Combinatorics

Three principles of combinatorics

Multiplication principle: If object A can be selected in m various ways and after each of these choices object B can be selected by n different ways, then the selection of two objects A and B in the specified order can be done in mn ways.

Addition principle: If object A can be selected in m various ways, and object B can be selected in other n various ways (provided that the simultaneous choice of A and B is impossible), then A or B can be done in $m + n$ ways.

Pigeonhole principle: If n objects are distributed over m places, and if $n > m$, then some place receives at least two objects.

Mappings and partial permutations

Let sets X and Y be given, and the set X contains n elements ($|X| = n$), and the set Y contains m elements ($|Y| = m$).

Lemma 1.

If $|X| = n$ and $|Y| = m$, then the number of all functions $f : X \to Y$ is equal to m^n.

Definitions.

- A function $f : X \to Y$ is surjective if and only if for every $y \in Y$, there is at least one $x \in X$ such that $f(x) = y$ (i.e., f(X) = Y).
- A function $f : X \to Y$ is injective if and only if whenever $f(x) = f(y)$, $x = y$.
- A function $f : X \to Y$ is bijective if it is a one-to-one correspondence between those sets, in other words both injective and surjective.
- If $x \in \mathbb{R}$, then we denote $[x]_n = x(x-1)\dots(x-n+1)$.

Definition. Let $f : X \to Y$. A function $g : Y \to X$ is the inverse of f if $f \circ g = 1_Y$ and $g \circ f = 1_X$ (such function g is denoted as f^{-1}).

Proposition 2.

A function $f : X \to Y$ is bijective if and only if it is invertible.

Lemma 3.

The total number of injective mappings from a finite set X with n elements to set Y with m elements is $[m]_n$.
(Equivalent statement. Number of words of length n without repetition of letters in the alphabet with m letters is $[m]_n$).

Combinations, partial permutations and permutations

Let $A = \{a_1, \ldots, a_n\}$ be a set of n objects.

Definitions.

- An arbitrary ordered set (tuple) of k elements of a given set, among which there may be duplicates, is called a partial permutation of length k from n-set with repetition (denoted as $\tilde{A}_n^k$). 从n个中取k个进行排列 $\tilde{A}_n^k = n^k$
- Accordingly, if the elements cannot be repeated, then the set is called an partial permutation of length k from n-set (denoted as A_n^k). Extremely important particular case $k = n$, such partial permutationss are called permutations. (排列) $A_n^k = \frac{n!}{(n-k)!}$
- A combination of n elements by k is a set of k elements of this set. Sets that differ only in the order of elements are considered the same (denoted as C_n^k or $\binom{n}{k}$). $C_n^k = \frac{n!}{k!(n-k)!}$
- Combinations with repetitions are defined similarly (denoted as $\tilde{C}_n^k$). $\tilde{C}_n^k = C_{n+k-1}^k = C_{n+k-1}^{n-1}$

Proposition 5.

i) $C_n^k = C_n^{n-k}$
ii) $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$
iii) $C_n^0 + C_n^1 + \ldots + C_n^n = 2^n$
iv) $(C_n^0)^2 + (C_n^1)^2 + \ldots + (C_n^n)^2 = C_{2n}^n$

Theorem 6 (Binomial formula).

$$(x+y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

Let us show the fourth equality. Fix some combination with repetitions $(a_1, \ldots, a_n)$. We now construct a sequence of 0 and 1 according to the following rule: first, write 1 as many times as the element a_1 occurs in combination. After that, we put 0 and write 1 as many times as a_2 occurs in combination and so on. At the end of the sequence, there will be 1 as many times as a_n occurs in the combination and we will not put 0 at the end. It is easy to understand that according to the described algorithm, two identical sequences of 0 and 1 are obtained only for the same combinations. Note that in each such sequence exactly k ones and $n-1$ zeroes. Hence, the mapping described above is a bijection between k-combinations with repetitions and sequences of 0 and 1 of length $n+k-1$ and containing exactly k ones. There are exactly C_{n+k-1}^k such sequences.■

1,1...1 0 1...1 0 ... 0 1...1
a_1个 a_2个 a_n个
0有n-1个. 0+1个 n+k-1个
组合0的位置即可
若$a_1 \ldots a_n$中有未出现的, 则两个0相邻

一种严格有序的写具体排列方法

We're going to introduce a more efficient way of writing permutations. This involves thinking about a special kind of permutation called a cycle. Let $m > 0$, let $a_0, a_1, \ldots, a_{m-1}$ be distinct positive integers. Then $\tau := (a_0, a_1, \ldots, a_{m-1})$ is defined to be the permutation (in S_n) such that

- $\tau(a_i) = a_{i+1}$ for $i < m-1$
- $\tau(a_{m-1}) = a_0$ 位置
- $\tau(x) = x$ for any number x which isn't equal to one of the a_i.

