

Лекции по дискретной математике

me and boyz

4 октября 2021 г.

Содержание

1	Дискретные функции и их представление. Индуктивное определение формулы. Полные системы. Критерий полноты.	1
2	Классическое представление булевых функций. КНФ. ДНФ.	5
3	Метод Блейка	7
4	Метод Квайна	8
5	Представление дискретных функций в базисах функциональных пространств. Алгоритм БПФ.	9

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

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

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

Замечание. Существуют функции k - значной логики.

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

Определение. Если $f(x_1; \dots; x_n)$ - булева функция и $\vec{\alpha} = (a_1; \dots; a_n) \in \Omega^n$, 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 $\vec{\alpha} = (a_1; \dots; a_n)$ обозначим $\|\vec{\alpha}\| = a_1 + \dots + a_n$ - вес вектора $\vec{\alpha}$.

$\tilde{a} = \sum_{i=1}^n a_i 2^{n-i}$ - 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 $\tilde{a} = i$.

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 $\varphi(a_{i_1}; \dots; a_{i_n}) = f'(a_1; \dots; a_{i-1}; b; a_{i+1}; \dots; a_n)$, называется функцией полученной из f' фиксацией i -ой переменной значением b .

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

Общее название таких функции φ - подфункции f .

Если $f(a_1; \dots; a_{i-1}; 0; a_{i+1}; \dots; a_n) = f(a_1; \dots; a_{i-1}; 1; a_{i+1}; \dots; a_n)$, 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 $X = \{x_1; \dots; x_n\}$.

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, \dots, A_m - формулы над \mathbb{K} , то $f_j(A_1; \dots; A_m)$ - 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 $f_j(A_1; \dots; A_n)$ - на сама и все подформулы формулы $A_1; \dots; A_n$.

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

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

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

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

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: $\vec{\alpha} \preceq \vec{\beta}$.

Пример.

$$T_0 = \{f(x_1; \dots; x_n) \mid f(0; \dots; 0) = 0\}$$

$$T_1 = \{f(x_1; \dots; x_n) \mid f(1; \dots; 1) = 1\}$$

$$L = \{f(x_1; \dots; x_n) = a_1 x_1 \oplus \dots \oplus a_n x_n \mid a_i \in \Omega, i \in \overline{0, n}\} - \text{класс линейных функций}$$

$$S = \{f(x_1; \dots; x_n) \mid f(x_1; \dots; x_n) \equiv \overline{f(\overline{x_1}; \dots; \overline{x_n})}\} - \text{класс самодвойственных функций}$$

$$M = \{f(x_1; \dots; x_n) \mid \text{верно } \vec{\alpha} \preceq \vec{\beta}, \text{ то } f(\vec{\alpha}) \leq f(\vec{\beta}) \forall \vec{\alpha}, \vec{\beta} \in \Omega^n\} - \text{класс монотонных функций}$$

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 $\vec{\alpha} \preceq \vec{\beta}$ 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 $F_2 \setminus T_0, F_2 \setminus T_1, F_2 \setminus M, F_2 \setminus S, F_2 \setminus L$.

Док-во:

Необходимость

\forall произвольного замкнутого класса $G \neq F_2$, если \mathbb{K} не содержит ни одной функции из $F \setminus G$, 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 $\mathbb{K} \not\subseteq G$, где $G \in \{T_0, T_1, S, M, L\}$, то \bar{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. $\mathbb{K} \not\subseteq T_1$, то $\exists f_2 \in \mathbb{K} \mid f_2(1; \dots; 1) = 0 \in [\mathbb{K}]$. Покажем, что $\bar{x} \in [\mathbb{K}]$. Т.к. $\mathbb{K} \not\subseteq M$, то $\exists f_3 \in \mathbb{K} \mid f_3 \notin M$, т.е. $\exists \vec{\alpha} \preceq \vec{\beta} \mid f_3(\vec{\alpha}) > f_3(\vec{\beta})$.

