Шаг	Символ (см. разр)	Вес симв	Слово (см разряд)
0	0111111010 1	8	1011000111111000010010 01
	0100110 3110	6	
	0001100000 11	4	
1	1111111010 10	8	0110001111100000100100 11
	1100111000 1	6	
	1001102 1100	6	
2	1010011 0 1 1	7	1100011111000010010011 0
	1001010 1100	5	
	1100000000 01	3	
3	0010001 1 01	4	1000111111000010010011 01
	0010001 0110	4	
	011 1011101 1	3	
4	0010001 1010	4	0001111100001001001 10 11
	0001000000 1	2	0001000000 01 ×1
			0000111100101001 0 1 0 11

Сдвигаем на 9 раз

1011000011110010100101 1

Прибавляем к синдрому

2) ~~Прибавляем~~ остатки от деления $x^{18}/g(x)$ и $x^{16}/g(x)$

1) 0011 0011 011

2) 0 1100110110

3) пр умнож. сдвиг синдрома влево сдвигаем если слева "0", иначе до сдвиг влево и прибав "0" + g(x)

```
  11111101010          111111010100
+ 00110011011        + 01100110110
------------         -------------
  11001110001          100110111100
```

4) Синдром на шаге (2).

```
+ 1 | 1 1 1 1 1 0 1 0 1 0 0
  1 | 0 1 0 1 1 1 0 0 0 1 1
-----------------------------
    1 0 1 0 0 1 1 0 1 1 1
+ 1 0 0 1 0 1 0 1 1 0 0
-----------------------------
    0 0 1 1 0 0 1 1 0 1 1
```

5) Синдром на шаге (3).

```
+ 1 | 0 1 0 0 1 1 0 1 1 1 0
  1 | 0 1 0 1 1 1 0 0 0 1 1
-----------------------------
    | 0 0 0 1 0 0 0 1 1 0 1
```

```
+ 0 0 0 1 0 0 0 1 1 0 1          + 0 0 0 1 0 0 0 1 1 0 1
  0 0 1 1 0 0 1 1 0 1 1            0 1 1 0 0 1 1 0 1 1 0
-----------------------          -----------------------
  0 0 1 0 0 0 1 0 1 1 0            0 1 1 1 0 1 1 1 0 1 1
```

6)
```
+ 0 0 1 0 0 0 1 1 0 1 0
  0 0 1 1 0 0 1 1 0 1 1
-----------------------
  0 0 0 1 0 0 0 0 0 0 1
```

7) Полученный синдром s^0.

9.

Граница (продолжение)

5) Граница Варшамова - Гилберта

Пусть заданы $[n, k, d]_q$ код и число w, такое, что. $1 \le w \le n$

w имеет смысл веса. Для кода выполняется следующее соотношение:

$$n - k \ge \log_q \binom{n}{w} + w \log_q (q-1) - \log_q d + \log_q A,$$

где $A = d - 2w + \frac{q w^2}{(q-1)n} > 0.$

Граница Варшамова.

Найдем код с заданными n и d, для которого k - максимально. Обозначим объем кода:

$$A(n,d) = q^k.$$

В арсенале n-ко $F(q^n)$ введем n-ое Q и определим его мощность $|Q|$.

Обозначим $A_Q(n,d)$ максимальное кол-во слов (векторов), расст. между которыми не менее d. Тогда очевидно, что выполнено следующее неравенство

$$\frac{A(n,d)}{q^k} \le \frac{A_Q(n,d)}{|Q|}$$

2-я граница Варшамова.

Пусть рассм. код является строгим, т.е. все слова имеют один и тот же вес w.

$A(n,d,w)$ - максимальное кол-во векторов веса w, расст между которыми не менее d.

Тогда учитывая предыдущ. шаги и то, что вес объем кода является в точности объемом шара записать

$$\frac{A(n,d,w)}{|\bar{w}|(q-1)^w} \ge \frac{A(n,d)}{q^k}$$

3-я теорема Варшамова.

$$A(n,d,w) \le \left\lfloor \frac{q^n}{\sum_{i=0}^{d-2w+\frac{2w^2}{(q-1)n}} C_n^i (q-1)^i} \right\rfloor$$

Используя это выражение и подставляя его в предыдущее получим исходную границу.

6) Граница линейного программирования.