A permutation of the form $(a_0, a_1, \ldots, a_{m-1})$ is called an m-cycle. A permutation which is an m-cycle for some is called a cycle.

Here we have $(a_1 \ldots a_n)^n = Id$.

In general, every $m-$cycle can be written m different ways since you can put any one of the m things in the cycle first. cycle 内可以任意循环换序.

Definition. Two cycles $(a_0, a_1, \ldots, a_{m-1})$ and $(b_0, b_1, \ldots, b_{k-1})$ are disjoint if no a_i equals any b_j .

One reason disjoint cycles are important is that disjoint cycles commute, that is, if σ and τ are disjoint cycles then, $\sigma \circ \tau = \tau \circ \sigma$

1.Cycle是映射，可视为一种运算符，是对给定排列集的运算（排列本身是一个双射）
2.多个cycle时，从右到左 对着数进行（不是对位置进行）
3.cycle相等是对运算（映射）相等 不是数相等

e.g. $\sigma = (a,b,c)$ $\sigma^2 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = (a,c,b)$
$\sigma^3(a) = \sigma(b) = c$
$\sigma^3(b) = \sigma(c) = a$
$\sigma^3(c) = \sigma(a) = b$

a → b → c → a

inverse

For every permutation π there is an inverse permutation π^{-1} such that $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = Id$. How do we find the inverse of a cycle? Let $\sigma = (a_0, a_1, \ldots, a_m)$, then σ^{-1} sends a_i to a_{i+1} for all i (and every number not equal to an a_i to itself).
In other words, σ^{-1} is the cycle $(a_{m-1}, a_{m-2}, \ldots, a_0)$.

Lemma 7.

Let $a_0, \ldots, a_m$ be distinct numbers. Then

此处是定义了一种运算, 从右至左.

$$(a_0, a_1)(a_1, a_2, \ldots, a_m) = (a_0, a_1, \ldots, a_m)$$

后数换, 是 → → →

Theorem 8.

Every $\sigma \in S_n$ equals a product of disjoint cycles.

排列.

e.g. $\sigma = (a_1, \ldots a_n) = (a_1 \ldots a_{k-1})(a_k, a_{k+1} \ldots a_n)$ where a_i are distinct.

Example.

1 ↷ 7, 4 ↶ ; 2 ↷ 5, 6 ↶ ; 3

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

$\sigma = (1,7,4)(2,6,5)(3)$ Since any 1-cycle is equal to the identity function, and because 1-cycles look confusingly like what we write when we evaluate a function, we usually omit 1-cycles like (3) from disjoint cycle decompositions, so we'd write the permutation σ of the previous example as $(1,7,4)(2,6,5)$.

$|\{\sigma \in S_n \mid \sigma = (j_1 \ldots j_{k_1})(\ldots)(i_1 j_{s_1} \ldots i_{j_{s+1}})\}| = \frac{n!}{k_1 \cdot k_2 \cdots k_s}$
n element

Definition. A transposition is a 2-cycle. (i.e., of the form (i, j) .) $i \rightleftarrows j$ 1-cycle is an identical map

Lemma 9.

Every cycle equals a product of transpositions.

Theorem 10.

Every permutation in S_n is equal to a product of transpositions.

Polynomial formula

Assume that we have n_1 objects of the form a_1, n_2 objects of the form a_2, ... , n_k objects of the form a_k. Let $n := n_1 + \ldots + n_k$. Denote by $P(n_1, \ldots, n_k)$ is the number of all possible permutations that can be obtained from these n objects. Arguing as in a problem with a word Combinatorics, we get that the following theorem is true:

Theorem 1.

$P(n_1, \ldots, n_k) = C_n^{n_1} C_{n-n_1}^{n_2} \ldots C_{n-n_1-\ldots-n_{k-1}}^{n_k} = \frac{n!}{n_1! n_2! \ldots n_k!}$

Corollary 2 (Polynomial formula aka Multinomial Theorem).

