Лекции по дискретной математике

me and boyz

3 октября 2021 г.

Содержание

1 Дискретные функции и их представление. Индуктивное определение формулы. Полные системы. Критерий полноты.

Определение. Дискретной функцией называется любая функция, отображающая конечное множество A в конечное множество B.

Область определения дискретной функции часто представляется в виде декартового произведения множеств относительно небольшой мощности.

Если $f : A \to B$ - дискретная функция и $A = A_1 \times \cdots \times A_n$, то f обозначают следующим образом $f(x_1; \ldots; x_n)$ и называют дискретной функцией от n переменных $x_1, \ldots, x_n$. При этом x_i принимает всевозможные значения из A_i. Если $A_1 = \cdots = A_n = B$ и $B = \{0, 1\}$, то f называется булевой функцией.

Определение. Обозначим далее $\Omega = \{0, 1\}$, тогда булевой функцией от n переменных называется любое отображение $f : \Omega^n \to \Omega$.

0-местными булевыми функциями будем называть элементы $0, 1 \in \Omega$.

Замечание. Существуют функции k - значной логики.

Обозначать булеву функцию будем $f(x_1; \ldots; x_n)$ или $f(\vec{x})$, если количество переменных известно из контекста.

Определение. Если $f(x_1; \ldots; x_n)$ - булева функция и $\vec{\alpha} = (a_1; \ldots; a_n) \in \Omega^n$, то образ $\vec{\alpha}$ при отображении f называют значением функции f на наборе $\vec{\alpha}$. Обозначение: $f(\vec{\alpha})$.

Определение. Если рассматривать 0 и 1 как числа $\in \mathbb{N}_0$, то для набора $\vec{\alpha} = (a_1; \ldots; a_n)$ обозначим $||\vec{\alpha}|| = a_1 + \cdots + a_n$ - вес вектора $\vec{\alpha}$.

$\widetilde{a} = \sum\limits_{i=1}^{n} a_i 2^{n-i}$ - лексикографический порядок.

Пример.

$$\vec{\alpha} = (1; 1; 0; 1) \Rightarrow ||\vec{\alpha}|| = 1 + 1 + 0 + 1 = 3.$$

Естественным образом задания является табличный, при этом координата i-вектора $f^{\downarrow}$ соответствует значению $f(\vec{\alpha})$, где $\widetilde{\alpha} = i$.

Пример.

x_0	x_1	$f^{\downarrow}$
0	0	0
0	1	1
1	0	1
1	1	1

Утверждение. $|F_2(n)| = 2^{2^n}$.

Определение. Весом булевой функции f называют величину $||f|| = |\{\vec{\alpha} \in \Omega^n \mid f(\vec{\alpha}) = 1\}|$.

Определение. Функция от $n-1$ переменной, определяемая равенством $\varphi(a_{i_n}; \ldots; a_{i_n}) = f'(a_1; \ldots; a_{i-1}; b; a_{i+1}; \ldots; a_n)$, называется функцией полученной из f' фиксацией i-ой переменной значением b.

Обозначением $\varphi = f_i^b(x_1; \ldots; x_n)$, аналогично фиксация k переменных значениями $b_1, \ldots, b_k : \varphi = f_{i_1;\ldots;i_n}^{b_1;\ldots;b_k}(x_1; \ldots; x_n)$.

Общее название таких функци φ - подфункции f.

Если $f(a_1; \ldots; a_{i-1}; 0; a_{i+1}; \ldots; a_n) = f(a_1; \ldots; a_{i-1}; 1; a_{i+1}; \ldots; a_n)$, то переменная x_i называется несущественной переменной функции f, в противном случае - существенной.

Определение. Пусть x_i -несущественная(*фиктивная*) переменная функции f, g получена из f фиксацией x_i любой константой, тогда говорят, что g получена удалением из f несущественной переменной x_i, а f получена из g добавлением фиктивной переменной x_i.

Пусть задано множество функций $\mathbb{K} = \{f_i : i \in I\}$ и множество символов переменных $X = \{x_1; \ldots; x_n\}$.

Определение.

1. Любой символ переменной есть формула над классом $\mathbb{K}$.

2. Если f_j - символ m - местной функции из $\mathbb{K}$, а $A_1, \ldots, A_m$ - формулы над $\mathbb{K}$, то $f_j(A_1; \ldots; A_m)$ - формула над $\mathbb{K}$.

3. Других формул нет.

Множество формул над $\mathbb{K}$ обозначается $\Phi(\mathbb{K})$. При $m = 0$ формула есть символ над $\mathbb{K}$, т.е. константа.

