построить посл-ко двоев каждый корень и определить его степени, соотв. эл-ту исходной группы.

Вычисл. все степени дан. эл-в получ. таблицу характеров.
Строки в этой табл. – лин. независ. векторы, преобраз. век-р. разл-ся по этим векторам.
Получ. матрица – мат. преобраз. i

В F_{2^m} (Галуа) в кач-ве образ-го эл-та $\varepsilon = 2 \Rightarrow$ FMC матрица, у кот-й элементы имеют вид $2^{\alpha k}$, где $\alpha, k = 0, 1, 2 \ldots n-1$.

11.10.06.

Свойства матрицы FMC

Пусть дано поле F_{2^m}, $n = 2^m - 1$.
Для данного поля полином $x^n + 1$.

$x^n + 1 = (x+1)(x+2)\ldots(x+n)$, $a \in F_{2^m}$
разделим "уголком" $x^n + 1$ на $x + a$.
Обозначим инд-м i шаг деления.

$$\begin{array}{l|l} x^n + 1 & x + a \\ \underline{x^n + ax^{n-1}} \quad i = 1 & x^{n-1} + ax^{n-2} + a^2x^{n-3} + \ldots + a^{n-1} \\ \quad ax^{n-1} + 1 & \\ \quad \underline{ax^{n-1} + a^2x^{n-2}} \quad i = 2 & a^n = 1. \\ \qquad a^2x^{n-2} + 1 & \\ \qquad \underline{a^2x^{n-2} + a^3x^{n-3}} \quad i = 3 & \\ \qquad\quad a^3x^{n-3} + 1 & \\ \qquad\quad \ldots & \\ i = n \qquad a^{n-1}x + 1 & \\ \qquad\quad \underline{a^{n-1}x + a^n} & \\ \qquad\qquad 0 & \end{array}$$

Частное от деления (x^n+1) на $(x+a)$ имеет вид $x^{n-1} + ax^{n-2} + a^2x^{n-3} + \ldots + a^{n-2}x + a^{n-1} = A(x)$

Рассмотрим строку коэф-в:
$1 \; a \; a^2 \; a^3 \ldots a^{n-2} \; a^{n-1}$

Стр-ка коэф. совп-т со строкой ТМС матрицы.

Построим полином, у кот-го x в старш. степени с коэф a^{n-1} — $\overleftarrow{A}(x)$

$$a^{n-1}x^{n-1} + a^{n-2}x^{n-2} + \ldots + a^2x^2 + ax + 1 \quad (3.1)$$

$\overleftarrow{A}(x) \cdot \frac{a}{a}$, где $a^{-1} = b$

$$\overleftarrow{A}(x) = b\left[x^{n-1} + a^{n-1}x^{n-2} + \ldots + a^3x^2 + a^2x + a\right] \quad (3.2)$$

$a^n = 1$.

$a^{n-1} \cdot a = a^n = 1 \Rightarrow a^{n-1} = a^{-1} = b$

$a^{n-2} = a^{n-1}a^{-1} = b^2$

$a^{n-3} = b^3$

Записываем (3.2) в виде.

$$\overleftarrow{A}(x) = b\left[x^{n-1} + bx^{n-2} + b^2x^{n-3} + \ldots + b^{n-2}x + b^{n-1}\right] \quad (3.3)$$

Содержимое кв. скобки имеет стр-ру полинома $A(x)$

Ранее было получено:

$$A(x) = \frac{x^n+1}{x+a}$$

$$\overleftarrow{A}(x) = b\left[\frac{x^n+1}{x+b}\right] \quad (3.4).$$

Если сост-ть полином из строки ТМС матрицы, где x в старш. степени имеет коэф a^{n-1} имеет вид (3.4)

$\Rightarrow$ св-во строк мат-цы ТМС

Преобразование Уолша

Примем ту же модель, что и для ТМС преобр., сделав изменения:

– обл. значения ф-й, кот. явл. моделью значений преобраз-го вектора, опр-ние в обл. компл. чисел.