$(x_1 + \ldots + x_k)^n = \sum_{\substack{(n_1,\ldots,n_k) \\ n_1+\ldots+n_k=n}} P(n_1, \ldots, n_k) x_1^{n_1} \ldots x_k^{n_k}$

Corollary 3.

$k^n = \sum_{\substack{(n_1,\ldots,n_k) \\ n_1+\ldots+n_k=n}} P(n_1, \ldots, n_k)$

Corollary 4.

$C_{n+m}^n = C_{n+m-1}^{n-1} + C_{n+m-2}^{n-1} + \ldots + C_{n-1}^{n-1}$

Lemma 5.

For all $n \geq 1, 0 \leq k \leq n$, we have $C_n^k \leq \frac{n^n}{k^k (n-k)^{n-k}}$

Proposition 6.

For all $k \geq 2$ and $n_1, \ldots, n_k \geq 0$, such that $n_1 + \ldots + n_k = n$ we have $P(n_1, \ldots, n_k) \leq \frac{n^n}{n_1^{n_1} \ldots n_k^{n_k}}$

In 1928 Emanuel Sperner asked and answered the following question: Suppose we are given the set $N = \{1, 2, \ldots, n\}$. Call a family $\mathcal{F}$ of subsets of N an antichain if no set of $\mathcal{F}$ contains another set of the family $\mathcal{F}$. What is the size of a largest antichain? → 可相交，但不能包含.

Clearly, the family $\mathcal{F}_k$ of all k-sets (k个元素) satisfies the antichain property with $|\mathcal{F}_k| = C_n^k$. Looking at the maximum of the binomial coefficients as above we conclude that there is an antichain of size $C_n^{\lfloor \frac{n}{2} \rfloor} = max_k C_n^k$. (组合的集合中有 C_n^k 个元素)

Theorem 7.

The size of a largest antichain of an n−set is $C_n^{\lfloor \frac{n}{2} \rfloor}$.

Inclusion–exclusion principle

$$|A \cup B| = |A| + |B| - |A \cap B| \quad \text{(can be extended to n sets)}$$

Theorem 1 (Inclusion–exclusion principle)

For any collection of finite sets $A_1, A_2, \ldots, A_n$, we have

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\varnothing \neq I \subset \{1,2,\ldots,n\}} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right|$$

For each set A_i, define the characteristic function $\chi_i(x) = \begin{cases} 1 & x \in A_i \\ 0 & x \notin A_i \end{cases}$

formula $\Xi(x) = \prod_{i=1}^{n} (1 - \chi_i(x))$ $\quad \sum_{x \in X} \Xi(x) = \left| X \setminus \bigcup_{i=1}^{n} A_i \right|$

$= \sum_{I \subset \{1,\ldots,n\}} (-1)^{|I|} \prod_{i \in I} \chi_i(x)$ → characteristic function of $\bigcap_{i \in I} A_i$

Derangement

Example II (Derangements). How many ways can n items be permuted so that none of the items are in their original position? Such permutations are called derangements.

$$D_n = F_\varnothing - F_{\{1\}} - \ldots - F_{\{n\}} +$$
$$+ F_{\{1,2\}} + F_{\{1,3\}} + \ldots + F_{\{n-1,n\}} - \ldots + (-1)^n F_{\{1,2,\ldots,n-1,n\}} =$$
$$= n! - C_n^1(n-1)! + C_n^2(n-2)! - C_n^3(n-3)! + \ldots + C_n^n(-1)^n =$$
$$= n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{n!}{n!}\right) =$$
$$= n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}$$

Alternative

Alternative form of inclusion-exclusion

Suppose there is a set of N elements and some "properties" $P_1, \ldots, P_n$.

Let also $N(P_i)$ denote the number of objects that satisfy the property P_i, $N(P_iP_j)$ – that simultaneously satisfy both properties P_i, P_j and so on.

Set $N(P_1'P_2' \ldots P_n')$ denote the number of elements that have none of the properties $P_1, \ldots, P_n$.

Then we will have:

$$N(P_1'P_2' \ldots P_n') = N - N(P_1) - \ldots N(P_n) +$$
$$+ N(P_1P_2) + \ldots N(P_{n-1}P_n) - \ldots + (-1)^n N(P_1P_2 \ldots P_n)$$

— There are $n!$ permutations of n elements.
— There are $(n-1)!$ permutations where element i stays in its original position (and some other elements might, but don't have to).
— There are $(n-2)!$ where any two elements stay in their original position (again with maybe some others staying).
— And so on: $(n-k)!$ ways to permute where a specific k elements stay in their original positions.
— Let's use F_I to denote the number of permutations where the elements of I are fixed (for example, $F_{\{1\}} = (n-1)!$ as we said above).

