Дискретная математика. I Семестр

Лектор: Пузынина Светлана Александровна
Автор конспекта: Буглеев Антон

2022

1 Булевы Функции

Булевы Функции. Базис

Def. *Булевой функцией* называется функция вида

$$f : \{0, 1\}^n \to \{0, 1\}.$$

Def. *Базис* - некоторое множество булевых функций.

Def. *Формула над базисом* определяется по индукции:
База: всякая функция $f \in F$ является формулой над F
Индуктивный переход: если $f(x_1, ..., x_n)$ - формула над F, а $\Phi_1, ..., \Phi_n$ - переменные, либо формулы над F, то тогда $f(\Phi_1, ...\Phi_n)$ - тоже формула над F.

ПК, ДНФ, СДНФ, ПД, КНФ, СКНФ, Многочлен (полином) Жегалкина

Def. *Простой конъюнкцией* (ПК) называется конъюнкция одной или нескольких переменных или их отрицаний, причём каждая переменная встречается не более одного раза.

Def. *Дизъюнктивная нормальная форма* (ДНФ) - дизъюнкция простых конъюнкций

Def. *Совершенная дизъюнктивная нормальная форма* (СДНФ) - ДНФ, в которой в каждой конъюнкции учавствуют все переменные.

Аналогично определяются *Простая дизъюнкция* (ПД), *Конъюнктивная нормальная форма* (КНФ), *Совершенная конъюнктивная нормальная форма* (СКНФ).

Def. *Многочлен (полином) Жегалкина* - сумма по модулю 2 конъюнкций переменных без повторений слагаемых, а также (необязательно) слагаемое 1.

$f(x_1, ..., x_n) = a \oplus a_1 \wedge x_1 \oplus ... \oplus a_{12} \wedge x_1 \wedge x_2 \oplus ... \oplus a_{1..n} \wedge x_1 \wedge ... \wedge x_n$

Например, $f(x, y, z) = x \oplus x \wedge y \wedge z \oplus 1$

Theorem. *Для каждой функции существует единственное представление многочленом Жегалкина.*

Proof. ... $\square$

Замыкание. Замкнутые классы. Полнота

Def. *Замыканием* $[F]$ базиса F называется множество всех функций, представимых формулой над F

Def. *Замкнутый класс* - класс, равный своему замыканию: $F = [F]$

1. $T_0 = \{f \mid f(0, \ldots, 0) = 0\}$
2. $T_1 = \{f \mid f(1, \ldots, 1) = 1\}$
3. $S = \{f \mid f(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n)\}$
4. $M = \{f \mid \forall$ двоичных наборов $\alpha \leq \beta : \ f(\alpha) \leq f(\beta)\}$
5. $L = \{f \mid f(x_1, \ldots, x_n) = x_1 \oplus ... \oplus x_n \oplus c\}$, где $c \in \{0, 1\}$

Theorem. *Классы T_0, T_1, S, M, L являются замкнутыми.*

Proof. ... $\square$

Def. Множество булевых функций F называется *полной системой*, если все булевы функции выразимы как формулы над данным базисом.

Theorem. *Множество булевых функций F является полным тогда и только тогда, когда F не содержится ни в одном из пяти классов T_0, T_1, S, M, L. (Теорема Поста)*

Proof. 1. $\Rightarrow$

Предположим, что F содержится в одном из классов $\Rightarrow [F]$ также содержится в одном из классов. Но все булевы функции не исчерпываются только одним классом. Получили противоречие.

2. $\Leftarrow$

Пусть $f_0, f_1, f_s, f_m, f_l \in F$ и $f_0 \notin T_0, f_1 \notin T_1, f_s \notin S, f_m \notin M, f_l \notin L$.

(a) $f_0 \notin T_0 \Rightarrow f_0(0,0,\dots,0) = 1$.
Если $f_0(1,1,\dots,1) = 1$, значит получена константа $\phi_1(x) = f_0(x,\dots,x) = 1$
Если $f_0(1,\dots,1) = 0$, значит получено отрицание $\overline{\phi(x)} = f_0(x,\dots,x) = \overline{x}$

(b) $f_1 \notin T_1 \Rightarrow f_1(1,\dots,1) = 0$.
Если $f_1(0,\dots,0) = 1$, значит получено отрицание $\overline{\phi(x)} = f_0(x,\dots,x) = \overline{x}$
Если $f_1(0,\dots,0) = 0$, значит получена константа $\phi_0(x) = f_1(x,\dots,x) = 0$

(c) $f_s \notin S \Rightarrow \exists\,(\sigma_1,\dots,\sigma_n) : f_s(\sigma_1,\dots,\sigma_n) = f_s(\overline{\sigma_1},\dots,\overline{\sigma_n})$. Имея лишь отрицание из пунктов (a) и (b) мы можем получить константу с помощью $f_s(x^{\sigma_1},\dots,x^{\sigma_n})$, а с помощью отрицания другую константу.