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

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

Рассмотрим $f_4 \in \mathbb{K} \mid f_4 \notin S \Rightarrow \exists (a_1; \dots; a_n) \mid f_4(a_1; \dots; a_n) = f_4(\bar{a}_1; \dots; \bar{a}_n) = \text{const} \in \{0, 1\} \in [\mathbb{K}]$. Т.к. $\bar{x} \in [\mathbb{K}]$, то 0 и 1 $\in [\mathbb{K}]$.

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

Т.к. $\mathbb{K} \not\subseteq L$, 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:

$$f(x_1; x_2) = f_5(x_1; x_2; a_3; \dots; a_n) = x_1 x_2 C_1 \oplus x_1 C_2 \oplus x_2 C_3 \oplus C_4.$$

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

2 Классическое представление булевых функций. КНФ. ДНФ.

Рассмотрим класс $K_0 = \{\cdot, \vee, \neg\}$. Символом x^a , где $a \in \Omega$, обозначим функцию переменной x , принимающую значение 1, если $x = a$, и 0 в противном случае. Таким образом:

$$x^a = \begin{cases} x, & a = 1 \\ \bar{x}, & a = 0 \end{cases}$$

Определение. Пусть i_1, \dots, i_k - различные натуральные числа. Формула вида $x_{i_1}^{a_1} \vee \dots \vee x_{i_k}^{a_k}$ называется элементарной дизъюнкцией ранга k .

Если заменить \vee на $\&$, то получаем элементарную конъюнкцию ранга k .

Если элементарная дизъюнкция рассматривается как формула от переменных x_1, \dots, x_n и её ранг равен n , то она называется совершенной.

Определение. Конъюнктивной нормальной формой (КНФ) называется \forall формула представляющая собой конъюнкцию конечного числа элементарных дизъюнкций.

Теорема. \forall булева функция может быть представлена в виде $f(x_1, \dots, x_n) = \&_{(b_1, \dots, b_k) \in \Omega^k} x_{i_1}^{\bar{b}_{i_1}} \dots x_{i_k}^{\bar{b}_{i_k}} f_{i_1, \dots, i_n}(x_1, \dots, x_n)$

Замечание. Аналогичным образом определяется элементарная дизъюнкция (ДНФ).

Теорема. \forall булевой функции $k \leq n$ представима формулой $f(x_1, \dots, x_n) = \vee_{(a_1, \dots, a_k) \in \Omega^k} x_{i_1}^{a_{i_1}} \dots x_{i_k}^{a_{i_k}} f_{i_1, \dots, i_n}(x_1, \dots, x_n)$

Следствие. $f(x_1, \dots, x_n) \equiv \bar{x}_1 f(0, x_2, \dots, x_n) \vee x_1 f(1, x_2, \dots, x_n)$

В случае $k = n$ получаем совершенные КНФ и ДНФ, называемые СКНФ и СДНФ.

Утверждение. $\exists!$ СДНФ и СКНФ $\forall f \in F_2$.

Пример. (две ДНФ одной функции)

$$\bar{x}_1 x_2 x_3 \vee \bar{x}_1 x_2 x_3 \vee x_1 x_2 \equiv \bar{x}_1 x_3 \vee x_1 x_2$$

Определение. Многочленом Жегалкина от переменных x_1, \dots, x_n называется формула над классом $K_5 = \{\oplus, \cdot, 1\}$ вида

$$a_0 \oplus \sum_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \cdot \dots \cdot x_{i_n} \\ 1 \leq i_1 \leq \dots \leq i_k \leq n; a_0, a_{i_1}, \dots, a_{i_n} \in \Omega$$

Здесь знак суммы означает исключающее "или" и суммирование ведётся по всем непустым подмножествам $\{i_1, \dots, i_k\}$ множества $\{1, \dots, n\}$.

Определение. Элементарной конъюнкцией входящей в многочлен Жегалкина в качестве слагаемых называется одночлен (моном), элементы a_{i_1, \dots, i_k} коэффициенты многочлена, a_0 - свободный член. Ранг конъюнкции называется степенью одночлена.

