Дискретная математика. Теория

Александр Сергеев

1 Производящие функции

Определение

Формальный степенной ряд(производящая функция) – $A(t) = \sum\limits_{n=0}^{\infty} a_n t^n$

Формальный означает, что вместо t мы ничего не подставляем
Формальный степенной ряд – некоторый способ задавать последовательность
$A(t) = a_0 + a_1t^1 + a_2t^2 + \dots$
$B(t) = b_0 + b_1t^1 + b_2t^2 + \dots$
$C = A + B = (a_0 + b_0) + (a_1 + b_1)t^1 + \dots$
$C = A - B = (a_0 - b_0) + (a_1 - b_1)t^1 + \dots$
$C = A \cdot B = (a_0b_0) + (a_1b_0 + a_0b_1)t^1 + (a_2b_0 + a_1b_1 + a_0b_2)t^2 \dots$
$c_n = \sum\limits_{k=0}^{n} a_k b_{n-k}$
$C = \frac{A}{B}$:
$A = C \cdot B$
Потребуем $b_0 \neq 0$
$a_0 = c_0b_0 \Rightarrow c_0 = \frac{a_0}{b_0}$
$a_1 = c_0b_1 + c_1b_0 \Rightarrow c_1 = \frac{a_1 - c_0b_1}{b_0}$
$c_n = \frac{a_n - \sum_{k=0}^{n-1} c_k b_{n-k}}{b_0}$
Если $a_0 \neq 0, b_0 = 0$, то получаем, что числитель не делится на t, а знаменатель делится
Т.о. такая дробь не является степенным рядом
Если $a_0 = 0, b_0 = 0$

Тогда мы можем сократить на t

$B := A'$ – формальная производная
$b_n = (n+1)a_{n+1}$
$(A \pm B)' = A' \pm B'$
$(A \cdot B)' = A' \cdot B + A \cdot B'$
$\frac{A}{B} = \frac{A'B - AB'}{B^2}$

Пример
$\frac{1}{1-t} = \sum t^n$
$(\frac{1}{1-t})'t = \frac{t}{(1-t)^2} = \sum nt^n$

$A(B(t))$ – возможно только при $b_0 = 0$
$C = A(B(t)) = a_0 + a_1(b_1t + b_2t^2 + b_3t^3 + \ldots) + a_2(b_1t + b_2t^2 + b_3t^3 + \ldots)^3 + \ldots =$
$a_0 + (a_1b_1)t + (a_1b_2 + a_2b_1^2)t^2 + (a_1b_3 + a_2b_1b_2 + a_2b_2b_1 + a_3b_1^3)t^3 + \ldots$
$c_n = \sum\limits_{k=1}^{n} a_k \sum\limits_{n=s_1+\ldots+s_k} \prod\limits_{i=1}^{k} b_{s_k}$
$(A(B))' = A'(B)B'$
$B := \int A$ – формальная первообразная
$b_n = \frac{a_{n-1}}{n}$
b_0 – может быть различным

1.1 Дробно-рациональные производящие функции

Определение

Дробно-рациональная производящая функция $A(t) = \frac{P(t)}{Q(t)}, q_0 \neq 0, P, Q$ – конечные многочлены

Определение

Линейное рекуррентное соотношение – $a_n = \sum\limits_{i=1}^{k} c_i a_{n-i}$

$a_1, \ldots, a_k$ – конкретные значения

Теорема ч.1 (теорема о дробно-рациональных производящих функ-

циях)

$A(t) = \dfrac{P(t)}{Q(t)} \Leftrightarrow a_n = \sum\limits_{i=1}^{k} c_i a_{n-i} \wedge Q(t) = 1 - c_1 t - \ldots - c_k t^k$

Доказательство $\Rightarrow$

$Q(t) = q_0 + \ldots + q_k t^k$

$1 + \dfrac{q_1}{q_0} t + \ldots + \dfrac{q_k}{q_0} t^k$

$c_i = -\dfrac{q_i}{q_0}$

$P(t) := \dfrac{P}{q_0}$

Рассмотрим $\dfrac{P}{1 - c_1 t - \ldots - c_k t^k}$

Для $n > \max(k, \deg P)$

$a_n = \dfrac{p_n - \sum_{i=0}^{n-1} a_i(-c_{n-i})}{c_0} = \sum\limits_{i=1}^{k} a_{n-i} c_i$

