

Лекции по дискретной математике

me and boyz

21 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.	6
2.1	Метод Блейка	8
2.2	Метод Квайна	9
3	Эквивалентность функций относительно групп преобразований.	10
3.1	Группы инерции	10
3.2	Инварианты, нахождение групп инерции и проверка эквивалентности.	13
4	Представление дискретных функций в базисах функциональных пространств. Алгоритм БПФ.	14
5	Трансверсали.	18
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 $\|f\| = |\{\vec{\alpha} \in \Omega^n \mid f(\vec{\alpha}) = 1\}|$. N_f - носитель булевой функции.

Определение. Функция от $n-1$ переменных, определяемая равенством $\varphi(a_1; \dots; a_{n-1}) = f'(a_1; \dots; a_{i-1}; b; a_{i+1}; \dots; a_{n-1})$, 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 функций φ - подфункции f .

Если $f(a_1; \dots; a_{i-1}; 0; a_{i+1}; \dots; a_n) = f(a_1; \dots; a_{i-1}; 1; a_{i+1}; \dots; a_n), \forall a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n \in \Omega$, 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 $f_j(A_1; \dots; A_n)$ - она 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 функция 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 $f(a_1; \dots; a_n) = f_j(b_1; \dots; b_m)$, 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 $\mathbb{K} \not\subset G$, 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. $\mathbb{K} \not\subset T_1$, 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. $\mathbb{K} \not\subset M$, 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 $f(a_1; \dots; a_{j-1}; x_j; a_{j+1}; \dots; a_n) \equiv \overline{x_j}$, 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 $f_4 \in \mathbb{K} \mid f_4 \notin S \Rightarrow \exists (a_1; \dots; a_n) \mid f_4(a_1; \dots; a_n) = f_4(\overline{a_1}; \dots; \overline{a_n}) = \text{const} \in \{0, 1\} \in [\mathbb{K}]$. 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:

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

$C_1 = 1$, 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 $f(x_1, \dots, x_n) = \&_{(b_1, \dots, b_k) \in \Omega^k} x_{i_1}^{\bar{b}_{i_1}} \dots x_{i_k}^{\bar{b}_{i_k}} f_{i_1, \dots, i_n}^{\bar{b}_{i_1}, \dots, \bar{b}_{i_n}}(x_1, \dots, x_n)$

Замечание. Аналогичным образом определяется элементарная дизъюнкция (ДНФ).

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

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

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

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 неленейности 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 разности $n - k$) 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 сокращённой 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.

2.1 Метод Блейка

Метод Блейка строит из ДНФ сокращённую 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: Сокращённая 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 сокращённой 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 $n-1$ переменных 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 - имплеканта 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.

2.2 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.

3 Эквивалентность функций относительно групп преобразований.

3.1 Группы инерции

Определение. Подстановкой непустого множества M называют любое биективное отображение M на себя. При известном n будем обозначать: $f(x_1; \dots, x_n) = f(\vec{x})$.

Определение. Пусть $f(\vec{x})$ и $h(\vec{x})$ - функции из $F_k(n)$ и G - произвольная группа подстановок множества Ω_k^n . Говорят, что f эквивалентно h относительно группы G , если существует подстановка $g \in G \mid \forall \vec{\alpha} \in \Omega_k^n$ выполняется:

$$f(\vec{\alpha}) = h(g(\vec{\alpha})).$$

Обозначение : $f \stackrel{G}{\sim} h$.

Утверждение.

1. $f \stackrel{G}{\sim} f$
2. $f \stackrel{G}{\sim} h \Leftrightarrow h \stackrel{G}{\sim} f$
3. $f \stackrel{G}{\sim} h, h \stackrel{G}{\sim} r \Rightarrow f \stackrel{G}{\sim} r$

$\stackrel{G}{\sim}$ - отношение эквивалентности.

Таким образом $F_k(n)$ разбивается на классы эквивалентности. Класс, содержащий функцию f , будем называть $[f]_G$. Очевидно $1 \leq |[f]_G| \leq |G|$.

Определение. Функция $f(\vec{x}) \in F_k(n)$ - называется инвариантной относительно подстановки $g \in G < S_{\Omega_k^n}$, если $f(g(\vec{x})) = f(\vec{x})$, относительно группы G , если она инвариантна относительно любой подстановки из этой группы.