Степенью нелинейности функции представляемой многочленом Жегалкина называется максимальная из степеней многочлена, входящих в многочлен Жегалкина этой функции с коэффициентом 1.

Теорема. \forall булева функция однозначно представима многочленом Жегалкина.

Определение. Двоичным n -мерным кубом называют множество точек пространства \mathbb{R}^n с координатами a_1, \dots, a_n , где $a_i \in \Omega$

Для задания булевой функции $f(x_1, \dots, x_n)$ на n -мерном кубе отмечают вершины соответствующие носителю этой функции.

Определение. Гранью n -мерного куба ранга k (или иначе размерности $n - k$) называется множество его вершин, соответствующее N_φ , где φ - произвольная элементарная конъюнкция ранга k , т.е. $\varphi = x_{i_1}^{a_1} \dots x_{i_k}^{a_k}$

Утверждение. (свойства)

1. $f = \varphi \Leftrightarrow N_f = N_\varphi$
2. $N_{f \cdot \varphi} = N_f \cap N_\varphi$
3. $N_{f \cup \varphi} = N_f \cup N_\varphi$
4. $f \cup \varphi \equiv f \Leftrightarrow N_\varphi \subseteq N_f$
5. $f \equiv \bigvee_{i=1}^m \varphi_i \Leftrightarrow N_f = \bigcup_{i=1}^m N_{\varphi_i}$

Определение. Длиной ДНФ называется сумма рангов входящих в неё элементарных конъюнкций. ДНФ с минимальной длиной называется минимальной ДНФ (МДНФ).

Определение. Элементарная конъюнкция $\psi = x_{i_1}^{a_1} \dots x_{i_k}^{a_k}$ называется имплекантой функции $f(x_1, \dots, x_n)$, если она входит в некоторую ДНФ представляющую функцию f .

Утверждение. (эквивалентно)

1. ψ - имплеканта функции f
2. $\psi \cup f \equiv f$
3. $\psi \rightarrow f \equiv 1$
4. $\psi \cdot f = \psi$

Определение. Говорят, что g поглощается функцией f , если $g \vee f \equiv f$, т.е. имплеканта это элементарная конъюнкция, поглощаемая функцией f .

Определение. Имплеканта функции f называется простой, если никакая её собственная часть не поглощается функцией f .

Пример.

$$f(x_1, x_2, x_3) \equiv x_1 x_2 \vee x_1 \overline{x_2} \vee \overline{x_2} x_3$$

$\overline{x_2} x_3$ - простая.

$x_1 x_2$ - нет, т.к. x_1 поглощается f .

Лемма. Пусть φ_1 и φ_2 имплеканты f , φ_1 поглощает $\varphi_2 \Leftrightarrow \varphi_1$ - часть φ_2

Теорема. \forall имплеканта функции f , содержащаяся в какой-либо МДНФ функции f является простой.

Теорема. Пусть $\varphi_1 \cup \dots \cup \varphi_m$ - дизъюнкция всех простых имплекантов функции f , тогда $f \leq \varphi_1 \vee \dots \vee \varphi_m$

Определение. Дизъюнкция всех простых имплекантов функции f называется сокращенной ДНФ.

Определение. ДНФ $\varphi_1 \cup \dots \cup \varphi_m$ функции f называется тупиковой, если все $\varphi_i, i \in \overline{1, k}$, входящие в неё, являются простыми имплекантами f и φ .

Всюду далее f — n -местная булева функция отличается от константы.

3 Метод Блейка

Метод Блейка строит из ДНФ сокращенную ДНФ.

Основной операцией данного алгоритма является операция неполного склеивания, в основе которого лежит тождество:

$$x\varphi_1 \vee \bar{x}\varphi_2 \equiv x\varphi_1 \vee \bar{x}\varphi_2 \vee \varphi_1\varphi_2$$

Вход: ДНФ

Выход: Сокращенная ДНФ

Этап 1 В исходной ДНФ находим пару имплекантов, в которой некоторая переменная входит в разных степенях: $\varphi_i = x_k\varphi'_i$ и $\varphi_j = \bar{x}_k\varphi'_j$.