Уберем исходное требование

$a_n = \sum\limits_{i=1}^{k} (c_i \cdot \begin{bmatrix} a_{n-i}, & n \geq i \\ 0, & n < i \end{bmatrix}) + p_n$

Доказательство $\Leftarrow$

$n \geq m$

$a_n = c_1 a_{n-1} + \ldots + c_k a_{n-k}$

Рассмотрим $A(t) = a_0 + a_1 t + a_2 t^2 + \ldots$

$c_1 t A(t) = c_1 a_0 t + c_1 a_1 t^2 + c_1 a_2 t^3 + \ldots$

$c_2 t^2 A(t) = c_2 a_0 t^2 + c_2 a_1 t^3 + c_2 a_2 t^4 + \ldots$

$c_k t^k A(t) = c_k a_0 t^k + c_k a_1 t^{k+1} + c_k a_2 t^{k+2} + \ldots$

$A(t)(1 - c_1 t - c_2 t^2 - \ldots - c_k t^k) = P(t), \deg P \leq m$

$A(t) = \dfrac{P}{1 - c_1 t - c_2 t^2 - \ldots - c_k t^k}$

Рассмотрим $a_n = c_1 a_{n-1} + \ldots + c_k a_{n-k}$

$$\begin{pmatrix} a_n \\ \vdots \\ a_{n-k+1} \end{pmatrix} = \begin{pmatrix} c_1 & c_2 & \ldots & c_k \\ 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 1 & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{n-1} \\ \vdots \\ a_{n-k} \end{pmatrix}$$

Применяя быстрое возведение матрицы в степень, можно найти a_n за $O(k^3 \log n)$

Рассмотрим $\dfrac{P}{Q}$

$\dfrac{P(t)}{Q(t)} \cdot \dfrac{Q(-t)}{Q(-t)} = \dfrac{P(t)Q(-t)}{Q_2(t)}$, где Q_2 – многочлен, где все нечетные коэффициенты нулевые

$Q_2 = \widetilde{Q}(t^2)$

Это следует из того, что $Q(t)Q(-t)$ – четная функция

$\deg Q = \deg \widetilde{Q}$

$\dfrac{P(t)}{Q(t)} = \dfrac{P(t)Q(-t)}{\widetilde{Q}(t^2)} = \dfrac{\widetilde{P}(t^2) + t\overline{P}(t^2)}{\widetilde{Q}(t^2)}$ (разбили на четные и нечетные степени)

Заметим, что нечетная подпоследовательность и четная подпоследовательность не связаны

У последовательности четных членов производящая функция – $\dfrac{\widetilde{P}}{\widetilde{Q}}$, у нечетных – $\dfrac{\overline{P}}{\widetilde{Q}}$

Т.о. мы можем каждый раз уменьшать последовательность в два раза

Итого асимтотика $O(k^2 \log n)$

Теорема ч.2 (о линейных рекуррентных соотношениях)

Тогда эквивалентны:

1. $n \geq m$ $a_n = \sum\limits_{i=1}^{k} c_i a_{n-i}$
2. $A(t) = \dfrac{P(t)}{Q(t)}, Q(t) = 1 - c_1 t - \ldots - c_k t^k$
3. $a_n = \sum\limits_{i=1}^{s} p_i(n) r_i^n, p_i$ – многочлен, $r_i \in \mathbb{C}$

Доказательство $2 \Rightarrow 3$

Пусть $Q = \prod\limits_{i=1}^{s} (1 - r_i t)^{d_i}$

$t_i = \dfrac{1}{r_i}$ – корни кратности d_i

$\deg p_i = d_i - 1$

Лемма (о разложении на простые дроби)

$Q(t) = \prod\limits_{i=1}^{s}(1 - r_i t)^{d_i}$

Тогда $\dfrac{P(t)}{Q(t)} = \sum\limits_{i=1}^{s} \dfrac{P_i(t)}{(1 - r_i t)^{d_i}}$