(d) $f_m \notin M \Rightarrow \exists(\sigma_1, dots, \sigma_n) : \begin{cases} f_s(\sigma_1,\dots,\sigma_k,0,\sigma_{k+2},\dots,\sigma_n) = 1 \\ f_s(\sigma_1,\dots,\sigma_k,1,\sigma_{k+2},\dots,\sigma_n) = 0 \end{cases}$
Таким образом, $f_s(\sigma_1,\dots,\sigma_k,x,\sigma_{k+2},\dots,\sigma_n) = \overline{x}$, получаем отрицание.

(e) $f_l \notin L \Rightarrow$ у f_l хотя бы одно из слагаемых содержит конъюнкцию. Расмотрим некоторую конъюнкцию. Выберем из неё два множителя x и y. Тогда, поскольку, данная конъюнкция принимают единицу, $\exists$ набор α, при котором остальные множители конъюнкции существуют. Тогда функция принимает вид:

$$f_l(x,y,\alpha) = xyp(\alpha) \oplus xs(\alpha) \oplus yq(\alpha) \oplus r(\alpha)$$
$$f_l(x,y,\alpha) = xy \oplus xs(\alpha) \oplus yq(\alpha) \oplus r(\alpha)$$
$$f_l(x,y) = xy \oplus xa \oplus yb \oplus c;\ \ a,b,c \in \{0,1\}$$

Если $a = b = c = 0$ тогда конъюнкция получена. В противном случае:

$$f_l(x \oplus b, y \oplus a) = (x \oplus b)(y \oplus a) \oplus (x \oplus b)a \oplus (y \oplus a)b \oplus c$$
$$f_l = xy \oplus xa \oplus yb \oplus ab \oplus xa \oplus ab \oplus yb \oplus ab \oplus c$$
$$f_l = xy \oplus ab \oplus c$$

При любом наборе (a, b, c) мы получаем либо конъюнкцию, либо её отрицание, но с помощью ещё одного отрицания получаем конъюнкцию. Что и требовалось

□

2 Комбинаторика

Выборки

Def. Введём $A = \{a_1, \ldots, a_n\}$. Некоторый набор элементов $(a_{i_1}, \ldots, a_{i_r})$ называется *выборкой объёма r из n элементов* или (n, r)*-выборкой.*

Выборки бывают *упорядоченные* (порядок элементов важен) или *неупорядоченные* (без разницы, в каком порядке элементы), а также *с повторениями* и *без повторений.*
Пусть объект A можно выбрать n способами, а объект B - m способами. Тогда важны два правила:

1. *Правило суммы.* Выбор «A или B» можно выбрать $n+m$ способами.

2. *Правило произведения.* Выбор пары (A, B) можно выбрать nm способами.

Def. Выборки k элементов из n:

1. *Упорядоченная с повторениями*: n^k

2. *Упорядоченная без повторений (размещения)*: $A_n^k = \dfrac{n!}{(n-k)!}$

3. *Неупорядоченная без повторений (сочетания)*: $C_n^k = \dfrac{n!}{k!(n-k)!}$

4. *Неупорядоченная с повторениями*: $\hat{C} = C_{n+k-1}^k$

Proof. Пусть $A = \{a_1, \dots, a_n\}$. Неупорядоченная выборка k элементов с повторениями задаётся вектором $(x_1, \dots, x_n)$, где x_i - число повторений элемента a_i. Таким образом, $x_1 + \dots + x_n = k$
Закодируем решение бинарным вектором $\underbrace{11\dots1}_{x_1}0\underbrace{11\dots1}_{x_2}0\dots0\underbrace{11\dots1}_{x_n}$.