Формируем $\varphi_1\varphi_2$ и добавляем её в ДНФ, повторяем до тех пор, пока не перестанут появляться новые имплеканты.

Этап 2 В полученной ДНФ применяем операцию поглощения используя тождество $\varphi\psi \vee \varphi \equiv \varphi$ до тех пор пока это возможно.

Теорема. Полученная на выходе алгоритма ДНФ является сокращенной ДНФ.

Док-во: Покажем, что ДНФ, полученная на Этапе 1 содержит все простые имплеканты функции f (индукция по n).

Пусть $n = 1$. Утверждение очевидно, т.к. ДНФ функции одной переменной отличной от константы есть x_1 или \bar{x}_1 .

Пусть \forall ДНФ и для \forall функции от $n-1$ переменной после Этапа 1 образуется ДНФ, содержащая все простые имплеканты.

Пусть теперь f - функция от n переменных и φ её имплеканта

а) Если ранг φ равен n , то φ содержится в \forall ДНФ функции f .

Действительно пусть $\varphi = x_1^{a_1} \cdot \dots \cdot x_n^{a_n}$, тогда она принимает значения $1 \Leftrightarrow$ все x_i равны a_i в любой ДНФ функции f должна присутствовать имплеканта φ' , принимающая значение 1 на $(a_1, \dots, a_n) \Rightarrow$ все переменные входят в неё в тех же степенях, что и в φ , но

б) Если ранг φ меньше, то $\exists x_i$ не входящее в φ .

Представим f в виде $f = x_i h \vee \bar{x}_i g \vee t$, где h, g, t - некоторые булевы функции, независимые от x_i . Т.к. φ - импликация функции f , то $\varphi \vee x_i h \vee \bar{x}_i g \vee t$ совпадает с $x_i h \vee \bar{x}_i g \vee t$. Полагая $x_i = 0$ или 1 имеем $\varphi \vee g \vee t \equiv$

$g \vee t$ и $\varphi \vee h \vee t \equiv h \vee t$ соответственно. Возьмём конъюнкцию этих тождеств и применим к левой части закон дистрибутивности. Получим $\varphi \vee (g \vee t)(h \vee t) \equiv (g \vee t)(h \vee t) \Rightarrow \varphi$ является имплекантой функции $f_1 = (h \vee t)(g \vee t) \equiv hg \vee t$.

ДНФ этой функции получается с помощью операции "неполного склеивания" из имплекант, входящих в ДНФ функции $x_i h \vee \bar{x}_i g \vee t$. При этом φ - простая для f , т.к. φ - простая для f_1 , а f поглощает f_1 .

Тогда по предположению индукции φ содержится в ДНФ, полученной после Этапа 1, применённого к ДНФ функции f_1 , но $\varphi \in$ аналогичной ДНФ функции f , т.к. \forall непростая имплеканта поглощается некоторой простой, то после Этапа 2 в ДНФ окажутся только простые имплеканты.

Лемма. Пусть ДНФ $A = \bigcup_{i=1}^k \varphi_i$ поглощает элементарную конъюнкцию φ и $\varphi \varphi_k \equiv 0$. Тогда φ поглощается ДНФ $A^1 = \bigcup_{i=1}^k \varphi_i$

Определение. Функции f_1 и f_2 называются ортогональными, если $f_1 f_2 \equiv 0$

Теорема. (Критерий поглощения)

Пусть $A = \bigcup_{i=1}^k \varphi_i$ - ДНФ некоторой функции, φ_0 - элементарная конъюнкция не ортогональная ни одной из конъюнкций $\varphi_1, \dots, \varphi_k$. Обозначим φ_{0_i} - конъюнкцию членов входящих в φ_0 и в φ_i , а φ_{1_i} - конъюнкция членов φ_i , не входящих в φ_0 (если $\varphi_i = \varphi_{0_i}, \varphi_{1_i} = 1$) ДНФ поглощает $\varphi \Leftrightarrow \bigvee_{i=1}^k \varphi_{1_i} \equiv 1$

Утверждение. Если f монотонна, то сокращённая ДНФ = МДНФ.