$\dfrac{P(t)}{Q(t)} = \sum\limits_{i=1}^{s} \dfrac{P_i(t)}{(1 - r_i t)^{d_i}} = \sum\limits_{i=1}^{s} A_i(t)$

$a_n = \sum\limits_{i=1}^{s} a_{i,n}$

Лемма

$\dfrac{1}{(1 - rt)^d} = \sum\limits_{n=0}^{\infty} p_d(n) r^n t^n$

$\deg p_d = d - 1$

Доказательство

1. База $d = 1$:
   $\dfrac{1}{1 - rt} = 1 + rt + r^2t^2 + \ldots; a_n = r^n$

2. переход
   $(\dfrac{1}{(1 - rt)^d})' = \sum\limits_{n=0}^{\infty}(n+1)p_s(n+1)r^{n+1}t^n$

   $\dfrac{1}{(1 - rt)^{s+1}} = \sum\limits_{n=0}^{\infty} \dfrac{n+1}{s} p_s(n+1) r^n t^n$

   $p_{s+1}(n) = p_s(n+1)\dfrac{n+1}{s} = \sum\limits_{i=0}^{s-1} p_{s,i}(n+1)^i \dfrac{n+1}{s}$

   $p_{s,i} = \dfrac{a_{s,i}}{s!}, a_{s,i} \in \mathbb{Z}$

Доказательство $3 \Rightarrow 2$

Достаточно доказать, что если $a_n = n^{d-1} r^n$, то $A(t) = \dfrac{P(t)}{(1 - rt)^d}$

1. $d = 1$
   Слева:

$a_n = r^n$
Справа:
$A(t) = \dfrac{1}{1-rt}$

2. $A_d(t) = \dfrac{P_d(t)}{(1-rt)^d}$
Справа:
$\dfrac{1}{r}A'_d(t) = \dfrac{1}{r}\dfrac{P'_d(t)(1-rt)^d + rd(1-rt)^{d-1}P_d(t)}{(1-rt)^{2d}} = \dfrac{1}{r}\dfrac{P'_d(t)(1-rt) + rP_d(t)}{(1-rt)^{d+1}}$
Слева:
$a_n = (n+1)^{d-1}(n+1)r^{n+1}\dfrac{1}{r} = (n+1)^d r^n = n^d r^n + \sum_{i=1}^{d}\binom{d}{i}n^{d-i}r^n$
$A(t) = \dfrac{1}{r}(A'_d(t)) - \sum_{i=1}^{d}\binom{d}{i}\dfrac{P_{d-i}(t)}{(1-rt)^{d-i+1}}$

Попробуем найти производящую функции чисел Каталана
$c_n = \sum_{i=0}^{n-1} c_i c_{n-1-i}$
Пусть $C(t) = c_0 + c_1 t + \dots$
$C(t)C(t)t = C(t) - 1$
$C^2(t)t + 1 = C(t)$
$C^2(t)t - C(t) + 1 = 0$
$C(t) = \dfrac{1 \pm \sqrt{1-4t}}{2t}$
$\sqrt{1-4t} = \sum_{k=0}^{\infty}\binom{\frac{1}{2}}{k}(-4t)^k$
$C(t) = \dfrac{1+\sqrt{1-4t}}{2t}$ – некорректная дробь, т.к. на t делить нельзя
$C(t) = \dfrac{1-\sqrt{1-4t}}{2t} = \dfrac{1-\sum_{k=0}^{\infty}\binom{\frac{1}{2}}{k}(-4t)^k}{2t} = \dfrac{-\sum_{k=1}^{\infty}\binom{\frac{1}{2}}{k}(-4t)^k}{2t}$
$C(t) = \dfrac{2^n(2n+1)!!}{n!}$ (почему-то численно не сходится)