Определение. Число символов функций из $\mathbb{K}$, встречающихся в формуле A назовем рангом формулы A. Обозначение: $r(A)$.

Определение.

1. Подформула формулы x_i - только она сама.

2. Подформулы $f_j(A_1; \ldots; A_n)$ - на сама и все подформулы формулы $A_1; \ldots; A_n$.

Определение. Пусть A - произвольная формула, в ее записи присутствует только переменные $x_{i_1}, \ldots, x_{i_k}$. Набор $x_{j_1}, \ldots, x_{j_m}$ называется допустимым, если $\{x_{i_1}, \ldots, x_{i_k}\} \subseteq \{x_{j_1}, \ldots, x_{j_m}\}$.

Каждой формуле при фиксированном допустимом наборе $(x_1; \ldots; x_n)$ сопоставляется по следующему правилу:

1. Если A есть x_i, то ей сопоставляется функция f, значения которой определяются равенством $f(a_1; \ldots; a_n) = a_i, (a_1; \ldots; a_n) \in \Omega^n$.

2. Если A есть $f_j(A_1; \ldots; A_m)$ и формулам $A_1, \ldots, A_m$ сопоставлены функции $\varphi_1(x_1; \ldots; x_n); \ldots; \varphi_m(x_1; \ldots; x_n)$, то формуле A сопоставляется функция f, значения которой определяются равенством $f(a_1; \ldots; a_n) = f_j(b_1; \ldots; b_n)$, где $b_\zeta = \varphi_\zeta(a_1; \ldots; a_n), \zeta \in \overline{1, n}$.

Определение. Формулы A и B равносильны, если они представляют одну и ту же функцию на любом допустимом наборе. Обозначение: $A \equiv B$.

Определение. Пусть A - произвольная формула над классом $\mathbb{K} = (\&, \vee, \neg)$. Двойственной к A называется формула полученная из A заменой $\& \leftrightarrow \vee$. Обозначение: A^*.

Теорема. $A^*(x_1; \ldots; x_n) = \overline{A(\overline{x_1}; \ldots; \overline{x_n})}$.

Следствие. $A \equiv B \Leftrightarrow A^* \equiv B^*$.

Определение. Замыканием системы $\mathbb{K}$ булевых функций называют множество всех булевых функций представимых формулами над $\mathbb{K}$. Обозначение: $[\mathbb{K}]$.

Утверждение.

1. $\mathbb{K} \subseteq [\mathbb{K}]$

2. $\mathbb{K}_1 \subseteq \mathbb{K}_2 \Rightarrow [\mathbb{K}_1] \subseteq [\mathbb{K}_2]$

3. $[[\mathbb{K}]] = [\mathbb{K}]$

Определение. Система $\mathbb{K}$ называется полной, если (замыкание) $[\mathbb{K}] = F_2$.

Пример.

$$\left.\begin{aligned} \mathbb{K}_0 &= \{x_1 \cdot x_2; x_1 \vee x_2; \overline{x_1}\} \\ \mathbb{K}_5 &= \{x_1 \cdot x_2; x_1 \oplus x_2; 1\} \end{aligned}\right\} \text{Полные}$$

Определение. Класс булевых функций называется замкнутым, если $\mathbb{K} = [\mathbb{K}]$.

Говорят, что набор $\vec{\beta}$ мажорирует набор $\vec{\alpha}$, если $\forall i \in \overline{1, n} : a_i \leq b_i$. Обозначение: $\vec{\alpha} \preccurlyeq \vec{\beta}$.

Пример.

$T_0 = \{f(x_1;\dots;x_n) \mid f(0;\dots;0) = 0\}$
$T_1 = \{f(x_1;\dots;x_n) \mid f(1;\dots;1) = 1\}$
$L = \{f(x_1;\dots;x_n) = a_1x_1 \oplus \dots \oplus a_nx_n \mid a_i \in \Omega, i \in \overline{0,n}\}$ – класс линейных функций
$S = \{f(x_1;\dots;x_n) \mid f(x_1;\dots;x_n) \equiv \overline{f(\overline{x_1};\dots;\overline{x_n})}\}$ – класс самодвойственных функций
$M = \{f(x_1;\dots;x_n) \mid \text{верно} \vec{\alpha} \preccurlyeq \vec{\beta}, \text{то} f(\vec{\alpha} \leq f(\vec{\beta})) \forall \vec{\alpha}, \vec{\beta} \in \Omega^n\}$ – класс монотонных функций

Лемма. Булева функция $f(x_1;\dots;x_n)$ не является монотонной $\Leftrightarrow \exists \vec{\alpha}$ и $\vec{\beta}$ отличающиеся только в одной координате (соседние наборы), такие что $\vec{\alpha} \preccurlyeq \vec{\beta}$ и $f(\vec{\alpha}) > f(\vec{\beta})$.