Пусть даны группы G_1 и G_2, тогда G – тензорный, внешний, декарт. произв. G_1 на G_2

$G = G_1 \otimes G_2 \Rightarrow$

$\Rightarrow$ Эл-ты $g \in G$ имеют вид $g = (g_1, g_2)$

$g_1 \in G_1$, $g_2 \in G_2$.

$g' = (g_1', g_2')$

$g'' = (g_1'', g_2'')$, $g', g'' \in G$, тогда

$g' \cdot g'' = (g_1' \cdot g_1'', g_2' g_2'')$, где

опер-е $g_1' g_1''$ опр-ся группой G_1

$g_2' g_2''$ опр-ся группой G_2

Данный вид произв. можно расп-ть на любое кол-во групп G_i

Рассмотрим постр-е преоб-й на примере прмоб-й 8.

$8 = 2^3$

Пусть дана H_2, сост-я из эл-в $\underline{e, a}$

Постр-м H 8-го порядка как внеш произв. H_2

$H = H_2 \otimes H_2 \otimes H_2$

Тогда эл-ми гр-пы H будут

(e, e, e) ...

(e, e, a) ...

(e, a, e) ... (a, a, a)

Построим матрицу преобраз-й данн. группы.

Осущ. отображ. группы H_2 с эл-ми e, a в поле компл. чисел, т.е. в группу кв-х корней из 1

$\sqrt{1} = +1, -1$, $\varepsilon = -1$ – образ-й эл-т.

Если $H = G_1 \otimes G_2 \otimes G_3$, то хар-ры этой гр. рассчит-ся как

$$X = \varepsilon_1^{\alpha_1 k_1} \varepsilon_2^{\alpha_2 k_2} \varepsilon_3^{\alpha_3 k_3}$$

Найдем хар-р для гр-пы $H = H_2 \times H_2 \times H_2$ и обозначим $\alpha_i \to u_i$, $k_i \to x_i$

$\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = \varepsilon = -1$.

$X = (-1)^{\sum_{i=1}^{3} x_i u_i}$ (3.5) => расп-е на большее число сомн-х H_2

Введем в-р x, как совокуп. компон. x_i

$x = (x_1, x_2, x_3)$

$u = (u_1, u_2, u_3)$

Тогда Σ можно рассм-ть как скаляр. произв этих в-в. $\langle x, u \rangle$ =>

=> $X = (-1)^{\langle x, u \rangle}$ (3.6)

Фиксир. знач-я двоич. в-ра u. Упоряд-м в-ры x и u в соотв. с их ест-м двоич. порядком. При данном значении u, подст. посл-но знач-я x в (3.6) получим строку искор. мат-цы. Изменяя u получим всю мат-цу => мат-ца преобраз-я Уолша – Адамара

Она состоит из эл-в 1 и -1. Если взять двоич. вектор длиной 2^3, то с помощью мат-цы можно реализ. преоб-е Уолша – Адамара.

При рассм-ии двоич. век-в компон. его комп-ты считают знач-ем булевой ф-ии при конкр-м знач. x. (с ест-м порядком суммир-я x) Пусть это ф-я $f(x)$, тогда назовем преобр-е У-А I-го рода

$$W_f(u) = \sum_{\forall x} f(x)(-1)^{\langle x, u \rangle} \quad (3.7)$$

нет куска...

т.е. несколько полиномов м. определять одну и ту же ф-ю. Поэтому будем реализ. данную ф-ю с помощью циклотомич. приведенных полиномов.

Рассм. их к-во:

пусть поле F_{2^m} имеет $m = p$, где p – простое число, тогда все циклотомич. классы имеют одинак. длину.

$F_{2}5$

6 циклот. классов по 5 элементов,

$m_s = 5 = const$, тогда различных циклот. прив. полиномов будет $2^5, 2^5, \ldots, 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^5 =$ (шесть классов)

$= 2^{30}$.

При $m = 5$ $\quad 2^{2^5} = 2^{32}$ – функций алгебр.

Пусть $m \neq p$

$F_2 4$ $\quad$ 3 циклот. класса длиной 4

5

$\Rightarrow$ Неприводимых полиномов не хватает.

