nu_2/((2, 3)) = 2$ is the same as the number of the cycles of length 2 of the bundle in question, so first part of τ will be $(1, 6)(5, 7)$.

Now to the second bundle that contains the cycles with $m = 3$. Here $\nu_3((3, 3)) = 1$, and $3((3, 3)) = 9$, which means that this one will give rise to one cycle of length 9. We begin by constructing a cycle with nine empty places. We place the elements of the first cycle of the bundle in the positions 1, 4 and 7 (2, -, -, 3, -, -, 8, -, -), then elements of the second cycle of the bundle in positions 2, 5 and 8 (2, 4, -, 3, 9, -, 8, 11, -) and finally, the elements of the last cycle in the remaining positions (2, 4, 10, 3, 9, 12, 8, 11, 13). Combining this with the first part of τ will give us

$$\tau = (1, 6)(5, 7)(2, 4, 10, 3, 9, 12, 8, 11, 13).$$

The exponential generating function of the sequence $\{f(n, k)\}_{n \geq 0}$ can be obtained using same method as in the case of square roots. Let $\exp_q(x)$ denote the part of the exponential series of e^x that contains only powers that can be divided by q . That is,

$$\exp_q(x) = \sum_{j \geq 0} \frac{x^{jq}}{(jq)!}, \quad q = 1, 2, 3, \dots$$

In $\exp_1(x) = 1 + x + x^2/2! + x^3/3! + \dots$, all the powers of x are divisible by $q = 1$. For $\exp_2(x)$, we are going to use $\exp_2(x) = \cosh(x) = 1 + x^2/2! + x^4/4! + \dots$. How about $q = 3$? Here it gets a little tricky. We know that if a power series converges to a function, then by using roots of unity, we can pick out desired terms from that series. For example, the two *square roots of unity* will provide us with

$$\frac{1^n + (-1)^n}{2} = \begin{cases} 1, & \text{if } n \text{ even;} \\ 0, & \text{if } n \text{ odd,} \end{cases}$$

which clearly gives us even-powered terms from the series. Using same principle with cubic, quartic, quintic, ... roots of unity, will give us the necessary terms we are looking for. So for every $r > 1$, the r th roots of unity give us the generalized formula

$$\frac{1}{r} \sum_{\zeta^r=1} \zeta^n = \begin{cases} 1, & \text{if } r|n; \\ 0, & \text{otherwise.} \end{cases}$$

And naturally the left side of the expression above can be expressed as

$$\frac{1}{r} \sum_{j=0}^{r-1} e^{2\pi i j n / r}.$$

Then, the generating function for the sequence $\{f(n, k)t^n/n!\}$ is

$$\sum_{n=0}^{\infty} f(n, k) \frac{t^n}{n!} = \prod_{m=1}^{\infty} \exp_{((m, k))} \left(\frac{t^m}{m} \right), \quad (k = 1, 2, 3, \dots)$$

Here we have a table of the sequence $\{f(n, k)t^n/n!\}$, for $0 \leq n \leq 7$ and $2 \leq k \leq 6$.

$\{f(n, k)t^n/n!\}$	n=0	n=1	n=2	n=3	n=4	n=5	n=6	n=7
k=2:	1	1	3	12	60	270	1890	14280
k=3:	1	2	4	16	80	400	2800	22400
k=4:	1	1	3	9	45	225	1575	11130
k=5:	1	2	6	24	96	576	4032	32256
k=6:	1	1	1	4	40	190	1330	8680

0.5 A Short Summary and Further Horizon

We would like to conclude the work with a short summary of the previous sections. We also would like to give the readers a brief taste, of some of the many applications that generating functions have to offer. The applications that we have chosen to take up are: probability theory, generating functions proven congruence, rook theory and unimodality.