Теорема. T_0, T_1, M, S, L - замкнуты.

Теорема. (Критерий Поста)

Система булевых функций $\mathbb{K}$ полна $\Leftrightarrow$ $\mathbb{K}$ содержит функции из $F_2 \backslash T_0, F_2 \backslash T_1, F_2 \backslash M, F_2 \backslash S, F_2 \backslash L$.

Док-во:

Необходимость

$\forall$ произвольного замкнутого класса $G \neq F_2$, если $\mathbb{K}$ не содержит ни одной функции из $F \backslash G$, то $\mathbb{K} \subset G \Rightarrow [\mathbb{K}] \subset [G] \neq F_2 \Rightarrow \mathbb{K}$ - не является полной.

Достаточность

Рассмотрим функции $f_1 \notin T_0, f_2 \notin T_1, f_3 \notin L, f_4 \notin S, f_5 \notin M$. Покажем, что если $\mathbb{K} \nsubseteq G$, где $G \in \{T_0, T_1, S, M, L\}$, то $\overline{x}$ и $x_1 \cdot x_2 \in [\mathbb{K}]$.

Рассмотрим 2 случая:

1. $f_1(1;\dots;1) = 1$, но тогда $f(x;\dots;x) = 1 \in [\mathbb{K}]$. Т.к. $\mathbb{K} \nsubseteq T_1$, то $\exists f_2 \in \mathbb{K} \mid f_2(1;\dots;1) = 0 \in [\mathbb{K}]$. Покажем, что $\overline{x} \in [\mathbb{K}]$. Т.к. $\mathbb{K} \nsubseteq M$, то $\exists f_3 \in \mathbb{K} \mid f_3 \notin M$, т.е. $\exists \vec{\alpha} \preccurlyeq \vec{\beta} \mid f_3(\vec{\alpha}) > f_3(\vec{\beta})$.

   Рассмотрим функцию $f_(a_1;\dots;a_{j-1};x_j;a_{j+1};\dots;a_n) \equiv \overline{x_j}$, т.к. 0 и 1 $\in [\mathbb{K}]$, то и $\overline{x} \in [\mathbb{K}]$.

2. $f_1(1;\dots;1) = 0$, то $f_1(x;\dots;x) = \overline{x} \in [\mathbb{K}]$. Покажем, что 0 и $1 \in [\mathbb{K}]$.

   Рассмотрим $f_4 \in \mathbb{K} \mid f_4 \notin S \Rightarrow \exists (a_1;\dots;a_n) \mid f_4(a_1;\dots;a_n) = f_4(\overline{a_1};\dots;\overline{a_n}) = const \in \{0,1\} \in [\mathbb{K}]$. Т.к. $\overline{x} \in [\mathbb{K}]$, то 0 и $1 \in [\mathbb{K}]$.

Покажем $x_1 \cdot x_2 \in [\mathbb{K}]$.

Т.к. $\mathbb{K} \notin L$, то $\exists f_5 \in \mathbb{K} \mid f_5 \notin L$, т.е. в ее многочлене Жегалкина $\exists$ *моном степени больше 1*(*) $\Rightarrow \exists$ моном, содержащий $x_1 \cdot x_2$.

Рассмотрим многочлен Жегалкина функции f_5:

$$f_5(x_1;\dots;x_n) = x_1 \cdot x_2 \cdot g_1(x_3;\dots;x_n) \oplus x_1 \cdot g_2(x_3;\dots;x_n) \oplus x_2 \cdot g_3(x_3;\dots;x_n) \oplus g_4(x_3;\dots;x_n).$$

Рассмотрим функцию f, полученную из f_5, следующим образом:

$$f(x_1;x_2) = f_5(x_1;x_2;a_3;\dots;a_n) = x_1x_2C_1 \oplus x_1C_2 \oplus x_2C_3 \oplus C_4.$$

$C_1 = 1$, т.к. см (*). Рассмотрим функцию $f(x_1 \oplus C_3; x_2 \oplus C_2) = x_1x_2 \oplus C_2C_3 \oplus C_4 \Rightarrow x_1x_2 \in [\mathbb{K}]$. ■