Данная граница использует обозначение спектров данного и двойного кодов. Тут стоит, сказать, что связь между отдельными компонентами $A_i' = q^{-k} \sum_{j=1}^{n} A_j P_i(j)$ и то, что каждая компонента больше нуля, получим:

$$\sum_{i=1}^{n} A_j P_i(j) \ge 0.$$

В данной границе оценивается наименьший вес кода. Из вида спектра можно определить, что:

$$q^k = 1 + \sum_{i=d}^{n} A_i$$

Пусть $q^k \to \max$, тогда:

$$\left(1 + \sum_{i=d}^{n} A_i\right) \to \max$$

Сформируем задачу линейного программирования и из нее получим выводы по границе Максимизируем величину $(1 + \sum_{i=d}^{n} x_i, x_i \ge 0)$ при условии:

$$\binom{n}{j}(q-1)^j + \sum_{i=0}^{n} P_j(i) x_i \ge 0, \quad j = 1, \dots, n$$

Решение её называется сделать следующий вывод, если A_i - набор ненулевых весов и для всех $j = 1, n$.

и $1 + \sum_{i=1}^{n} a_i P_i(j) \geq 0$, тогда:

$$q^k \geq 1 + \sum_{i=1}^{n} a_i \binom{n}{i} (q-1)^i .$$

7) Граница Варшамова - Гилберта

Данная граница определяет возможность построения кода.

Если выполняется соотношение:

$q^{n-k} \geq \sum_{i=1}^{d-2} \binom{n-1}{i} (q-1)^i$, то всегда можно построить код с параметрами $[n, k, d]$.

Т.к. q^{n-k} - объем дуального кода, то данную теорему для дуального кода.

Рассм. проверочную матрицу H (порожд. матрицу дуального кода). Выражение в правой части определяет некую сумму векторов в дуальном пр-ве. Проверочная матрица H можно составить последовательно. Первый вектор можно взять произвольно. Последующие векторы выбираются таким образом, чтобы $(d-1)$ столбец H были линейно независимыми

Первый столбец состоит. Вектору b пр-ва дуального кода, чтобы исправить вектор не был линейно зависим с первым, необходимо, чтобы удалить все вектора, лежащие на одной прямой с первым.

Выбираем второй вектор, независимый от первого.

Третий вектор нужно выбрать так, чтобы он был линейно независим 3-х векторов на данный момент. Для этого нужно удалить из пространства все вектора, лежащие в n-ти, образованных двумя первыми векторами

раз наоборот. подействовать тем-то остальных
и данными векторов.
Если до конца данного обмена удается построить матрицу H, т.е. m-то векторов,
из которых каждый $(d-1)$ линейно независим,
то алгоритм код
Если таких векторов недостаточно, то код
перестраивается

В зависимости правил такого отбора есть m-то
деталей, необходимых для построения матрицы,
которая удаляется из условия линейной
независимости векторов.

Преобразования в теории кодирования.

Наиболее широко в теории кодирования
используются Фурье - подобные преобразования:
- преобразование Адамара - Уолша;
- преобразование Фурье - Мэттсона - Соломона (РМС).

В основе всей теории преобразования лежит
теоретико-групповой принцип.
Рассм. некое множество, состоящ. из конечного
числа n-тов. Пусть они образуют циклич.
группу. Отобразим эту группу в некоторое
поле. Рассм. один из таких случаев однозначного
отображения.
Пусть a - образующий элемент исходной группы; α - однозначный образ a. Тогда запишем, что
$$\Gamma(a) = \alpha.$$
Возьмем элемент a^2, тогда $\Gamma(a^2) = \Gamma(a)\Gamma(a) = \alpha^2$.
Аналогично $\Gamma(a^3) = \alpha^3$.
Пусть порядок цикл. группы n. Тогда:

$$\Gamma(a^n) = \Gamma(e) = \alpha^n = 1.$$

Тогда $\alpha = \sqrt[n]{1}$

Возьмем эл-т a^2. Его тоже также можно построить степенью элемента a:

$$\Gamma(a^2) = \alpha^2$$
$$\Gamma(a^4) = \alpha^4 \quad \text{и т.д.}$$

В первом случае для каждого a все степенные (степени α) образуют строку $1, a, a^2, a^3$, для эл-та a^2: $1, a^2, a^4, a^6$ и т.д. для всех эл-тов a^i можно построить строки.

Рассмотрим поле $GF(2^3)$. В кач-ве первообразного корня из 1 удобно взять эл-т α:

$$\sqrt[7]{1} = \alpha$$

От одной строки к другой можно перейти, возводя образующий элемент поля в степень. Поэтому нам. нам каждую строку с "1", кто соотв. нулевому столбцу. Можно составить таблицу всех неприводимых при отображении нулей в заданное поле. Элементы этой таблицы - характеры.