1.2 Конструируемые комбинаторные объекты

Мы будем говорить о непомеченных комбинаторных объектах
Представим, что $A(t) \leftrightarrow a_0, a_1, \dots, a_n, \dots$

a_n – количество комбинаторных объектов размера n
Комбинаторные объекты размеров n и m можно сложить в комбинаторный объект размера $n+m$ единственным способом
$A \sqcup B \leftrightarrow A + B$ – объединение дизъюнктных множество
$A \times B \leftrightarrow AB$
$C = List(A) = \sqcup_{k=0}^{\infty} A^k$

$$C(t) = \sum_{k=0}^{\infty} A^k(t) = \frac{1}{1 - A(t)}$$

$$List(A) = \underbrace{1}_{[\,]} + A \times List(A)$$

Пример (натуральные числа)
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
$U = \{0\}$
$U(t) = t$

$$\mathbb{N}_0 = List(U) = \frac{1}{1-t} = 1 + t + t^2 + t^3 + \dots$$

$$\mathbb{N} = \frac{1}{1-t} - 1 = \frac{t}{1-t}$$

Пример (натуральные числа)
$B = \{\circ, \bullet\}$
$B(t) = 2t$

$$List(B) = \frac{1}{1-2t}$$

Пример (замощение)
$D = \{-^2, |\}$
$D(t) = t + t^2$

$$List(D) = \frac{1}{1 - t - t^2}$$

$Set(A) = \prod\limits_{x \in A}(1 + x)$ – каждый объект либо берем, либо нет
$//w(x)$ – количество объектов в x | вес x

$Set(A) = \prod\limits_{k=0}^{\infty} \prod\limits_{x \in A, w(x) = k} (1 + x)$ – сгруппируем по весу

$$Set(A) = \prod_{k=0}^{\infty}(1 + t^k)^{a_k} = B$$

$//[t^n]A$ – возвращает множитель при t^n

$b_n = [t^n]\prod_{k=0}^{\infty}(1+t^k)^{a_k} = [t^n]\prod_{k=0}^{n}(1+t^k)^{a_k}$
$Set(U) = 1 + t$
$Set(B) = 1 + 2t + t^2$
$Set(N) = \prod_{k=1}^{n}(1+t^k) = 1 + t + t^2 + 2t^3 + 2t^4 + 3t^5 + 4t6 + \ldots$ – количество разбиений на различные слагаемые

$Multiset(A) = \prod_{x\in A}(1 + x + x^2 + x^3 + \ldots) = \prod_{x\in A}\frac{1}{1-x} = \prod_{k=0}^{\infty}\frac{1}{(1-t^k)^{a_k}}$
$MSet(U) = \frac{1}{1-t}$
$MSet(B) = (\frac{1}{1-t})^2$
$MSet(N) = \sum_{k=0}^{\infty} p_n t^n, p_n$ – число разбиений n на слагаемые
$Cyc(A) = List(A)/_{\sim}, \sim$ – равенство с точностью до перестановки
C_n – циклы веса n
$C_n = \bigcup_{l=1}^{n} C_{n,l}$
//todo продолжить

1.3 Регулярные языки

Напоминание
Регулярный язык – язык, который можно задать регулярным выражением
Регулярный язык – язык, который можно задать детерменированным конечным автоматом

Язык $L \subset \Sigma^*$
$\Sigma^m \leftrightarrow\leftrightarrow \frac{1}{1-|\Sigma|t}$
Казалось бы, $| \leftrightarrow \cdot, \cup \leftrightarrow Seq, + \leftrightarrow \frac{1}{1-\bullet}$
Но бывают проблемы

Определение
Регулярное выражение – однозначное, если любая строка однозначно «метчится» с регулярным выражением
К примеру, $(a|b)^*a(a|b)^*$ неоднозначное, поэтому для него производящие функции будут работать неверно
Его можно перестроить в $b^*a(a|b)^*$
Теорема
L – регулярное $\Leftrightarrow \exists\, S$ – регулярное выражение для L

