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

Proof.

1. $\Rightarrow$

   ...

2. $\Leftarrow$

   ...

$\square$

2 Комбинаторика

Выборки

Def. Введём $A = \{a_1, \dots, a_n\}$. Некоторый набор элементов $(a_{i_1}, \dots, a_{i_r})$ 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. □

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

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

□

Theorem. *Формула Стирлинга.*

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