Тогда любой эл-т таблицы можно представить в виде α^{ik}, где

i - номер строки,

k - номер столбца.

Каждая новая строка начинается с $k=0$, потому первый столбец единичный.

Кол-во строк в таблице равно кол-ву эл-тов в группе.

Пример $GF(2^3)$.

$\alpha = 2$:

1	1	1	1	1	1	1
1	2	3	4	5	6	7
1	3	5	7	2	4	6
1	4	7	3	6	2	5
1	5	2	6	3	7	4
1	6	4	2	7	5	3
1	7	6	5	4	3	2

$\alpha = 0, k = 0, 1, \ldots, 6$

$\alpha = 1, k = 0, 1, \ldots, 6$

$\alpha = \alpha, k = 0, 1, \ldots, 6$

- таб. 1 (лист 7)

- это и есть матрица преобразования ФНС в поле α^3. Она находит смещ. векторов данных в

Преобразование Холла

Элементы исходной группы можно расп. по другому, сам порядок эл-тов в группе тот же a^{α}. Каждый элемент в группе характеризуется, в подходящем случае порядком базы порядков $1, 2, \dots, g$. В данном случае можно сделать другую нумерацию g эл. порядок группы a^{γ}, то номер каждого эл-та можно записать в виде строки, содержащей "0" или "1", которая называется п-ка. В этом случае говорят, что группа является прямой суммой (произведением) групп H_2. $H = H_2 + H_2 + \dots + H_2$

Реализуем изоморфизм эл-тов некой группы в некоторое поле. В теории преобразований обычно расм. исходную группу - аддитивной, а отвечающую в поле - мультипликативной.
Каждый эл-т исходной группы можно разложить в сумму п-ок, каждый из которых содержит только одну единицу.
Поэтому изоморфизм от суммы п-ок рассматривается как пр-ие гомоморфизмов от каждой п-ки с одной единицей.

Тогда элементы таблицы будут иметь вид:

$$\varepsilon^{d_1 k_1} \varepsilon^{d_2 k_2} \cdot \varepsilon^{d_e k_e} \rightarrow$$

ε - образующий элемент подгруппы Галуа поля.

Если группы, на которые разложена исходная все одинаковы, то соот-ие будут одинаковы и ε_i.
Тогда каждый эл-т может быть представлен в виде:

$$\varepsilon^{\sum_i d_i k_i}$$

Данное св-во широко используется при разложении исходной функции f в прямую сумму (пр-ий) функ f_2.

В этом случае введем вектор α и вектор k, состоящие соот-но из компонент α_i и k_i.

Ещ-но, в показателе - скалярное пр-ие векторов;

$$e^{\langle \alpha, k \rangle}$$

В двоич-ных Галуа $\mathcal{E} = -1$. Поэтому, обозначая α как преобразуемый вектор X, а k - как спектральная переменная, сводя дел. двоичных векторов пр-во V_n, получим первое преобразование Уолша-Адамара

1-ое преобразование Уолша-Адамара:

$$\overline{W_f(u)} = \sum_{x \in V_n} f(x) (-1)^{\langle x, u \rangle}$$

Введем двоичную экспоненту $\exp f(x) = (-1)^{f(x)}$, тогда получаем преобразование Адамара-Уолша 2-го рода:

$$W_f(u) = \sum_{x \in V_n} \exp f(x) (-1)^{\langle x, u \rangle} = \sum_{x \in V_n} (-1)^{f(x) + \langle x, u \rangle}.$$

Свойства матрицы ФМС.

Анализируя структуру матрицы можно обнаружить внимание на её симметрию. Это дало, чтобы охарактеризовать вытекающие отсюда св-ва ряды. каждую строку матрицы в начинающуюся отображением.

Семинар.

Сократительные к-ки циклического кода 3^5.

Найдем код, двойственный коду $[11,6,5]_3$.

Для нахождения образующего порождающего полинома для двойственного кода найдем полином $h(x)$ для этого необх. разделить (x^n-1) на $g(x)$ - порождающий полином исходного кода.