Пусть L – язык
A – ДКА для L
Для вершины $u : L_u = \{x : x \overset{x}{\rightsquigarrow} t, t \in T\}$
$L = L_s, s$ – стартовая
$u \notin T : L_u = c_1 L_{\sigma(u,c_1)} \cup \ldots \cup c_m L_{\sigma(u,c_m)}$
$u \in T : L_u = c_1 L_{\sigma(u,c_1)} \cup \ldots \cup c_m L_{\sigma(u,c_m)} \cup \varepsilon$
$u \notin T : L_u(t) = \sum t L_{\sigma(u,c_i)}(t)$
$u \in T : L_u(t) = \sum t L_{\sigma(u,c_i)}(t) + 1$
$\overrightarrow{L(t)} = \begin{pmatrix} L_1(t) \\ \vdots \\ L_q(t) \end{pmatrix}$ $\Delta_{i,j} =$ число ребер$i \to j$
$\overrightarrow{L(t)} = t\Delta\overrightarrow{L(t)} + \overrightarrow{f}$
$\overrightarrow{f}_i = \begin{cases} 1, & i \in T \\ 0, & i \notin T \end{cases}$
$(I - t\Delta)\overrightarrow{L(t)} = \overrightarrow{f}$
$\overrightarrow{L(t)} = (I - t\Delta)^{-1}\overrightarrow{f}$
$\det I - t\Delta = \sum\limits_{\sigma} \prod\limits_{i} (I - t\Delta)_{i,\sigma_i} = \prod\limits_{i} (I - t\Delta)_{i,i} + \sum\limits_{\sigma \neq id} \prod\limits_{i} (I - t\Delta)_{i,\sigma_i} =$
$\underbrace{\prod\limits_{i=1}^{q} (1 - \sigma_{i,i} t)}_{1+tP(t)} + \underbrace{\sum\limits_{\sigma \neq id} \prod\limits_{i} (I - t\Delta)_{i,\sigma_i}}_{tQ(t)} = 1 + t(P(t) + Q(t))$
$(I - t\Delta)^{-1} = \dfrac{Q(t)}{1 + t(P(t) + Q(t))}$

Теорема
L – регулярный $\Rightarrow L(t)$ – дробно-рациональное

$L(t) = \overrightarrow{S}^t (I - t\Delta)^{-1} \overrightarrow{f}$
$\overrightarrow{S}_i = \begin{cases} 1, & i = s \\ 0, & i \neq s \end{cases}$

Определение
Бордер строки s – одновременный префикс и суффикс s
$c_i = \begin{cases} 1, & s[i:] = s[:-i] \\ 0 \end{cases}$
$c(t)$ – автокорреляционный многочлен s
S – не содержит подстроки s
T – содержит s, единственное вхождение как суффикса
$S + T = \varepsilon + S \times \Sigma$
$S(t) + T(t) = 1 + mtS(t)$
$S(t)t^k = T(t)c(t)$
Отсюда $S(t) = \dfrac{c(t)}{(1 - mt)c(t) + t^k}$
Пентагональная теорема Эйлера
Разбиения на слагаемые:
$P(t) = \prod\limits_{i=1}^{\infty} \dfrac{1}{1 - t^i} = \dfrac{1}{Q(t)}$
$Q(t) = \prod\limits_{i=1}^{\infty} (1 - t^i) = 1 - t - t^2 + t^5 + t^7 - t^{12} - t^{15} + \dots$
$R(t) = \prod\limits_{i=1}^{\infty} (1 + t^i)$ – разбиения на различные слагаемые
$q_n = e_n - o_n, e_n$ – число разбиений на четное число различных слагаемых, o_n – на нечетное число различных слагаемых
Лемма
$n \neq \dfrac{3k^2 \pm k}{2}$
Тогда $e_n = o_n$
$n = \dfrac{3k^2 \pm k}{2}$
$e_n - o_n = (-1)^k$
$Q(t) = 1 + \sum\limits_{k=1}^{\infty} (-1)^k (t^{\frac{3k^2+k}{2}} + t^{\frac{3k^2-k}{2}})$

1.4 Экспоненциальные производящие функции и помеченные комбинаторные объекты

$a_0, a_1, \ldots \leftrightarrow A(t) = \sum\limits_{n=0}^{\infty} \frac{a_n}{n!} t^n$

$b_0, a_2, \ldots \leftrightarrow B(t) = \sum\limits_{n=0}^{\infty} \frac{b_n}{n!} t^n$