A Short Summary

Throughout this paper we have witnessed how the generating functions could help us solve some relatively difficult problems. In pursuit of finding permutation with square roots, we saw how the ordinary generating function $\phi(x) = \sum_{n \geq 0} c(n)x^n$, evolved to a "grand" exponential generating function $C(\mathbf{x}, \mathbf{t}) = \sum_{n \geq 0} \phi(\mathbf{x})t^n/n!$, from which we were able to construct a new exponential generating function

$$\sum_{n \geq 0} f(n, 2) \frac{t^n}{n!} = e^t \cosh(t^2/2) e^{t^3/3} \cosh(t^4/4) e^{t^5/5} \cosh(t^6/6) \dots$$

which gave rise to the number of the permutations with n letters that had square roots.

In finding how "exact", a covering sequence $A = \{(a_i, b_i)\}$, $i = 1, 2, \dots, k$ is, we used the ordinary generating function $\sum_{n=0}^k x^n$, and the congruence relation $n \equiv a_i \pmod{b_i}$ which equals $n = a_i + tb_i$ where $n \in \mathbb{Z}^+$, and obtained $\sum_{i=1}^k \sum_{t \geq 0} x^{a_i + tb_i}$. We performed summation over t and ended up with

$$\sum_{i=1}^k \frac{x^{a_i}}{1 - x^{b_i}} = \frac{1}{1 - x},$$

and by multiplying both sides with $(1 - x)$ and letting $x \rightarrow 1$ we arrived at the conclusion that A is an exact covering sequence if and only if $\sum_i 1/b_i = 1$.

These applications, beside being fascinating, have proven to be highly practical. But they are not all what generating functions have to offer. Taking a deeper look inside the world of generating functions we will find many ways in how they are applied on a wide range of ideas and principles.

Generating Functions and Probability Theory

The *probability mass function* $f(x)$ tells us how probable it is for the event x , which is an element from a sample space Ω , to take certain values called *random variables* X . For all $t \in \mathbb{R}$ which have expected value, a *probability generating function* $P(t)$ of X is expressed as $P_X(t) = \sum_{x=0}^{\infty} f(x)t^x$.

Now, the common way of calculating *expected value* and *variance* of X would be, $E[X] = \sum_{x \in \Omega} xf(x)$, and $\text{Var}(X) = E[(X - E[X])^2]$. We differentiate $P(t)$ with respect to t and let $t = 1$ obtaining $P'(1) = \sum_{x \geq 0} xf(x)$, and since x takes only the values from the sample space, we can write $P'(1) = \sum_{x \in \Omega} xf(x)$. Now, we can express both expected and variance of X in the terms of probability generating function $P(t)$,

$$E[X] = P'(1), \quad \text{Var}(X) = P''(1) + P'(1)[1 - P'(1)].$$

Sometimes, in order to have a better understanding of a random variable X , we need to know more than just the expected value and the variance. In those cases, we turn to the *moments* $E[X^1], E[X^2], E[X^3], \dots, E[X^k]$ of the X , where the first moment represents the expected value and the second moment is used in finding the variance of X . For calculating these moments, one uses so-called *moment generating function* denoted

$$M_X(t) = \begin{cases} \sum_{x \in \Omega} e^{tX} f_X(x), & \text{if discrete} \\ \int_{x=0}^{\infty} e^{tX} f_X(x), & \text{if continuous.} \end{cases}$$

With some algebra we easily come to the conclusion that for $t = 0$ the different order of derivatives of moment generating function corresponds to a moment with the respective order. Just to give an example, we can see that $M_X^{(1)}(0) = \sum_{x \in \Omega} xf_X(x)$, which is equal to $E[X^1]$.

Proving Congruence

This subsection consists of one example that hopefully will give the reader some understanding about how well the generating functions can help us to prove congruence among combinatorial numbers.