Утверждение. Множество подстановок $g \in G$, относительно которых функция f инвариантна образует подгруппу в группе G .

Определение. Подгруппа, определенная в утверждении, несёт название - Группа инерции - функции f в группе G . Обозначение: $I_G(f)$.

Теорема. Если $f \in F_k(n)$ и $G < S_{\Omega_k^n}$, то $|[f]_G| = \frac{|G|}{|I_G(f)|}$

Определение. Орбитой группы подстановок $G < S_{\Omega_k^n}$, содержащей элемент α , называется множество

$$\Delta_\alpha = \{\beta \in \Omega_k^n \mid \exists g \in G \mid \beta = g(\alpha)\}.$$

Утверждение. f инвариантна относительно группы $G \Leftrightarrow$ на элементах каждой орбиты она принимает постоянные значения. То есть $\forall p \in \Delta_\alpha \mid f(\beta) = f(\alpha)$.

Следствие. G - транзитивна $\Leftrightarrow f$ инвариантна $\Leftrightarrow f \equiv \text{const}$.

Следствие. Число функций k - значной логики инвариантно относительно группы G равно $k^{\nu(G)}$, где $\nu(G)$ - число орбит группы G .

Пример.

1. Группа подстановок координат векторов $\alpha \in \Omega_k^n$:

$$g_s(a_1, \dots, a_n) = a_{i_1}; \dots; a_{i_n} \text{ в соответствии с перестановкой } g_s = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$$

Обозначение: S_n .

2. Группа сдвигов: Σ_n . Пусть $\alpha = (a_1; \dots; a_n) \in \Omega_k^n$, тогда

$$\Sigma_n = \{g_\alpha \mid g_\alpha(c_1; \dots; c_n) = (c_1 + a_1; \dots; c_n + a_n); \alpha, \vec{c} \in \Omega_k^n\}$$

Суммирование ведется по модулю k .

3. Группа Джевонса Q_n :

$$Q_n = \langle \Sigma_n; S_n \rangle.$$

4. $GL(n; k)$ - полная линейная группа. Пусть A - невырожденная матрица размеров $n \times n$ над \mathbb{Z}_k , тогда

$$GL(n; k) = \{q_A \mid q_A(a_1; \dots; a_n) = (a_1; \dots; a_n) \cdot A; A \in (\mathbb{Z}_k)_{n \times n}^*\}$$

5. Полная аффинная группа $AGL(n; k) = \langle GL(n; k); \Sigma_n \rangle$.

Диаграмма вложения группы:

$$\begin{array}{ccc} S_n & \longrightarrow & GL(n; k) \\ & \searrow & \downarrow \\ & & AGL(n; k) \\ \Sigma_n & \longrightarrow & Q_n \\ & \nearrow & \uparrow \\ & & AGL(n; k) \end{array}$$

$\Sigma_n; Q_n; AGL(n; k)$ - транзитивные \Rightarrow инвариантны относительно них только константы.

Орбитами группы S_n являются множества векторов одинакового веса. Число функций одинакового веса инвариантных относительно S_n равно $k^{\binom{k+n-1}{k-1}}$.

Теорема. Орбитами группы $GL(n; k)$ являются все множества $M_\alpha = \{(a_1; \dots; a_n) \in \Omega_k^n \mid \text{НОД}(a_1; \dots; a_n; k) = d\}$, где $d \mid k$.

Следствие. Число функций n - значной логики (от n -переменных), инвариантных относительно $GL(n; k)$ равно $k^{\nu(k)}$, где $\nu(k)$ - число делителей k .

Теорема. Пусть $T_k(n)$ - множество всех функций k -значной логики с тривиальной группой инерции в $AGL(n; k)$. Тогда

$$\lim_{n \rightarrow \infty} \frac{|T_n(k)|}{|F_k(n)|} = 1$$

Док-во: 1) Оценим сверху число неподвижных точек нетождественного аффинного преобразования $g \in AGL(n; k)$. Рассмотрим уравнение $g(\vec{x}) = \vec{x}A + \alpha; \alpha \in Z_k^n$; A -невырожденная матрица над Z_k ; В матричном виде уравнение переписывается следующим образом:

$$\vec{x}(E - A) = \alpha.$$

Если $A = E$, то \nexists решений, так как $\vec{\alpha} \neq \vec{0}$ (g - нетождественное преобразование). Пусть $C = (C_{ij})_{n \times n} = E - A \neq 0$.