Пусть $m \neq p$. $F_2^4 \Rightarrow$ 3 неприводимых класса длиной $n_s = 4$ и 1 класс $n_s = 2$
Число неприводимых приведённых полиномов:
$2^4 \cdot 2^4 \cdot 2^4 \cdot 2^2 = 2^{14}$
Булевых ф-ий:
$2^{2^4} = 2^{16}$
Если $m = p$, то все неприводимые приведённые полиномы не являются полиномами по следу.
Если m - непростое число как F_2^4, то полином $a_s x^s$, где $s \in$ классу не тех длины не все являются неприводимыми последовательностями

Для реализации всех булевых функций введём $c_0, c_{2^m-1} \in F_2$
$\alpha \in F_{2^n}$ примем $tr_m(\alpha) = 1$.
$P'(x) = c_0 \cdot \alpha + P(x) + c_{2^m-1} \alpha x^{2^m-1}$.
$\Rightarrow$ полиномов хватает

Векторное пространство

Рассмотрим мн-во A эл-тов кот-го назовем векторами и опр-м Σ двух век-в.

Пусть F - поле и $\alpha \in F$, $\beta \in F$, $a, b \in A$
$\Rightarrow$ мн-во A - векторное пр-во, если

1. Элементы мн-ва A с Σ - т Абелеву группу по сложению.
2. Дистр-ти $\alpha a \in A$
3. Выполн-ся след. соотн-я
   $\alpha\beta a = \alpha(\beta a) = (\alpha\beta)a$
   $(a+b)\alpha = a\alpha + b\alpha$
   $(\alpha+\beta)a = \alpha a + \beta a$

1. Подпространства

Подмн-во A_1 явл. подпростр-ва, если для $a, b \in A_1$, $(a+b) \in A_1$,
$\alpha a \in A_1$
В век-м пр-ве опр-м базис $\Rightarrow \forall$ век-р однозначно разложить по базису и своим коорд-там

Ортогональное дополнение подпростр-ва

Пусть A - пр-во и A_1 - подпр-во
Пусть канд. б-р $a \in A_2 \perp \forall b \in A_1$.
Тогда A_2 - подпр-во $\perp A_1$
каждый базисный б-р $\perp \forall$ базис. б-ру A_1
Подпр-во A_2 будет ортогон-м дополн. A_1, если $A = A_1 + A_2$, т.е. $\forall$ б-р $c \in A$ опр-ся как Σ б-ров $a \in A_2$, $b \in A_1$

Афинные пространства

Введем в векторном пр-ве понятие $(\cdot)$.

С кажд. век-м связаны 2 (·) означ. начало и конец.
Вект-е пр-во, дополн-е мн-м (·) — аффинное пр-во, если выполн-ся 2 условия:

1. $\forall$ (·) M и вектора x с началом в дан. (·) всегда найдется (·) N $\overline{MN} = x$

2. $\forall$ 3 (·) M, N, P най-ся 3 таких вектора, что
$$\overline{MN} + \overline{NP} = \overline{MP}$$

Каждой (·) можно пост-ть в соотв. вектор, исход. из начала коорд в дан. (·), тогда при выб. базисе можно ввести коорд. (·)

Пусть коорд (·) $x_i \in A$, разм-ть вект. пространства — n $\Rightarrow$ кажд. (·) хар-ся строкой коорд: $(x_1, x_2, \dots x_n)$

Все афин. пр-ва уст-вы одинак. и различ. только полем и пр-м.

Плоскости.

Рассм. аффин. пр-во A^n
Запишем СУ:

$$\begin{cases} a_{11} x_1 + a_{12} x_2 + \dots + a_{1n} x_n = b_1 \\ a_{21} x_1 + a_{22} x_2 + \dots + a_{2n} x_n = b_2 \\ \dots \\ a_{n1} x_1 + a_{n2} x_2 + \dots + a_{nn} x_n = b_n \end{cases}$$

Рассм. $x_1, x_2 \dots x_n$ как (·)
Пусть ранг матрицы коэф. в левой части $= 2$.
Пусть $k = n - 2$

Тогда мн-во (·) — реш-е ур-ий $\Rightarrow$ k-мерная плоскость.
Если $k = 1$ — прямая
$k = n - 1$ — гиперплоскость