Получаем вектор, состоящий из k единиц и $(n-1)$ нулей. Число таких векторов: C_{n-1+k}^k, что и требовалось □

Полезные свойства сочетаний

Theorem. $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$

Proof.

$$\begin{aligned}
&C_{n-1}^k + C_{n-1}^{k-1} = \\
&\frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} = \\
&\frac{(n-k)(n-1)! + k(n-1)!}{k!(n-k)!} = \\
&\frac{(n-1)!((n-k)+k)}{k!(n-k)!} = \\
&\frac{n!}{k!(n-k)!} = C_n^k
\end{aligned}$$

□

Треугольник Паскаля ...

Theorem. *Бином Ньютона.*

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

Proof. Член $a^k b^{n-k}$ участвует в разложение $(a+b)^n$ столько раз, сколько есть способов выбрать a в k множителях из n - а это C_n^k. $\square$

Lemma. *Грубые оценки для $n!$:*

$$(n/e)^n < n! < n^n$$

Proof. Верхняя оценка очевидна. Докажем нижнюю по индукции:

1. База: $(1/e)^1 < 1 \Leftrightarrow 1/e < 1$
2. Переход: пусть верно для n:

$$\begin{aligned} & n! > \left(\frac{n}{e}\right)^n \Leftrightarrow \\ & (n+1)n! > (n+1)\left(\frac{n}{e}\right)^n \\ & (n+1)! > (n+1)\left(\frac{n}{e}\right)^n \end{aligned}$$

   Теперь покажем, что

$$\begin{aligned} & (n+1)\left(\frac{n}{e}\right)^n > \left(\frac{n+1}{e}\right)^{n+1} \Leftrightarrow \\ & e(n+1)n^n > (n+1)^{n+1} \Leftrightarrow \\ & en^n > (n+1)^n \text{ (верно в курсе матанализа)} \end{aligned}$$

$\square$

Theorem. *Формула Стирлинга.*

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

Язык Дика. Число Каталана

Def. *Правильная скобочная последовательность.* Определим по индукции:

1. пустая строка ϵ - ПСП
2. если w - ПСП, то (w) - ПСП
3. если w, u - ПСП, то wu - ПСП

Def. *Языком Дика* называется множество всех ПСП: $\epsilon, (), ()(), (()), (()()) \ldots$

Def. *Числа Каталана* задаются количеством ПСП с n парами скобок

Пример:

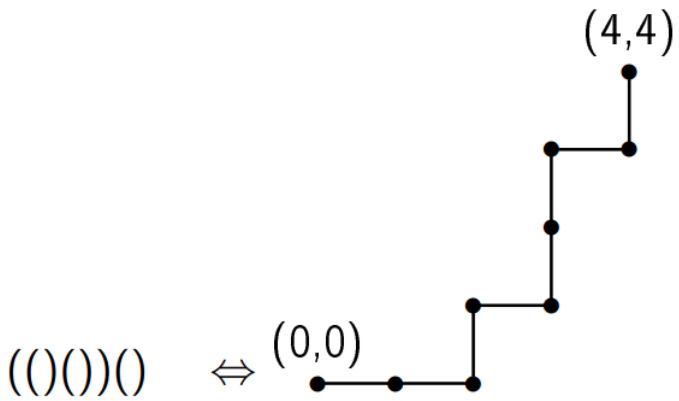
1. $D_0 = 1 : \epsilon$
2. $D_1 = 1 : ()$
3. $D_2 = 2 : (()), ()()$
4. $\ldots$

Theorem. *Рекурентная формула чисел Каталана:*

$$D_0 = 1; D_n = \sum_{k=0}^{n-1} D_k D_{n-1-k}$$

Proof. Пусть w - произвольная ПСП длины $2n$. Она начинается с открывающей скобки. Найдём ей парную закрывающуюся и представим в виде: $w = (u)v$, где u, w - ПСП.
Если длина u есть $2k$, то u можно составить D_k способами. Тогда длина v есть $2(n-k-1)$. v можно составить D_{n-k-1} способами. Применим правило произведения и получим, что способов составить $D_n = D_k D_{n-k-1}$. Перебрав все k от 0 до $n-1$ и проссумировав получим нужный ответ. $\square$