Не ограниченная общность $c_{11} \neq 0$, тогда $c_{11}x_1 + \dots + c_{n1}x_n = a_1$ - слогаемые системы, если зафиксировать $x_2; \dots; x_n$ произвольными значениями из Z_k , то полученное уравнение будет иметь не более $(C_n; k)$ решений, а так как $C_{11} \neq 0$, то число решений при произвольной фиксации $x_2; \dots; x_n \leq \frac{k}{2} \rightarrow$ для всего уравнения имеем $(\frac{k}{2})^n$. (то есть число решений $\vec{x}(E - A) = \alpha$, не превосходит $(\frac{k}{2})^n \leq \frac{k^n}{2}$.)

2) Поскольку количество точек (неподвижных) аффинной подстановки $(k^{l(g)})$, где $l(g)$ -число циклов не превосходят $\frac{k^n}{2}$, то количество независимых циклов в её разложении может превосходить $\frac{3k^n}{4}$. ($\frac{k^n}{2}$ - циклов длины 1; $\frac{k^n}{4}$ - циклов длины 2)

\rightarrow количество функций инвариантных относительно фиксированных подстановок g не превосходят $k^{\frac{3k^n}{4}}$, так как функция должна принимать одинаковые значения на элементах каждой орбиты.

3)

$$|AGL(n; k)| \leq k^{n^2+n} \rightarrow k^{\frac{3k^n}{4}+n^2+n} \rightarrow \lim_{n \rightarrow \infty} \frac{|T_n(k)|}{|F_k(n)|} = \frac{k^{k^n} - k^{\frac{3k^n}{4}+n^2+n}}{k^{k^n}} = 1$$

Классы эквивалентности по \sim^G назовем G -типом. Для осуществления полной классификации необходимо построить список представителей G типов. $f^{(1)}; \dots; f^{l(G)}; l(g)$ - число G -типов. Строится последовательность $f_1; f_2; \dots$. Среди них могут быть одинаковые представители из какого-то класса. Полагаем $f^{(1)} = f_1$ и считаем:

$|I_G(f^{(1)})|$, проверяем $f_2 \in I_G(f^{(1)})$; если нет, то считаем:

$|I_G(f^{(2)})|, f^{(2)} = f_2$ и так далее \dots

Останавливаемся, когда :

$$\sum_{i=1}^l \frac{|G|}{|I_G(f^{(i)})|} = k^{k^n}$$

то есть необходимость вычисления порядка групп инерции. Значение параметра $l(G)$ упрощает метод. Задача поиска этого параметра носит название задачи перечисления G - типов.

3.2 Инварианты, нахождение групп инерции и проверка эквивалентности.

Определение. Отображение φ - называется инвариантом группы G , если для любого $g \in G$ и произвольной $m \in M$ справедливо равенство:
 $\varphi(g(m)) = \varphi(m)$.

Инвариант φ называется полным, если из $\varphi(m_1) = \varphi(m_2) \rightarrow$ что элементы m_1 и m_2 лежат на одной орбите группы G . Принимая во внимание факт, что для G , действующей на $F_k(n)$, орбита будет являться G - типом, сформируем правило проверки эквивалентности f_1 и $f_2 \in F_k(n)$.

Пусть φ - инвариант группы G , действующей на $F_k(n)$, если φ -полный, то $\varphi(f_1) = \varphi(f_2)$ равносильно тому, что $f_1 \stackrel{G}{\sim} f_2$;

Если φ неполный инвариант, то $\varphi(f_1) = \varphi(f_2)$ - только необходимое условие эквивалентности. В случае, когда равенство выполнено, надо проверять другие инварианты:

$$\sqsupset k = ?$$

1. Для $AGL(n; k); S_n; \sum_n; Q_n$ инварианты - вес, степени нелинейности.
2. Q_n - число простых импликант, число существенных переменных.
3. S_n - число одночленов в многочлене Жегалкина.

Пример. Пусть $f(x_1; x_2; x_3) = x_1 \oplus x_2$

$$f_2(x_1; x_2; x_3) = x_1 \oplus x_2 \oplus x_3$$

Они не эквивалентны относительно $S_n; Q_n$, но $f_2(x_1; x_2; x_3) = f_1((x_1; x_2; x_3)A)$

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

$$x_1 \oplus x_2; x_1; x_3.$$

Теорема. Для любого натурального $m \geq 2$ и произвольной группы G :
 $|G| = m, \exists n$ и $f \in F_2(n) \mid I_{S_n}(f) \cong G$.