Example VIII (**Euler's function.**) → 与n互质的数的数量.
Let $\phi(n)$ be the number of positive integers $x \leq n$ which are mutually prime to n i.e. have no common factors with n, other than 1 (i.e. $\phi(n) := |\{x \in \{1, 2, \ldots, n\} | gcd(x, n) = 1\}|$)

Let n be any positive integer, and let $p_1, p_2, \ldots, p_t$ be the prime divisors of n. Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_t}\right)$$

Remark. The formula above can be rewritten into the following possibly more friendly form. Let $n = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t}$ be the prime factorisation of n. Then

$$\phi(n) = p_1^{a_1-1}(p_1 - 1)p_2^{a_2-1}(p_2 - 1) \ldots p_t^{a_t-1}(p_t - 1)$$

Euler's thm. $a^{\varphi(n)} \equiv 1 \pmod{n}$, $gcd(a, n) = 1$

Let $\mu(n)$ be the **Möbius function** defined for $n \in \mathbb{N}$ by:

squarefree

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{if } n \text{ is not squarefree} \\ (-1)^s & \text{if } n = p_1 \cdots p_s \text{ is the product of } s \text{ distinct primes.} \end{cases}$$

$n = p_1^{i_1} \cdots p_s^{i_s}$, $i_j \le 1$

Lemma 1.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n \ge 2 \end{cases}$$

$\sum_{d|n} \mu(d) = [\frac{1}{n}]$

Definition. An arithmetic function f is called multiplicative if $f(mn) = f(m)f(n)$ where m and n are relatively prime positive integers.

Proposition 2.

The function $\mu(n)$ is multiplicative.

Theorem 3 (Möbius Inversion Formula).

If g is any arithmetic function and $f(n) = \sum_{d|n} g(d)$, then $g(n) = \sum_{d|n} f(d)\mu(\frac{n}{d}) = \sum_{d|n} \mu(d) f(\frac{n}{d})$

Proposition 4.

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

$$\phi(n) = \sum_{k=1}^{n} \lfloor \frac{1}{gcd(n,k)} \rfloor = \sum_{k=1}^{n} \Big(\sum_{d|gcd(n,k)} \mu(d) \Big) = \sum_{k=1}^{n} \sum_{d|n, d|k} \mu(d) = \sum_{d|n} \sum_{q=1}^{\frac{n}{d}} \mu(d) = \sum_{d|n} \mu(d) \Big(\sum_{q=1}^{\frac{n}{d}} 1 \Big) = \sum_{d|n} \mu(d)\frac{n}{d}$$

Enumeration of cyclic sequences

Let the set $X = \{b_1, \ldots, b_r\}$ be an alphabet, and make a directed cycle from its letters. We want to find $T_r(n)$ – number of all possible cyclic words of length n composed of arbitrary letters (with repeats) from the alphabet X.

Solution: We call the period of a cyclic word $mind \ge 1$ such that after d cyclic shifts by 1 symbol, the word goes into itself.

Lemma A. Any period d divides n.

lemma的具象解释.

Observation. Any cyclic sequence of length n and period d has the form $A = a_1 \ldots a_d a_1 \ldots a_d a_1 \ldots a_d$, i.e. consists of $\frac{n}{d}$ repeating blocks of length d — ehit follows from the previous lemma and the fact that after d shifts, the letter a_i goes into a_{d+i}.

Möbius function of a poset

Let P be a poset. We define a map $\mu : P \times P \to \mathbb{Z}$ by induction.

$$\mu(x,x) = 1, \text{ for all } x \in P$$

$$\mu(x,y) = -\sum_{x \le z < y} \mu(x,z), \text{ for all } x < y \text{ in } P$$

Proposition 5.

Let P be a finite poset. (In fact this Proposition holds in more generality but we will not need this.) Let $f, g : P \to \mathbb{C}$. Then $g(x) = \sum_{y \ge x} f(y)$ for all $x \in P$ if and only if $f(x) = \sum_{y \ge x} g(y)\mu(x,y)$ for all $x \in P$.

Proposition 6.