4 Метод Квайна

Составляется таблица, строчки которой обозначают всеми простыми имплекантами длиной функции, столбцы - наборами, на которых функция принимает значение 1. На пересечении ставится значение имплеканты на соответствующем наборе. Для построения ДНФ или МДНФ надо удалять строки так, чтобы в каждом столбце была хотя бы одна 1.

5 Представление дискретных функций в базисах функциональных пространств. Алгоритм БПФ.

Определение. Пусть K - произвольное поле, 0 и 1 - нуль и единица поля K соответствует псевдобулевой функции от n переменных называется произвольное отображение $f : \{0, 1\}^n \rightarrow K$. Обобщение $GF(p)^n \rightarrow K$. Множества таких функций будем называть $K_p(n)$. На $K_p(n)$ естественным образом задаются операции $+$ и \cdot на элементах поля.

Утверждение. $K_p(n)$ - векторное пространство над K размерности p^n

Теорема. Множеству всех различных гомоморфизмов $\varphi : (GF(p)^n, +) \rightarrow (\mathbb{C}, *)$ состоит из p^n различных гомоморфизмов \mathcal{X}_α ; $\alpha = (\alpha_1, \dots, \alpha_n) \in GF(p)^n$, каждый из которых однозначно определяется своим действием на вектора стандартного базиса $e_j, j \in \overline{1, n}$ следующим образом $\mathcal{X}_\alpha(e_j) = \exp(\frac{2\pi i}{p} \cdot \alpha_j)$.

Утверждение. Для любых $\alpha, \beta \in GF(p)^n$ верно $\frac{1}{p^n} \sum_{\gamma \in GF(p)^n} \mathcal{X}_\alpha(\gamma) \overline{\mathcal{X}_\beta(\gamma)} = \delta_{\alpha, \beta}$, т.е.

$$\delta_{\alpha, \beta} = \begin{cases} 1, & \alpha = \beta \\ 0, & \alpha \neq \beta \end{cases}$$

Теорема. $\{\mathcal{X}_\alpha \mid \alpha \in (GF(p))^n\}$ - базис $\mathbb{C}_p(n)$

Определение. Разложение произвольной функции $f \in \mathbb{C}_p(n)$ по базису характера $\{\mathcal{X}_\alpha \mid \alpha \in (GF(p))^n\} : f(\vec{x}) = \sum_{\alpha \in GF(p)^n} C_\alpha^f \mathcal{X}_\alpha(\vec{x})$ называется разложением f в ряд Фурье, соответствующий набору α . Комплексное число C_α^f - коэффициент Фурье функций f соответствующий набору α .

Определение. Преобразование из $\mathbb{C}_p(n)$ в \mathbb{C}^{p^n} , ставящее в соответствие каждой функции ее коэффициенты Фурье («Спектр Фурье»), будем называть преобразование Фурье.

Утверждение.

1. Пусть $\gamma \in GF(p)^n$, тогда $C_\gamma^f = \frac{1}{p^n} \sum_{\beta \in GF(p)^n} f(\beta) \overline{\mathcal{X}_\gamma(\beta)}$.

2. Пусть f - булева функция, тогда $C_\gamma^f = \frac{1}{2^n} \|(f(\vec{x}))\|$.

В некоторых случаях вместо функции f удобнее свойства функции $F(\vec{x}) = (-1)^{f(\vec{x})}$. Коэффициенты Фурье такой функции называется коэффициентом Уолша-Адамара второго рода функции $f(x)$. Обозначается $C_\alpha^F = W_\alpha^f$.

Свойства.

1. $W_\alpha^f = 1 - \frac{1}{2^{n-1}} \|(f(\vec{x}) \oplus <\alpha, \vec{x}>)\|$, где $<\alpha, \vec{x}> = \alpha_1 x_1 \oplus \dots \oplus \alpha_n x_n$.