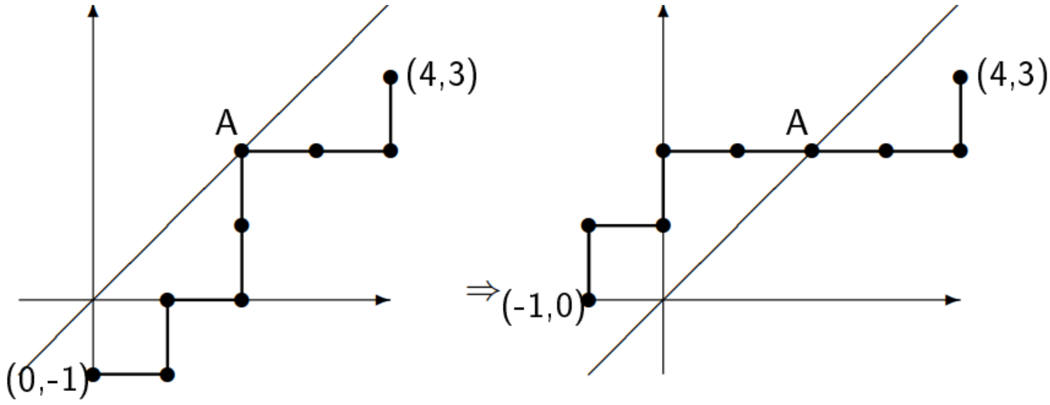
Числа Каталана через монотонные пути.
ПСП длины $2n$ поставим в соответствие путь в квадрате $[0,n]\times[0,n]$ из точки $(0,0)$ в точку (n,n).
Открывающей скобки сопоставим горизонтальный отрезок длины 1, а закрывающей - вертикальный.
Если путь сопоставлен ПСП, то ни одна его точка не может лежать выше главной диагонали квадрата.



Theorem. *Аналитическая формула для чисел Каталана.*

$$D_n = \frac{1}{n+1}C_{2n}^{n}$$

Proof. Сместим правильный путь на клетку вниз: теперь правильный путь идёт из $(0,-1)$ в $(n,n-1)$ и не имеет общих точек с прямой $y=x$.
Число правильный путей = общее число путей − число неправильных.
Общее число путей $= C_{2n}^{n}$
Рассмотрим неправильный путь и его первую точку на прямой $y=x$ - пусть это точка A. Отрезок до A заменим симметричным относительно $y=x$. Получили путь длины $2n$ из $(-1;0)$ в $(n;n-1)$.
Неправильных путей из $(0;-1)$ в $(n;n-1)$ столько же, сколько и путей из $(-1;0)$ в $(n,n-1)$. Учитывая, что при пути из $(-1;0)$ в $(n,n-1)$ $n-1$ вертикальных сегментов, имеем количество путей равное C_{2n}^{n-1}



$$D_n = C_{2n}^n - C_{2n}^{n-1} = \frac{1}{n+1} C_{2n}^n$$

□

Theorem. *Асимптотика чисел Каталана.*

$$D_n = (1 + o(1)) \cdot \frac{4^n}{n^{\frac{3}{2}}\sqrt{\pi}}$$

Proof. Применим формулу Стирлинга. ... □

3 Графы

Много определений

Def. *Графом* называется пара $G = (V, E)$, где V - конечное множество вершин, а $E \subseteq V \times V$ - множество рёбер.

Def. Граф можно задать *матрицей смежности* $A = (a_{ij})$ порядка $|V|$:

$$\begin{cases} 1, (i,j) \in E \\ 0, (i,j) \notin E \end{cases}$$

Def. Граф *неориентированный*, если $(u, v) \Rightarrow (v, u)$. Иначе граф называется *ориентированным*.

Def. При *мультиграфе* допускаются кратные рёбра. Тогда в таблице смежности будут присутствовать $n \in \mathbb{N}$.

Def. Две вершины u, v называются *смежными*, если $(u, v) \in E$.

Def. Вершина v и ребро e называются *инциндетными*, если $e = (v, u)$ для некоторой вершины u.

Def. Ребро, концевые вершины которого совпадают, называется *петлёй*

Def. *Степень* $\deg(v)$ вершины v - число инциндетных ей ребёр (петля считается дважды)

Lemma.

Во всяком графе сумма степеней всех вершин равна удвоенному числу рёбер

Proof. ... □

Lemma. *В ориентированном графе сумма входящих степеней равна сумме исходящих степеней*

Proof. ... □

Lemma. *Всякий конечный граф содержит чётное число вершин нечётной степени*

Proof. ... □