Используем реальное разложение:

$$x^{11}-1 = (x-1)(x^5+x^4+x^3+x^2-1)(x^5-x^3+x^2-x-1)$$

$g_1(x)$ $g_2(x)$, найдем $h(x)$, умножив $g(x)$ на $(x-1)$.

$$h_1(x) = (x-1)(x^5-x^3+x^2-x-1) = x^6-x^4+x^3-x^2-x-x^5+x^3-x^2+x+1 =$$
$$= x^6-x^5-x^4-x^3+x^2+1$$

$$h_2(x) = (x-1)(x^5+x^4+x^3+x^2-1) = x^6+x^5+x^4+x^3-x-x^5-x^4+x^3-x^2+1 =$$
$$= x^6 \text{ сократились } +x^4-x^3-x^2-x+1$$

$$g_1(x) = x^6 h\left(\frac{1}{x}\right) = x^6\left(\frac{1}{x^6}+\frac{1}{x^4}-\frac{1}{x^3}-\frac{1}{x^2}-\frac{1}{x}+1\right) = x^6+x^5-x^4+1$$

$$x^6\left(\frac{1}{x^6}+\frac{1}{x^4}-\frac{1}{x^3}-\frac{1}{x^2}-\frac{1}{x}+1\right) = x^6-x^5-x^4-x^3+x^2+1$$

Кодирование можно двояко:

1) умножая полином $g_1(x)$ на информ. блок, длиной 5 символов.

2) построив матрицу.

В итоге

Получим код $[11, 5, d_1]$.

Построим матрицу:

$g_1(x) = x^6-x^5-x^4-x^3+x^2+1 \rightarrow [1\ 2\ 2\ 2\ 1\ 0\ 1]$

$$\begin{pmatrix} 1 & 2 & 2 & 2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 2 & 2 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 & 1 \end{pmatrix}$$

Расчет веса кодового кода:

1 слов - 0
136 слов - 6
110 слов - 9
} вес

Найдем вектор исходного кода с наименьшим весом

Первый вектор - базисный

Второй вектор - базисный

$$W_{c_1}(x;y) = 3^{-k} W_c[x+(3-1)y : x-y]$$

$3 = 3$, $k=5$ порядок

$$W_{c_2}(x;y) = 3^{-5} W_c[x+2y : x-y] = \frac{1}{243} W_c[x+2y : x-y]$$

$$W_c(x;y) = 1 \cdot x^2 y^0 +$$

Свойства строк матрицы ФИС.

Пусть a - некоторый элемент поля. Разделим (X^n+1) на $(X+a)$, рассматривая каждый i-ый шаг.

$i=1$, $X^n + 1 \mid X + a$

$\underline{X^n + aX^{n-1}}$ $\quad X^{n-1} + aX^{n-2} + a^2 X^{n-3} + \dots + a^{k} X^{n-k} + \dots + a^{n-1}$

$i=2$ $\quad aX^{n-1} + 1$

$\underline{+\ aX^{n-1} + a^2 X^{n-2}}$

$i=3$ $\quad a^2 X^{n-2} + 1$

$\underline{a^2 X^{n-2} + a^3 X^{n-3}}$

$i=k$ $\quad a^{k-1} X^{n-k+1} + 1$

$\underline{a^{k-1} X^{n-k+1} + a^k X^{n-k}}$

$i=n$ $\quad +\ a^{n-1} X + 1$

$\underline{a^{n-1} X + a^n}$

0, т.к. $a^n = 1$.

При делении полинома (X^n+1) на линейный множитель получается полином, строка коэффициентов которого имеет вид: $1 \quad a \quad a^2 \quad a^3 \dots a^{n-1}$.

Выразим a как α^l: $a = \alpha^l$, где

α - образующий элемент поля

$l = 0, 1, \dots, 14$ в $GF(14)$

Т.о. от выбора a будет получаться разная линейка коэффициентов.

Пусть $a = \alpha$, тогда получаем первую ненулевую строку в матрице ФИС: Вторая строка ФИС матрицы получается как коэффициенты полинома $(X^n+1)/(X+2)$.

Если $a = \alpha^2 = 3$, то получаем n-ый, со сдвигом 3-ей строки матрицы.

Обозначим получившийся полином как $A(G, x)$.

Построим полином, инвертировав функцию:

$\overleftarrow{A(b,x)} = a^{n-1}x^{n-1} + a^{n-2}x^{n-2} + \dots + a^2x^2 + ax + 1.$

$a^{n-1} = a^{-1} = b$, тогда

учитывая, что $a^{n-2} = a^{n-1}a^{-1} = b \cdot b = b^2$

$a^{n-3} = a^{n-1}a^{-2} = b^3$ ..., запишем новый

полином в виде.

$\overleftarrow{A(b,x)} = b[x^{n-1} + bx^{n-2} + b^2x^{n-3} + \dots + b^{n-3}x^2 + b^{n-2}x + b^{n-1}]$.