$a_n + b_n \leftrightarrow A(t) + B(t)$

$\frac{c_n}{n!} = \frac{1}{n!} \sum\limits_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \leftrightarrow A(t)B(t) = C(t)$

$A \times B \leftrightarrow A(t)B(t)$ – количество пар с различными нумерациями

$a_n = n! \leftrightarrow \frac{1}{1-t}$

$b_n = a_{n+1} \leftrightarrow B = A'$

$a_n = 1 \leftrightarrow e^t$

Найдем $B = Seq(A) : B = 1 + A \times B$

$B = \frac{1}{1-A}$

$Set = MSet = \sum\limits_{k=0}^{\infty} \frac{A^k}{k!} = e^{A(t)}$

$Set(U = \{\circ\}) = e^t \leftrightarrow a_n = 1$

$B = \{\circ, \bullet\}$

$Set(B) = e^{2t}$

Числа Белла – количество способов разбить множество на какие-то множества

$B = Set(\underbrace{Set(U) - 1}_{\mathbb{N}}) = e^{e^t - 1}$

$A(t) = t^k e^t$ (размещения по k)

$a_n = \frac{n!}{(n-k)!}$

$C(t) = \frac{t^k}{k!} e^t$ (сочетания по k)

$C_n = \frac{n!}{(n-k)!k!}$

Числа Стирлинга по k

$\frac{(e^t - 1)^k}{k!}$ – число Стирлинга 2 рода по k

$$Cyc(A) = \sum_{k=1}^{\infty} \frac{A^k}{k} = -\ln(1 - A(t)) = \ln(\frac{1}{1 - A(t)}) = \ln(Seq(A(t)))$$

$Cyc(U)$ – перестановки с точностью до циклического сдвига

$Set(Cyc(U)) = Seq(U)$

Числа Стирлинга 1 рода по k

$\dfrac{Cyc(U)^k}{k!}$

Деревья

$T = U \times Seq(T)$ – деревья с порядком на детях

$T = U \times Set(T)$ – деревья без порядка на детях

1.5 Формула Лагранжа

Пусть есть уравнение для производящих функций $A(t) = t\phi(A(t))$

Тогда $a_n = \dfrac{1}{n}[s^{n-1}](\phi(s))^n$

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

Пусть есть уравнение для экспоненциальных производящих функций $A(t) = t\phi(A(t))$

Тогда $\dfrac{a_n}{n!} = \dfrac{1}{n}[s^{n-1}](\phi(s))^n$

$$A(t) = \sum_{n=0}^{\infty} \frac{a_n}{n!} t^n$$

1.6 Производящие функции от нескольких переменных

$$A(u, z) = \sum_{n,k=0}^{\infty} a_{u,z} z^n u^k$$

n – вес, k – стоимость

Пример

Рассмотрим $\{z, uz\}$, где z обозначает невзятый объект, а uz – взятый

$$Seq\{z, uz\} = \frac{1}{1 - z - uz} \leftrightarrow a_{n,k} = \binom{n}{k}$$

1.7 Средняя стоимость

Пусть есть $a_{n,k}$
Узнаем среднюю стоимость при фиксированном весе
$W_n = \frac{\sum_{i=0}^{\infty} ka_{n,k}}{\sum_{i=0}^{\infty} a_{n,k}}$
$\sum\limits_{k=0}^{\infty} ka_{n,k} = [z^n](\frac{\partial}{\partial u}A(u,z))\Big|_{u=1}$
$\sum\limits_{k=0}^{\infty} a_{n,k} = [z^n]A(1,z)$