4 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}^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 $C_0^f = \frac{1}{2^n} \|(f(\vec{x}))\|$.

В некоторых случаях вместо функции f удобно рассматривать свойства функции $F(\vec{x}) = (-1)^{f(\vec{x})}$. Коэффициенты Фурье такой функции называется коэффициентом Уолша-Адамара второго рода функции $f(\vec{x})$. 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 $K_2(n)$. $f^\downarrow = A^{-1}f^\downarrow$, 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 $m \times m$ 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'_α 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 $B_i \in K_{2 \times 2}^*$ вида $\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$, т.е. $A = \otimes_{i=1}^n B_i$, тогда базисная функция g_ω , соответствующая столбцу A и занумерованная набором $\omega = (\omega_1, \dots, \omega_n)$ имеет вид $g_\omega(x_1; \dots; x_n) = \prod_{i=1}^n \bar{\omega}_i(a_i x_i + c_i \bar{x}_i) + \omega_i(b_i \bar{x}_i + d_i x_i)$.

Пример.

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

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

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

$$B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} - \text{вырожденная матрица.}$$

Теорема. Пусть B - невырожденная матрица размера 2×2 над K , $A = B^{[n]}$, где $[n]$ - 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 \mathfrak{X}^\downarrow произвольный вектор длины 2^n над полем K . Опишем алгоритм умножения D_i на \mathfrak{X}^\downarrow .

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

$$\mathfrak{X}^\downarrow = \begin{pmatrix} \mathfrak{X}_1^\downarrow \\ \vdots \\ \mathfrak{X}_{2^{n-i}}^\downarrow \end{pmatrix}, \text{ тогда } D_i \mathfrak{X}^\downarrow = \begin{pmatrix} \hat{D}_i \mathfrak{X}_1^\downarrow \\ \vdots \\ \hat{D}_i \mathfrak{X}_{2^{n-i}}^\downarrow \end{pmatrix}.$$

2. Каждый из векторов $\mathfrak{X}_j^\downarrow$ разбиваем на 2 подвектора равной длины.

$$\begin{aligned} \mathfrak{X}_j^\downarrow &= \begin{pmatrix} \mathfrak{X}_{j_0}^\downarrow \\ \mathfrak{X}_{j_1}^\downarrow \end{pmatrix}, \text{ тогда } D_i \mathfrak{X}_j^\downarrow = \begin{pmatrix} aE_{2^{i-1}} & bE_{2^{i-1}} \\ cE_{2^{i-1}} & dE_{2^{i-1}} \end{pmatrix} \begin{pmatrix} \mathfrak{X}_{j_0}^\downarrow \\ \mathfrak{X}_{j_1}^\downarrow \end{pmatrix} = \\ &= \begin{pmatrix} aE_{2^{i-1}} \mathfrak{X}_{j_0}^\downarrow + bE_{2^{i-1}} \mathfrak{X}_{j_1}^\downarrow \\ cE_{2^{i-1}} \mathfrak{X}_{j_0}^\downarrow + dE_{2^{i-1}} \mathfrak{X}_{j_1}^\downarrow \end{pmatrix} = \begin{pmatrix} a\mathfrak{X}_{j_0}^\downarrow + b\mathfrak{X}_{j_1}^\downarrow \\ c\mathfrak{X}_{j_0}^\downarrow + d\mathfrak{X}_{j_1}^\downarrow \end{pmatrix}. \end{aligned}$$

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

5 Трансверсали.

Определение. Пусть 2^X - булеан множества X , т.е. совокупность всех подмножеств множества X . Пусть $(X_1; \dots; X_n)$ - некоторая n -выборка из булеана. Вектор $(x_1; \dots; x_n)$, состоящий из элементов множества X , называется трансверсалью семейства $(X_1; \dots; X_n)$, если выполнены следующие отношения:

1. $x_i \in X_i$; $1 \leq i \leq n$;
2. $x_i \neq x_j$; $i \neq j$; $1 \leq i, j \leq n$.

Иными словами имеем систему различных представителей семейства $(X_1; \dots; X_n)$.