Учитывая предыдущее деление, можно полином b квадратных скобках записать соотношением $n-1$ полиномов:

$\overleftarrow{A(b,x)} = b\frac{x^n+1}{x+b}$.

Полином, построенный на любой строке ФНС матрицы, у которой последний ненулевой элемент строки - k-й, или начиная с нулевой степени полинома, может быть представлен как отношение двух полиномов $(x+b)$ зависит только от номера строки.

Коды Рида - Соломона.

Коды можно определить исходя из свойств полиномов в конечных полях.

Рассмотрим поле F_q и находящуюся в нем систему n точек. Канд. Боккиери называет такую систему n точек, в которой m - число q - тов идентичных нулю точек

Ранг множества полиномов степень которых не превышает a. Они образуют n-во $L(a)$ размерностью $(a+1)$.

Ранг отображения $\mathcal{A}$ полиномов, называемый также тот, которым пользуются вычисления значения полинома в каждой n-ке.

Пусть все n-ки поля естественно упорядочены. Возьмем некоторый полином $f(x)$ из всего n-ва. Составим слово вида $\{f(P_1), f(P_2), \dots, f(P_n)\}$, где

$P_1, P_2, \dots, P_n$ - точки поля

Получившееся слово является кодом, получ. с помощью полинома $f(x)$

Элементы информационного блока - это веса k-ых членов $f(x)$. Здесь $k = a+1$.

Очевидно, что $n > a$. След-но, полином отлич. от нуля в $(n-a)$ точках.

Учитывая мощность кода и об-ва мин. кодового расстояния можем записать параметры кода $[n, a+1, n-a]_q$.

Проверим для кода условие Синглтона, т.е соотношение между $(n-k+1)$ и d.

$$n-k+1 = n-(a+1)+1 = n-a$$

$$d = n-a.$$

Т. е. код Рида - Соломона достигает границы Синглтона. Это MDR (максимально достижимое кодовое расстояние) - код.

Рассмотрим процедуру кодирования, напр. в $GF(2^3)$.

Пусть имеется полином $f(x)$, который обладает $m(a+1)$ членов. Возьмем свободный член полинома. Подставляем поочер-но точки. Значение данного члена подставляем и равно значению свободного члена

Возьмем член с множителем x. Подставим поочер-но в него все точки. Очевидно, что получается первый (неединичный) столбец МС напр., относящийся к к-ту при x.

Возьмем член с множителем x^2. Получим следующую строку напр., относящуюся к к-ту при x^2.

$$ФИС = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 \\ 1 & 4 & 7 & 3 & 6 & 2 & 5 \\ 1 & 5 & 2 & 6 & 3 & 7 & 4 \\ 1 & 6 & 4 & 2 & 7 & 5 & 3 \\ 1 & 7 & 6 & 5 & 4 & 3 & 2 \end{pmatrix}$$

Если элемент равнялся a, то подобное расположение затрагивает (a+1) строку ФИС матрицы.

След-но, можно кодировать не с помощью полинома, а с помощью усеченной ФИС матрицы.

Умножим каждую её строку на соотв. к-т из полинома. Сложим эти строки. Получим кодовое слово.

(строка к-тов полиномов) · (усеч. ФИС матрица) = (строка код слова)

Если использовать данный вид матрицы, то 6 строка к-тов им. вид слева

Используя св-во строк ФИС матрицы. Построим в соот-е каждой строке полином $(A(C, X))$. Построим код, как сумму полиномов соотв (a+1) строке → получим кодовое слово-полином.

Далее. строим матрицу полученного полинома.

Для этого разложим каждую строку матрицы в виде полинома. Учитывая, что (X^n+1) – это произведение всех неприводимых многочленов, то каждая строка – это произведение всех неприводимых многочленов без одного:

$$\frac{X^n+1}{X+1} \leftrightarrow 1 \quad * (X+2)(X+3)(X+4)(X+5)(X+6)(X+8)$$

$$\frac{X^n+1}{X+2} \cdot 2 \quad (X+1)(X+2)(X+3)(X+4)(X+5)(X+6) *$$

$\frac{x^n+1}{x+6}$ 6	$(x+1)(x+2)(x+3)(x+4)(x+5)*(x+7)$
$\frac{x^n+1}{x+5}$ 5	$(x+1)(x+2)(x+3)(x+4) * (x+6)(x+7)$
$\frac{x^n+1}{x+4}$ 4	$(x+1)(x+2)(x+3) * (x+5)(x+6)(x+7)$
$\frac{x^n+1}{x+3}$ 3	$(x+1)(x+2) * (x+4)(x+5)(x+6)(x+7)$
$\frac{x^n+1}{x+2}$ 2	$(x+1) * (x+3)(x+4)(x+5)(x+6)(x+7)$