1.8 Производящие функции Дирихле

$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots$ – дзета-функция
Определение $a_1, \ldots$ – последовательность
$A(s) = \frac{a_1}{1^s} + \frac{a_2}{2^s} + \ldots$ – производящая функция Дирихле
ζ – последовательность единиц
$A(s) \pm B(s) \leftrightarrow a_i + b_i$
$A(s)B(s) \leftrightarrow \sum\limits_{d|n} a_d b_{\frac{n}{d}}, d|n$ – n делится на d
$A(s)\zeta = C(s) \leftrightarrow \sum\limits_{d|n} a_d$
$\frac{A(s)}{B(s)}$
$c_1 = \frac{a_1}{b_1}$
$c_n = \frac{a_n - \sum_{d|n, d\neq 1} b_d c_{\frac{n}{d}}}{b_1}$
$\frac{1}{\zeta} \leftrightarrow -\sum\limits_{d|n, d\neq n} c_d$:
$c_p = -1, p$ – простое
$\frac{1}{\zeta} = M \leftrightarrow \mu(n) = \mu_n$ – функция обращения Мебиуса
Теорема

$$\mu_n = \begin{cases} 1, & n \text{ – произведение четного числа простых делителей} \\ -1, & n \text{ – произведение нечетного числа простых делителей} \\ 0, & p^2|n, p \text{ – простое} \end{cases}$$

Доказательство

$$\prod_{p \text{ – простое}} \frac{1}{1-p^{-s}} = \zeta(s)$$

Очевидно

Тогда $M(s) = \dfrac{1}{\zeta(s)} = \prod\limits_{p \text{ – простое}} (1 - p^{-s})$

Пусть $g_n = \sum\limits_{d|n} f_d$

Тогда $G(s) = F(s)\zeta(s)$

Отсюда $F(s) = \dfrac{G(s)}{\zeta(s)} = G(s)M(s)$

$f_n = \sum\limits_{d|n} g(d)\mu(\dfrac{n}{d}) = \sum\limits_{d|n} g(\dfrac{n}{d})\mu(d)$ – формула обращения Мебиуса

Пример

$\zeta(s)^2 = \Sigma(s)$

$\sigma_n = \sum\limits_{d|n} 1 \cdot 1$ – количество делителей числа n

$\zeta(s-1)\zeta(s)$ – производящая функция для суммы делителей

$\zeta(s-2)\zeta(s)$ – производная функция суммы квадратов делителей

Заметим, что наши функции *мультипликативны*: $f(ab) = f(a)f(b), a, b$ – взаимно простые

Отсюда $f(p_1^{a_1} \dots p_k^{a_k}) = f(p_1^{a_1}) \dots f(p_k^{a_k})$

Лемма

f_n – мультипликативна $\Leftrightarrow F(s) = \prod\limits_{p} \sum\limits_{k=0}^{\infty} f_{p^k} p^{-ks}$

Лемма

$F(s), G(s)$ – производящие функции Дирихле мультипликативной последовательности

Тогда $F(s)G(s), \dfrac{F(s)}{G(s)}$ – тоже

$1, 0, 0, \dots$ – мультипликативна

Отсюда мультипликативные операции образуют группу

Пример

ϕ – число взаимно простых чисел с n

$\phi(n)$ – мультипликативна
$\phi(p^k) = p^k - p^{k-1}$
$\Phi(s) = \prod\limits_{p \text{ – простое}} \sum\limits_{k=0}^{\infty} \phi(p^k) p^{-ks}$
$= \prod\limits_{p \text{ – простое}} (1 + \sum\limits_{k=0}^{\infty} (p^k - p^{k-1}) p^{-ks})$
$= \prod\limits_{p \text{ – простое}} (\frac{1}{1 - p^{-(s-1)}} (1 - p^{-s}))$
$= \prod\limits_{p \text{ – простое}} \frac{1}{1 - p^{-(s-1)}} \prod\limits_{p \text{ – простое}} (1 - p^{-s})$
$= \frac{\zeta(s-1)}{\zeta(s)}$
Теорема
$\Phi(s) = \frac{\zeta(s-1)}{\zeta(s)}$
$\phi_n = \sum\limits_{d|n} \mu(d) \frac{n}{d}$

2 Вычислимость

Пример (задача о соответствии Поста)
Дано: $n \in \mathbb{N}, a_i, b_i \in \{0,1\}^*$
Вывести: $k_1, \ldots, k_n : a_{k_1} \ldots a_{k_n} = b_{k_1} \ldots b_{k_n}$
Задача не имеет алгоритмического решения