2.

$$W_\alpha^f = \begin{cases} -2C_\alpha^f : & \alpha \neq \vec{0} \\ 1 - 2C_\alpha^f : & \alpha = \vec{0} \end{cases}$$

3. $\sum_{\alpha \in \Omega_2^n} W_\alpha^f = (-1)^{f(\bar{0})}$
4. $\sum_{\alpha \in \Omega_2^n} (W_\alpha^f)^2 = 1$
5. $\frac{1}{2^{\frac{n}{2}}} \leq \max_{\alpha \in \Omega_2^n} |W_\alpha^f| \leq 1$

Зафиксируем некоторую обратимую $2^n \times 2^n$ матрицу A над полем K . Пусть f^\downarrow - вектор столбцов значений f из $K_2(n)$. $\widetilde{f^\downarrow} = A^{-1}f^\downarrow$, тогда задано биективное отображение из $K_2(n)$ в K^{2^n} . Вектор $\widetilde{f^\downarrow}$ - представление функции f . Если столбцы матрицы A занумеровать наборами из Ω_2^n , то $f^\downarrow = \sum_{\alpha \in \Omega_2^n} g_\alpha^\downarrow \widetilde{f}(\alpha)$. Каждый столбец g_α^\downarrow есть задание некоторой функции из $K_2(n)$, A - невырожденная $\Rightarrow \{g_\alpha\}_{\alpha \in \Omega_2^n}$ - базис $K_2(n)$.

Определение. Пусть A и B - матрицы над размерами $m \times n$ и $n \times n$ над полем K соответственно. Тензорным произведением матриц A и B называется матрица $= A \otimes B$ следующего вида:

$$C = \begin{pmatrix} \alpha_{11}\beta & \alpha_{12}\beta & \dots & \alpha_{1m}\beta \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m1}\beta & \alpha_{m2}\beta & \dots & \alpha_{mn}\beta \end{pmatrix} - \text{размерность } mn \times mn.$$

Утверждение.

1. $A \otimes (B \otimes C) = (A \otimes B) \otimes C$
2. $(A + B) \otimes C = A \otimes C + B \otimes C$ ($m = n$)
 $A \otimes (B + C) = A \otimes B + A \otimes C$
3. $A, C \in K_{m;m}, B, D \in K_{n;n} \Rightarrow (A \otimes B)(C \otimes D) = AC \otimes BD$
4. $A \oplus B$ обратимо $\Leftrightarrow A$ и B обратимы, причем $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$

Лемма. Пусть A - матрица размера $2^n \times 2^n$ над K и $A = B \otimes A'$, где $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in K$, а A' - матрица размером $2^{n-1} \times 2^{n-1}$ причем обе матрицы B и A' невырожденные. Пусть столбцы матриц A и A' задают базисы функциональных пространств $K_2(n), K_2(n-1)$, функции из которых обозначаются g_α и $g'_{\alpha'}$ соответственно. Тогда $\forall \alpha \in \Omega_2^{n-1}$ верно:

$$\begin{aligned} g_\alpha(0, \alpha') &= (a\bar{x}_1 + cx_1)g_{\alpha'}(x_2; \dots; x_n) \\ g_\alpha(1, \alpha') &= (b\bar{x}_1 + dx_1)g_{\alpha'}(x_2; \dots; x_n). \end{aligned}$$

Теорема. Пусть A - тензорное произведение матриц $B_j \in K_{2 \times 2}^*$ вида $\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$, т.е. $A = \otimes \prod_{i=1}^n B_i$, тогда базисная функция g_ω , соответствующая столбцу A и занумерованная набором $\omega = (\omega_1, \dots, \omega_n)$ имеет вид $g_\omega(x_1; \dots; x_n) = \prod_{i=1}^n \omega_i(a_i\bar{x}_i + c_ix_i) + \omega_i(b_i\bar{x}_i + d_ix_i)$.