Общее при кодировании сдвиговый младший разряд информационного слова умножается на полином, соотв. первой строке следующий разряд - на полином, соотв. 2-й строке и т.д. для всех $(a+1)$ строк

Получившиеся полиномы можно упростить

Сложив $(a+1)$ взвешенных полиномов, соотв. строкам матрицы, увидим, что во всех полиномах можно вынести за скобки некий общий множитель. След-но, любое кодовое слово будет делиться без остатка на получившийся общий множитель. След-но код Рида-Соломона - циклический.

Основным методом анализа кодов РС является рассмотрение порождающего и дуального кода. Расс. дуальный код для данного примера.

Формально у кода РС как циклического имеется пули кода, поэтому для $a=2$ пули это $2, 3, 4, 5$. След-но, нулями дуального будут $\alpha^{-1}, \alpha^{-2}, \alpha^{-3}, \alpha^{-4}, \alpha^{-5}$.
$\alpha^{7}, \alpha^{6}, \alpha^{5}, \alpha^{4}$.

Тогда нулями являются $1, 2, 3$.

Дуальный код также можно получить как объединение строк с общей четностью, один которого объединяем.

Для данного типа кодирования с помощью матрицы проверки кода + вектора + первая строка ФМС матрицы.

В основном алгоритм тот, поэтому нужно смотреть, что дуальный код этого кода РС.

Коды РС - циклические коды, чтобы процесс кодирования - декодирования можно было как с помощью ФМС матрицы, так и с помощью порождающего полинома.

Укороченные коды Рида - Соломона.

В укороченных кодах берется кол-во точек меньше, чем порядок мультипликативной группы.

Кодирование может осуществляться с помощью полинома или "вектора" из ФМС матрицы.

Коды с циклическими идеалами.

Анализ полиномов, соотв. их строкам ФМС матрицы показывает, что каждый получен. таким полиномом имеет максимально возможную степень или заданную ($X^n + I$).

След-но данные полиномы являются порождающими полиномами левых циклических идеалов кольца. Проверка показывает, что они не являются идемпотентными.

След-но, при сложении строк, что производится при кодировании, реализовывается операция сложения циклических идеалов.

Получившееся кодовое слово также должно принадлежать новому идеалу, которое также будет являться

по ранее сформулир. утверждению у любого идеала порожд. полином отлич. как наиб. больший делитель всех исходных полиномов. Порожд. идеальный будет равен одному полиному миним. идеалов.

Укороченные коды РС (продолжение).

Построим для укороченного кода дуальный код аналогично. то - бо $\mathcal{R}(a)$ следующим образом.

Введем ф-цию $g_0(x) = \prod_{P_i} \frac{l}{(x+P_i)}$

Расм. параметры дуального кода.

Из предыдущего расм. имеем, что:

$$K_1 = n - K = n - a - 1$$

След-но, полином, задающий дуальному коду имеет $d_1 = n - a - 2$.

Можно расм. минимальное кодовое расст.

$$d_1 = n - a_1$$

К g_0 добавим полиномы вида $g_c(x) = x^l g_0(x)$

$$1 \le l \le n - a - 2.$$

Расм. ф-ции $g_0(x)$ и $g_c(x)$ как базисные ф-ции в тр-ве $\mathcal{R}(a)$.

Возьмем $g \in \mathcal{R}(a)$, тогда кодовое слово дуального кода образуется как $(Res_{P_1} g, Res_{P_2} g, \dots, Res_{P_n} g)$

$Res_{P_i} g$ - вычет ф-ции g в т-ке P_i.

Произвольный вектор $g \in \mathcal{R}(a)$ может быть разложен по базису и представлен в виде:

$$f(x) = f(x) g_0(x)$$

Фактор тр-ва $\mathcal{R}(a)$ - это отношение двух полиномов, причем $g_0(x)$ имеет максимальную возможную степень, а полином в числителе имеет меньшую степень

Семинар.