Обозначается $(x_1; \dots; x_n)$ тр. $(X_1; \dots; X_n)$

Теорема. (Критерий Ф.Холла) Для того, чтобы семейство $(X_1; \dots; X_n)$ имело трансверсаль, необходимо и достаточно, чтобы $\forall k \in \overline{1, n}$ и $\forall k$ -сочетания $i \leq j_1 \leq \dots \leq j_k \leq n$ выполнялось условие:

$$|X_{j_1} \cup \dots \cup X_{j_k}| \geq k. (*)$$

Доказательство:

Необходимость:

Пусть $\exists (x_1; \dots; x_n)$ тр. $(X_1; \dots; X_n)$. Тогда $\forall k \in \overline{1, n}$ и \forall набора $1 \leq j_1 \leq \dots \leq j_k \leq n$ имеем $x_{j_1} \in X_{j_1}, \dots, x_{j_k} \in X_{j_k}$ и $x_{j_s} \neq x_{j_t}$ при $j_t \neq j_s \Rightarrow |X_{j_1} \cup \dots \cup X_{j_k}| \geq k = |x_1; \dots; x_k|$.

Достаточность:

Индукция по n . Пусть $n = 1$, тогда $|X_1| \geq 1 \Rightarrow x_1$ тр X_1 . Предположение индукции: $\forall n' < n$ из условия $(*) \Rightarrow \exists$ трансверсали для n' множеств.

Рассмотрим 2 случая:

а) Для всех $1 \leq k \leq n-1$ и $\forall j_1 < \dots < j_k \leq n$ верно $|X_{j_1} \cup \dots \cup X_{j_k}| \geq k+1$ **(**)** При $k = 1$ $|X_1| \geq 2 \Rightarrow \exists$ трансверсаль x_1 тр. X .

Рассмотрим семейство $(X'_2; \dots; X'_n)$, где $X'_i = X_i \setminus \{x_1\}$, $2 \leq i \leq n$. Согласно **(**)** для этого семейства при $\forall 1 \leq k < n$ и $\forall 2 \leq j_1 < \dots < j_k \leq n$ имеем $|X'_{j_1} \cup \dots \cup X'_{j_k}| \geq k$ и по предположению индукции существует $(x_2; \dots; x_n)$ тр. $(X'_2; \dots; X'_n)$, но тогда (x_1, x_2, \dots, x_n) тр. $(X_1; \dots; X_n)$.

б) $\exists k$ и такое сочетание $1 \leq j_1 < \dots < j_k \leq n$, что $|X_{j_1} \cup \dots \cup X_{j_k}| = k$.

Т.к. можно перенумеровать подмножества, то не ограничивая общности считаем $|X_1 \cup \dots \cup X_k| = k$. По предположению индукции \exists трансверсаль $(x_1; \dots; x_k)$ тр. $(X_1; \dots; X_k)$, т.к. $k < n$ и $\{x_1; \dots; x_k\} = |X_1 \cup \dots \cup X_k|$.

Рассмотрим семейство множеств $(X'_{k+1}; \dots; X'_n)$, где $X'_i = X_i \setminus \{x_1; \dots; x_k\}$, $k+1 \leq i \leq n$. Для этого семейства верно условие **(*)**, т.к. $\forall 1 \leq l \leq k$ и $\forall 1 \leq \nu_1 < \dots < \nu_l \leq n - k$ имеем $|X'_{k+\nu_1} \cup \dots \cup X'_{k+\nu_l} \cup X_1 \cup \dots \cup X_k| - k \geq$ (Штрихи можно снять, т.к. $\{x_1; \dots; x_k\}$ и так содержится в $X_1 \cup \dots \cup X_k$).

$\geq k+l-k=1$, т.к. верно условие (*) для нештрихованных множеств. Таким образом $\exists(x_{k+1}; \dots; x_n)$ тр. $(X'_{k+1}; \dots; X'_n) \Rightarrow \exists(x_1; \dots; x_n)$ тр. $(X_1; \dots; X_n)$.

Пример. 1. Представители различных классов эквивалентности

Пример. 2. Остовное дерево графа. Его ребра - трансверсали множества рёбер графа.