Σ – алфавит
Σ^* – алфавит слов
$L \subset \Sigma^*$ – язык
Зафиксируем язык программирования $Prog \subset \Sigma^*$
Будем считать, что язык программирования и входной файл заданы на одном языке
Будем считать, что все программы корректны
Распознаватели – программы, которые получают на вход программу и возвращают true или false: $p(x) \in \{0,1\}$
Преобразователи – программы, которые получают слово и возвращают слово: $p(x) = y \in \Sigma^*$

Также программы могут зависать, $p(x) = \perp$
Однако, зависание – не значение. Нельзя понять, зависла ли программа или нет

Тезис Тьюринга-Черча

Некоторое вычисление можно провести на обычном компьютере $\Leftrightarrow$ его можно провести на машине Тьюринга

Определение

Язык A называется *разрешимым (рекурсивным)*, если существует программа $p : x \in A \Rightarrow p(x) = 1, x \notin A \Rightarrow p(x) = 0$

Определение

Язык A называется *полуразрешимым (перечислимый/рекурсивно перечислимый)*, если существует программа $p : x \in A \Leftrightarrow p(x) = 1$
Разница в том, что тут при $x \notin A$ программа может зависать

Пример

$A = \{n : x^n + y^n = z^n\}$

```
    def p(n):
        for b = 1 to inf:
            for x = 1 to b:
                for y = 1 to b:
                    for z = 1 to b:
                        if x^n + y^n = z^n: return true
```

Язык A полуразрешим

Утверждение

A – разрешим $\Rightarrow A$ – полуразрешим

Определение

A – перечислимый, если $\exists\, p : p()$ перечисляет все слова A

Теорема

A – перечислимый $\Leftrightarrow A$ – полуразрешимый

Доказательство $\Rightarrow$

Пусть p – перечислитель a

```
    def q(x):
        for i in p():
            if i == x: return true
        return false
```

Доказательство $\Leftarrow$

q – полуразрешитель

```
    def p():
        for t=1 to inf:
            for x in all_words[:t]:
                if run(q(x), TL=t):
                    print(x)
```

Префикс нужен, чтобы не было двух бесконечных вложенных циклов

Определение

$f : A \subset \Sigma^* \to \Sigma^*$

f – вычислимая, если существует преобразователь $p : x \in A \Rightarrow p(x) = f(x), x \notin A \Rightarrow p(x) = \perp$

$A = \Sigma^*$ – всюду определенная вычислимая

$U(p, x) := p(x)$ – универсальная функция

u – вычислима

$U = \{\langle p, x\rangle : p(x) = 1\}$ – универсальный язык

Теорема

U – полуразрешим, но не разрешим

Доказательство полуразрешимости

$u(p, x) = p(x)$

Опровержение разрешимости

Пусть U – разрешим

```
    def q(x):
        if u(x,x):
            return 0
        else:
            return 1
```

$q(q) = 1 \Leftrightarrow \neg u(q, q) \Leftrightarrow q(q) \neq 1$

Отсюда U не разрешим

Теорема

A – перечислимый

$\overline{A}$ – перечислимый

Тогда A – разрешим

Доказательство

a – полуразрешитель A

b – полуразрешитель $\overline{A}$

```
    for t = 0 to inf:
```

```
        if run(a(x), TL=t): return 1
        if run(b(x), TL=t): return 1
    new Thread(if (a): return 1)
    new Thread(if (b): return 0)
```

Тогда $\overline{U}$ – не перечислим

Теорема

Следующие 3 свойства нельзя выполнить одновременно

1. программы не зависают
2. можно вычислить все, что можно вычислить на компьютере
3. любую программу можно запустить

(не существует вычислимой нумерации всех всюду определенных вычислимых функций)

(любые два свойства можно выполнить)

Доказательство

Пусть существует

Пронумеруем все программы: $p_1, p_2, \ldots$

Пронумеруем все входы: $x_1, x_2, \ldots$

$q(k) = p_k(x_k) + 1$ – вычислима

$q(k)$ должна иметь номер как вычислимая программа

Но q отличается от любой программы выходом

Противоречие