Нахождение отдельных спектральных компонент
- производится с помощью полиномов Кравчука.

$$A_i' = \beta^{-k} \sum_{j=0}^{n} A_j P_i(j)$$

$$P_i(x) = \sum_{j=0}^{i} (-1)^j (\beta-1)^{i-j} \binom{x}{j}\binom{n-x}{i-j}$$

Расш. код $[11,5,6]_3$ (двоичный к исходному) как основной. Применение ф-ции Мак-Вильямс к нему определит параметры основного кода, коорд. бит будут двоичными к нему.

Если известны все спектр. компоненты B', то можно получить значение любой спектральной компоненты в двоичном коде.

Известны спектр. компоненты:

	вес
$B_0 = 1$	0
$A_6 = 132$	6
$A_9 = 110$	9

Найдем 5-ю компоненту в код, двоичному данному.

$\beta = 3$
$k = 5$
$n = 11$

$$A_5' = \frac{1}{243}\left\{A_0 P_5(0) + A_6 P_5(6) + A_9 P_5(9)\right\}$$

$$P_5(0) = \sum_{j=0}^{5} (-1)^j 2^{5-j} \binom{0}{j}\binom{11}{5-j}$$

Ф-ла предлагает значение j, только как $j=0$

$$P_5(0) = 1 \cdot 2^5 \cdot 1 \cdot \frac{11!}{5!6!} = 2^5 \cdot \frac{11\cdot 10^2\ 9^3 \cdot 8 \cdot 7}{5\cdot 4\cdot 3\ 2} = 2^5 \cdot 11\cdot 42 =$$

$$= 32 \cdot 11 \cdot 42 = 14784$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

$$P_5(6) = \sum_{j=0}^{5} (-1)^j 2^{5-j} \binom{6}{j}\binom{5}{5-j} = 2^{32} - 2^4 \cdot 6 \cdot 5 + 2^3 \frac{6!}{2!4!} \cdot \frac{5!}{3!2!} -$$

$$- 2^2 \frac{6!}{3!3!} \cdot \frac{5!}{2!3!} + 2 \frac{6!}{4!2!} \cdot \frac{5!}{1!4!} - 2^0 \frac{6!}{5!1!} \cdot \frac{5!}{0!5!} =$$

$j=0 \quad \frac{6!}{0!6!} = 1 \quad \frac{5!}{0!5!} = 1$

$$= 2^5 - 2^4 \cdot 30 + 2^3 \cdot 150 - 2^2 \cdot 200 + 2 \cdot 75 - 6 =$$

$j=1 \quad \frac{6!}{1!5!} = 6 \quad \frac{5!}{4!1!} = 5$

$$= 32 - 480 + 1200 - 800 + 150 - 6 =$$

$$= 96$$

$$P_5(9) = \sum_{\substack{j=0 \\ 3 \le j \le 5}}^{5} (-1)^j 2^{5-j} \binom{9}{j}\binom{2}{5-j} = -2^{32} \frac{9!}{3!6!} \cdot \frac{2!}{2!0!} + 2 \frac{9!}{4!5!} \cdot \frac{2!}{1!1!} -$$

$$- 2^0 \cdot \frac{9!}{5!4!} \frac{2!}{0!2!} =$$

$$= -2^2 \cdot 3 \cdot 84 + 2 \cdot 9 \cdot 2 \cdot 7 \cdot 6^2 - 9 \cdot 7 \cdot 7 \cdot 6 = -336 + 504 - 126 = 42.$$

$$A_5' = \frac{1}{243} \left\{ 1 \cdot 14784 + 132 \cdot 96 + 110 \cdot 42 \right\} = \frac{32076}{243} = 132$$

Доказано ранее утверждение коды РС (определенные ранее было показано, что любой вектор ф-ции могут быть представлены в виде ф-ции).

$F(x) = f(x) g_0(x)$, где

$f(x)$ - записан в числителе.

Для данного п-ва существует св-во, связанное с построением данного кода. Рассм. комплексное п-во:

Окаймим все полюсы ф-ции $F(x)$ окр-ю, радиуса R из начала координат. Проинтегрируем ф-ю $F(x)$ по кругу, устремив $R \to \infty$.

Тогда интегралы будут равны:

$$\int_C f(x)\,dx = \sum_{p_i \in P} \operatorname{Res}_{p_i} F(x)$$

Пусть ф-ция $F(x)$ как отношение 2-х полиномов имеет степень числителя m, знаменателя - n.

Пусть $m \le n-2$.