Let P and Q be finite posets, and let $P \times Q$ be their direct product. If $(x,y) \le (x',y')$ in $P \times Q$, then

$$\mu_{P\times Q}((x,y),(x',y')) = \mu_P(x,x')\mu_Q(y,y').$$

Gauss's formula

Let $\mathbb{F}_q$ denote the finite field of q elements. Then in general, the number of monic irreducible polynomials of degree n over the finite field $\mathbb{F}_q$ is given by Gauss's formula

$$M(q,n) := \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) q^d$$

Estimates for n!

Proposition 1.

If $n \ge 6$

$$\left(\frac{n}{3}\right)^n \le n! \le \left(\frac{n}{2}\right)^n$$

Proposition 2.

If $n \ge 1$

$$e\left(\frac{n}{e}\right)^n \le n! \le ne\left(\frac{n}{e}\right)^n$$

Lemma 3.

If $k \ge 2$,

$$\int_{k-1}^{k} ln(x)dx + ln(\frac{2k}{2k-1}) \le ln(k) \le \int_{k-1}^{k} ln(x)dx + \frac{1}{2}ln(\frac{k}{k-1})$$

Proposition 4.

$$\frac{4}{5}e\sqrt{n}\left(\frac{n}{e}\right)^n \leq n! \leq e\sqrt{n}\left(\frac{n}{e}\right)^n$$

Lemma 5.

$$\int_0^{\frac{\pi}{2}} sin^{2n}(x)dx = \frac{(2n-1)(2n-3)\ldots 3\cdot 1}{2n(2n-2)\ldots 4\cdot 2}\frac{\pi}{2}$$

$$\int_0^{\frac{\pi}{2}} sin^{2n+1}(x)dx = \frac{2n(2n-2)\ldots 4\cdot 2}{(2n+1)(2n-1)\ldots 3\cdot 1}$$

Lemma 6.

$$\frac{2^{2n}}{\sqrt{\pi n}}e^{-1/4n} \leq C_{2n}^n \leq \frac{2^{2n}}{\sqrt{\pi n}}$$

Theorem 7.

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{-1/4n} \leq n! \leq \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{1/4n}$$

Corollary 8 (Stirling's formula).

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n (1+o(1))$$

Let $n \to \infty$ and $k = o(n^{2/3})$, then

$$C_n^k = \frac{n^k e^{\frac{-k^2}{2n}}}{k!}(1+o(1))$$

Proposition 9.

For all integers n and k such that $n \geq k \geq 1$, we have that

$$\left(\frac{n}{k}\right)^k \leq C_n^k$$

Lemma 10.

Fix integers n and k such that $n \geq k \geq 1$. Then for all real numbers x such that $0 < x \leq 1$, we have that

$$\sum_{i=0}^{k} C_n^i \leq \frac{(1+x)^n}{x^k}.$$

Proposition 11.

For all integers n and k such that $n \geq k \geq 1$, we have that:

$$\sum_{i=0}^{k} C_n^i \leq \left(\frac{en}{k}\right)^k$$

Random walks

Consider the set of integers $\mathbb{Z}$. We begin our walk at 0, and at each step we move at random either one step to the left or one step to the right.

the probability of returning to the origin after exactly $2m$ steps

$$\frac{C_{2m}^m}{2^{2m}}.$$

(回原点的概率)

Generating functions (For enumeration problem 枚举问题)

Definition.

Let $(a_n)_{n\geq 0}$ be a sequence of numbers. The generating function associated to this sequence is the series $F(x) = \sum_{n=0}^{\infty} a_n x^n$

- Differentiate $F(x)$ term-wise
  $F'(x) = \sum_{n=0}^{\infty} (n+1)a_{n+1}x^n$
- Multiply $F(x)$ by a scalar $\lambda \in \mathbb{R}$ term-wise
  $\lambda F(x) = \sum_{n=0}^{\infty} \lambda a_n x^n$
- $F(x) + G(x) = \sum_{n=0}^{\infty} (a_n + b_n)x^n$
- $F(x) \cdot G(x) = \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) x^n$

Example 1

Binomial formula shows that $(1+x)^n$ is the generating function for the sequence (a_k) with $a_k = C_n^k$.

Definition (Binomial Coefficients for Real Numbers). Recall that for $n, k \in \mathbb{N}$ we have: $C_n^k = \frac{n(n-1)\ldots(n-k+1)}{k!}$.

It does not make sense to talk about permutations of sets of size $n \in \mathbb{R}$ and it is unclear what $n!$ should be, but the formula above is well-defined for general $n \in \mathbb{R}$. With this in mind, we define $p(n,k) := n(n-1)\ldots(n-k+1)$ and $C_n^k := \frac{p(n,k)}{k!}$.