Пример.

$$B = \begin{Bmatrix} 1 & 0 \\ 0 & 1 \end{Bmatrix} - \text{тождественное преобразование.}$$

$$B = \begin{Bmatrix} 1 & 0 \\ 1 & 1 \end{Bmatrix} - \text{многочлен Жегалкина.}$$

$$B = \begin{Bmatrix} 1 & 1 \\ 1 & -1 \end{Bmatrix} - \text{коэффициент Фурье.}$$

Теорема. Пусть B - невырожденная матрица размера 2×2 над K , $A = B^{[n]}$ - тензорная степень. Тогда существует алгоритм вычисления \widetilde{f}^\downarrow по вектору f^\downarrow , имеющий сложность $O(n \cdot 2^n)$ операций поля K

Док-во: Пусть $B^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Из свойств тензорного произведения матриц вытекает, что $A^{-1} = (B^{-1})^{[n]} = D_n \cdot D_{n-1} \cdot \dots \cdot D_1$, где D_i - матрица вида:

$$D_i = \left(E_2^{[n-i]} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes E_2^{[i-1]} \right), \text{ где } E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Обозначим $f_0^\downarrow = f^\downarrow$ и $\forall i \in \overline{1, n} \mid f_i^\downarrow = D_i \cdot f_{i-1}^\downarrow$, тогда $\widetilde{f}^\downarrow = f_n^\downarrow$.

Покажем, что каждое из умножений D_i на f_{i-1}^\downarrow может быть выполнено за $O(2^n)$ операций поля K . Тогда общее количество операций, необходимое для вычисления \widetilde{f}^\downarrow по f^\downarrow будет составлять $O(n2^n)$ операций.

$$D = \left(E_{2^{n-i}} \otimes \begin{pmatrix} aE_{2^{i-i}} & bE_{2^{i-i}} \\ cE_{2^{i-i}} & dE_{2^{i-i}} \end{pmatrix} \right) = \begin{pmatrix} \hat{D}_i & & 0 \\ & \ddots & \\ 0 & & \hat{D}_i \end{pmatrix}$$

\hat{D}_i - матрица размера $2^i \times 2^i$ вида

$$\begin{pmatrix} aE_{2^{i-1}} & bE_{2^{i-1}} \\ cE_{2^{i-1}} & dE_{2^{i-1}} \end{pmatrix}.$$

Пусть теперь X^\downarrow произвольный вектор длины 2^n над полем K . Опишем алгоритм умножения D_i на X^\downarrow .

1. Разобьем X^\downarrow на 2^{n-1} частей длины 2^i , тогда

$$X^\downarrow = \begin{pmatrix} X_1^\downarrow \\ \vdots \\ X_{2^{n-i}}^\downarrow \end{pmatrix}, \text{ тогда } D_i X^\downarrow = \begin{pmatrix} \hat{D}_i X_1^\downarrow \\ \vdots \\ \hat{D}_i X_{2^{n-i}}^\downarrow \end{pmatrix}.$$

2. Каждый из векторов X_j^\downarrow разбиваем на 2 подвектора равной длины.

$$\begin{aligned} X_j^\downarrow &= \begin{pmatrix} X_{j_0}^\downarrow \\ X_{j_1}^\downarrow \end{pmatrix}, \text{ тогда } D_i X_j^\downarrow = \begin{pmatrix} aE_{2^{i-1}} & bE_{2^{i-1}} \\ cE_{2^{i-1}} & dE_{2^{i-1}} \end{pmatrix} \begin{pmatrix} X_{j_0}^\downarrow \\ X_{j_1}^\downarrow \end{pmatrix} = \\ &= \begin{pmatrix} aE_{2^{i-1}} X_{j_0}^\downarrow + bE_{2^{i-1}} X_{j_1}^\downarrow \\ cE_{2^{i-1}} X_{j_0}^\downarrow + dE_{2^{i-1}} X_{j_1}^\downarrow \end{pmatrix} = \begin{pmatrix} aX_{j_0}^\downarrow + bX_{j_1}^\downarrow \\ cX_{j_0}^\downarrow + dX_{j_1}^\downarrow \end{pmatrix}. \end{aligned}$$

Таким образом для вычисления $\widetilde{f^\downarrow}$ необходимо $O(n \cdot 2^n)$ операций.