Example 0.5.1. We know that the Stirling numbers of the first kind $c(n, k)$, have the generating function

$$\sum_{k=0}^n c(n, k)x^k = x(x+1) \dots (x+n-1). \quad (0.5.0.1)$$

We would like to find some basis for determining the oddness/evenness of these numbers. We start by finding out what $\sum_{k=0}^n c(n, k)x^k \pmod{2}$ becomes. And since

$$(x + h) \equiv \begin{cases} x \pmod{2}, & \text{if } h \text{ even;} \\ x + 1 \pmod{2}, & \text{if } h \text{ odd,} \end{cases}$$

our (5.0.1) $\pmod{2}$ becomes

$$\begin{aligned} \sum_{k=0}^n c(n, k)x^k &\equiv x(x+1)x(x+1)\dots \pmod{2} \\ &= x^{\lceil n/2 \rceil} (x+1)^{\lfloor n/2 \rfloor}, \end{aligned}$$

where the coefficients of x^k in $x^{\lceil n/2 \rceil} (x+1)^{\lfloor n/2 \rfloor}$ is the sequence generated by $\sum_{n=0}^{\infty} c(n, k)x^k \pmod{2}$.

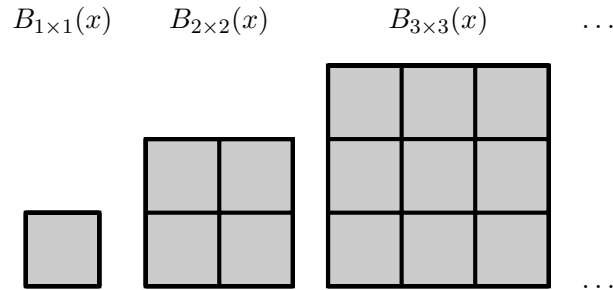
$$\begin{aligned} c(n, k) &\equiv [x^k]x^{\lceil n/2 \rceil} (x+1)^{\lfloor n/2 \rfloor} \pmod{2} \\ &= [x^{k-\lceil n/2 \rceil}] (x+1)^{\lfloor n/2 \rfloor} \\ &= \binom{\lfloor n/2 \rfloor}{k - \lceil n/2 \rceil}. \end{aligned}$$

This tells us that Stirling numbers of $c(n, k)$, and the binomial coefficient $\binom{\lfloor n/2 \rfloor}{k - \lceil n/2 \rceil}$, both have the same parity. In particular, if $k < \lceil n/2 \rceil$, then $c(n, k)$ is an even number.

Rook Polynomial

A *rook polynomial* $R_B(x) = \sum_{k=0}^{\infty} a_{B,k}x^k$, is a ordinary generating function that determines the number of the ways k non-attacking rooks - no two rooks in the same row or column - can be placed on a chess-like board $B_{m \times n}$ with $m \times n$ squares. The first few rook polynomials of a $B_{n \times n}$ boards are

$$\begin{aligned} R_{B_{1 \times 1}}(x) &= x + 1 \\ R_{B_{2 \times 2}}(x) &= 2x^2 + 4x + 1 \\ R_{B_{3 \times 3}}(x) &= 6x^3 + 18x^2 + 9x + 1 \\ R_{B_{4 \times 4}}(x) &= 24x^4 + 96x^3 + 72x^2 + 16x + 1. \end{aligned}$$



For a board $B_{m \times n}$, the general formula for calculating all the values of $a_{B,k}$ in $R_{B_{m \times n}}(x)$ would be

$$a_{B,k} = \begin{cases} \frac{m!n!}{(m-k)!(n-k)!k!}, & \text{if } k \leq \min(m, n) \\ 0, & \text{otherwise.} \end{cases}$$

These polynomials are of course for boards without any forbidden squares. For instance, a 2×2 board with one forbidden square would have the polynomial $R_{B_C}(x) = x^2 + 3x + 1$, where B_C denotes that specific board. But analysing each board that contains forbidden squares tends to be an exhausting task, specially as the size of the the boards increases.

A way of solving this problem is to divide the board C into pairwise disjoint sub-boards $C_1, C_2, C_3, \dots, C_n$, then

$$R_{B_C} = R_{B_{C_1}} + R_{B_{C_2}} + R_{B_{C_3}} + \dots + R_{B_{C_n}}.$$

As you may have realized by now, the boards and their conditions get more complicated and unfortunately we wont be able to cover all those situations here. However, for further reading we recommend John Riordan works on this subject.