Additionally we have

$$p(n,k) = (n-k+1)p(n,k-1) = np(n-1,k-1)$$

Lemma A. For any integer $n \geq 1$ we have

$$C_{\frac{1}{2}}^n = (-1)^{n+1} C_{2n-2}^{n-1} \frac{1}{2^{2n-1} \cdot n}$$

Corollary.

$$\sqrt{1+x} = \sum_{n=0}^{\infty} C_{\frac{1}{2}}^n x^n = 1 + \sum_{n=1}^{\infty} -2C_{2n-2}^{n-1}(-1)^n \frac{1}{2^{2n}n} x^n$$

We are now able to find the coefficients of the generating function for Catalan's numbers $F(x)$:

$$F(x) = \frac{1-\sqrt{1-4x}}{2x} = \frac{1}{2x} \sum_{n=1}^{\infty} 2C_{2n-2}^{n-1}(-1)^n \frac{1}{2^{2n}n}(-4x)^n =$$

$$= \frac{1}{x} \sum_{n=1}^{\infty} C_{2n-2}^{n-1} \frac{1}{n} x^n = \sum_{n=0}^{\infty} C_{2n}^n \frac{1}{n+1} x^n$$

Finally, we get the Catalan numbers $\mathfrak{C}_n = C_{2n}^n \frac{1}{n+1}$.

Fibonacci numbers

The famous Fibonacci sequence is defined by its initial terms $f_0 = f_1 = 1$ and the relation

$$f_{n+2} = f_{n+1} + f_n.$$

To derive the generating function formula

$$Fib(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \dots$$

$$(x + x^2)Fib(x) = Fib(x) - 1 \quad \Longrightarrow \quad Fib(x) = \frac{1}{1 - x - x^2}$$

$$\frac{1}{1 - x - x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{x - x_1} + \frac{1}{x - x_2}\right) = \frac{1}{\sqrt{5}}\left(\frac{1}{x_1(1 - \frac{x}{x_1})} + \frac{1}{x_2(1 - \frac{x}{x_2})}\right)$$

$x_1 = \frac{-1+\sqrt{5}}{2}$, $x_2 = \frac{-1-\sqrt{5}}{2}$ - roots of the equation $1 - x - x^2 = 0$.
From this we immediately obtain

$$Fib(x) = \frac{1}{\sqrt{5}x_1}\left(1 + \frac{x}{x_1} + \frac{x^2}{x_1^2} + \dots\right) - \frac{1}{\sqrt{5}x_2}\left(1 + \frac{x}{x_2} + \frac{x^2}{x_2^2} + \dots\right)$$

Therefore

$$f_n = \frac{1}{\sqrt{5}}(x_1^{-1-n} - x_2^{-1-n}) = \frac{(-1)^n}{\sqrt{5}}(x_1^{n+1} - x_2^{n+1}) =$$

$$= \frac{(-1)^n}{\sqrt{5}}\left(\left(\frac{-1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{-1-\sqrt{5}}{2}\right)^{n+1}\right)$$

More algebraic operations

Let $A(s) = a_0 + a_1 s + a_2 s^2 + \dots$, $B(t) = b_0 + b_1 t + b_2 t^2 + \dots$ - two generating functions, and $B(0) = b_0 = 0$.

Definition. A substitution of a generating function B into a generating function A is a generating function

$$A(B(t)) = a_0 + a_1 B(t) + a_2 B(t)^2 + a_3 B(t)^3 + \dots =$$

$$= a_0 + a_1 b_1 t + (a_1 b_2 + a_2 b_1)t^2 + (a_1 b_3 + 2a_2 b_1 b_2 + a_3 b_1^3)t^3 + \dots$$

Theorem (Inverse function).

Let $B(t) = b_1 t + b_2 t^2 + \dots$, and $b_1 \neq 0$, then there exists $A(s) = a_1 s + a_2 s^2 + \dots$ and $C(u) = c_1 u + c_2 u^2 + \dots$ such that

$$A(B(t)) = t \quad \text{and} \quad B(C(u)) = u.$$

Moreover, the functions A and C are unique.

Proposition.

$A(s) = \sum_{i=0}^{\infty} a_i x^i$ - generating function, and $A(0) = a_0 \neq 0$. Then there is a unique $B(s) = \sum_{i=0}^{\infty} b_i x^i$, such that $A(s)B(s) = 1$.