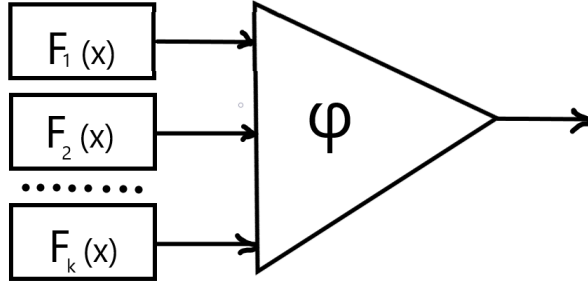
Определение. Пусть $P = GF(q)$ - конечное поле из q элементов, $q = p^d$, где $p \in \mathbb{P}$ (простое). Пусть $F(x)$ - реверсивный многочлен (т.е. $F(0) \neq 0$) над P . Найдутся $a \in P$ и $k \in \mathbb{N} : F(x) | x^k - a$. Наименьшее k с таким свойством назовём редуцированным периодом (Обозначение: $T_{red}(F)$). Элемент a назовём мультипликатором многочлена $F(x)$. Обозначение $(Mult(F))$ - множество всех мультипликаторов.

Пусть $F(x) | x^t - b$, где $t = T_{red}(F)$.

Утверждение.

1. $Mult(F) = \langle b \rangle$;
2. $t * |Mult(F)| = T_{red}(F)$;
3. Если f - примитивный, то $t = \frac{q^m - 1}{q - 1}$, где $m = deg(f(x))$, $Mult(F) = P^*$, $b = F(0)$.

Рассмотрим следующую модель ДСЧ (Датчик случайных чисел).



Пусть F_1, \dots, F_k - многочлены попарно взаимнопростых степеней m_1, \dots, m_k .

Тогда $T = [T(F_1), \dots, T(F_k)] = \frac{(q^{m_1} - 1) \dots (q^{m_k} - 1)}{(q - 1)^{k-1}}$.

$(q^{m_1} - 1) \dots (q^{m_k} - 1)$, каждый из них лежит на цикле длины T и таких циклов $(q - 1)^{k-1}$. Будем считать, что начальное состояние $\vec{\alpha}_0 = (u_1(0), \dots, u_1(m_1 - 1), u_2(0), \dots, u_2(m_2 - 1), \dots, u_k(0), \dots, u_k(m_k - 1))$ выбирается из множества S всех состояний, тогда $\vec{\alpha}_i = (u_1(i), \dots, u_1(i + m_1 - 1), \dots, u_k(i), \dots, u_k(i + m_k - 1)) \in S$. Последовательность $((\vec{\alpha}_i)_{i=0}^\infty)$ - чисто периодическая с периодом T . Каждый вектор $\vec{\alpha} \in S$ запишем в виде $\vec{\alpha} = (\vec{\alpha}(1); \dots; \vec{\alpha}(k))$, где $\vec{\alpha}(j) \in P^{m_j} \setminus \{0\}$.

Зададим отношение \sim : $\forall \vec{\alpha}, \vec{\beta} \vec{\alpha} \sim \vec{\beta} \Leftrightarrow \exists c_1, \dots, c_k \in P^* | \vec{\alpha}(j) = c_j \vec{\beta}(j) \forall j \in \overline{1, k}$

Пусть a_j - корень многочлена $F_j(x)$ в расширении $GF(q^{m_j})$ поля P , где $j \in \overline{1, k}$. Из пункта 3 утверждения следует, что $b_j = a_j^{\frac{q^{m_j}-1}{q-1}} = a_j^{T_{red}(F_j)}, i \in \overline{1, k}$, т.е. имеем мультипликатор многочлена $F_j(x)$. Пусть $m = m_1; \dots; m_k$, положим $\forall \vec{\alpha}, \vec{\beta} \in S \vec{\alpha} \stackrel{red}{\sim} \vec{\beta} \Leftrightarrow \exists i \in \{0, \dots, q-2\} | \vec{\alpha}(j) = \vec{\beta}(j) * b^{m-i/n_j}, \forall j \in \overline{1, k}$.

Для любого вектора \exists ровно $q-1$ вектор, находящийся с ним в отношении $\stackrel{red}{\sim}$.

Теорема. Пусть $\vec{\gamma}_1, \vec{\gamma}_2 \in S$, тогда

$$1) \vec{\gamma}_1 \sim \vec{\gamma}_2$$

$$2) \vec{\gamma}_1 \not\stackrel{red}{\sim} \vec{\gamma}_2$$

Тогда $\vec{\gamma}_1$ и $\vec{\gamma}_2$ лежат на различных циклах.