Unimodality

A sequence is called *unimodal* if it has a maximum point that it rises to and then falls from. The set $\{\binom{n}{k}\}_{k=0}^n$, which contains the coefficients from a binomial expansion is an excellent example of that. In combinatorics, unimodality is common among sequences. Proving unimodality for a sequence can sometimes be a difficult task, but generating functions, although not always being the definitive method, are of great help for finding unimodality.

We need now to turn to a stronger property than unimodality, namely, *logarithmic concavity*. The sequence $c_0, c_1, c_2, \dots, c_n$ of positive numbers is called log concave if $\log c_x$ is a concave function of x . In other words

$$c_{x-1}c_{x+1} \leq c_x^2, \quad x = 1, 2, 3, \dots, n-1.$$

By replacing ' \leq ' with '<' our sequence turns from log concave to *strictly log concave*. And if a sequence of positive numbers $\{c_k\}_{k=0}^n$ is log concave, then it is also unimodal. Otherwise it would have three consecutive elements such as $c_{k-1} > c_k < c_{k+1}$ which is a contradiction to the assumption of logarithmic concavity.

Now according to the *Theorem 4.27* [1, p. 146], if all the zeros of a given polynomial $p(x) = c_0 + c_1x + \dots + c_nx^n$ are real and negative, then $p(x)$ is a generating function whose sequence of coefficients $\{c_k\}_{k=0}^n$ is strictly log concave. And as mentioned above, it is also unimodal.

Bibliography

- [1] Herbert S. Wilf, **Generatingfunctionology**, A K Peters/CRC Press, 3rd Edition.
- [2] Sergei K. Lando, **Lectures on Generating Functions**, American Mathematical Society, 2003.
- [3] Miklós Bóna, **Combinatorics of Permutations**, Chapman and Hall/CRC Press, 2nd edition.
- [4] John A. Beachy, William D. Blair, **Abstract Algebra**, Waveland Press, Inc., 3rd edition.
- [5] Håkan Lennerstad, Claes Jogr eus, **Serier och Transformer**, Studentlitteratur, 2006.
- [6] Deborah Hughes-Hallett, Andrew M. Gleason, William G. McCallum, et al., **Calculus: *Single and Multivariable***, Wiley, 6th Edition, 2012.
- [7] Richard A. Mollin, **Algebraic Number Theory**, Chapman and Hall/CRC Press, 2nd Edition, 2011.
- [8] G. H. Hardy, Edward M. Wright, **An Introduction to the Theory of Numbers** , Oxford University Press, 6th Edition, 2008.
- [9] John Riordan, **An introduction to Combinatorial Analysis**, John Wiley and Sons, INC., 1967.
- [10] Ralph P. Grimaldi, **Discrete and Combinatorial Mathematics**, Pearson/Addison Wesley, 5th Edition, 2003.
- [11] Ron L. Graham, Martin Gr otschel, L aszl  Lov asz, **Handbook of Combinatorics**, North-Holland, Amsterdam, 1995.

- [12] Allan Gut, **An Intermediate Course in Probability**, Springer; 2nd ed. 2009 edition.
- [13] J. Leños, R. Moreno and L. M. Rivera-Martínez, **On the number of m th roots of permutations**, <http://arxiv.org/pdf/1005.1531.pdf>
- [14] Yvesd Gallot, **Cyclotomic Polynomials and Prime Numbers**, <http://yves.gallot.pagesperso-orange.fr/papers/cyclotomic.pdf>
- [15] Yimin Ge, **Elementary Properties of Cyclotomic Polynomials**, http://www.yimin-ge.com/doc/cyclotomic_polynomials.pdf
- [16] Wikipedia: The Free Encyclopaedia, **Generating function**, http://en.wikipedia.org/wiki/Generating_function