Оценим ф-цию $F(x)$:

$$|F(x)| = \left|\frac{a^m x^m + a^{m-1} x^{m-1} + \dots + a_0}{b^n x^n + b^{n-1} x^{n-1} + \dots + b_0}\right| = \left|\frac{a^m}{b^n} \frac{1}{x^{n-m}}\right| \left|\frac{1 + \dots + \frac{a_0}{a_m x^m}}{1 + \dots + \frac{b_0}{b_n x^n}}\right|$$

Считаем x комплексной переменной. Заменим x^{n-m} на модуль этого выражения. Пусть этот обозначен x как R.

Устремим R к бесконечности, тогда второй модуль не превысит 2, следовательно:

$$|F(x)| \le \left|\frac{a^m \cdot 2}{b^n R^2}\right|$$

Если взять $F(x)$ максимальной в интервале и взять за этот интервал, то значение интеграла будет равно $\pi \cdot R$.

Тогда:

$$\int |F(x)|\,dx \le \left|\frac{2a^m}{b^n}\right| \frac{1}{R^2} \cdot \pi R$$

Устремим $k \to \infty$, тогда кратность в числе нулей нуль.

След-но, сумма кратностей ф-ции $F(x)$ будет равна нулю. Данное утверждение равно-сильно и по сути конечных полей.
Укороченные коды циклическими не являются

Определение циклического РС кода.

Ранее обнаружено, что коды РС - циклические и могут быть построены путем разложения бинома многочленов. Но на практике определение кода РС было дано другому классу кодов, которые и были изначально исследованы.
Определим циклический код РС с помощью вида его порождающего полинома.

$$g(z) = \prod_{i=\nu}^{\nu+m-1} (z - \alpha^i)$$

$m = n - k$ - длина слова
$n = q - 1$
$\nu = 0, 1, 2, \ldots$
α - образующий элемент мультипликативной группы
Все недвоичные коды с помощью данного вида и относят к кодам РС.

Чаще всего $\nu = 0$ или 1.

Наиболее распространенным методу декодирования РС кодов во внешней области. Где декодирование - многочленом порождающим H.

$$g(x) = g_0 + g_1 x + \ldots + g_{n-k} x^{m-1}$$

Пусть в результате действия помехи символ примет α^i, в РМС матрице возникнет ошибка, образующая этим элементом. Очевидно, что

его информационный слой, но он обладает большей помехоустойчивостью за счет избыточности. Существуют и другие коды, позволяющие исправлять ошибки, возникающие при передаче данных по каналам с шумом, например, циклические коды.

Циклические коды являются наиболее широко применяемыми. Они будут рассмотрены в последующих разделах.

Основы декодирования кодов РС.

Пусть принятое слово из канала связи имеет вид:

$$S = CH_1^T$$

H_1 - матрица из РМС матрицы.

Каждый элемент S_i - некоторая линейная комбинация e_i - ошибок. Всего v ошибок $e_1, e_2, \dots, e_v$ - числа двоичных позиций. e_i - i-ая ошибка в e_i - позиции.

Для вычисления значений ошибок надо:

$$\sum_i e_{p_i} \alpha^{e_i(j+v-1)} = S_{j+v}$$

$$\alpha^{e_i(j+v-1)} = \alpha^{e_i j} \alpha^{e_i(v-1)}$$

$Y_i = e_{p_i} \alpha^{je_i}$ - i-ая величина ошибки,

$X_i = \alpha^{e_i}$ - i-ая для определения позиции ошибки.

$$\sum_{e_i} Y_i X_i^{\nu-1} = S_\nu$$

Изменяя $\nu = 1..m$ можно получить следующую систему ур-ий:

$$\left.\begin{array}{ll}
\sum_{i=1}^{v} Y_i X_i^0 = Y_1 + Y_2 + .. + Y_v = S_1 & \nu = 1 \\
\sum_{i=1}^{v} Y_i X_i^1 = Y_1 X_1 + Y_2 X_2 + .. + Y_v X_v = S_2 & \nu = 2 \\
\cdots & \cdots \\
\sum_{i=1}^{v} Y_i X_i^{m-1} = Y_1 X_1^{m-1} + Y_2 X_2^{m-1} + .. + Y_v X_v^{m-1} = S_m & \nu = m
\end{array}\right\} \text{Исходная система}$$

Рассмотрим полином $\sigma(z)$, корнями которого являются величины, обратные локаторам ошибок:

$$\sigma(z) = (1 - zX_1)(1 - zX_2)..(1 - zX_v) = \sigma_v z^v + \sigma_{v-1} z^{v-1} + .. + \sigma_1 z + \sigma_0$$

– это полином локаторов.

Подставим $z = X_i^{-1}$ в полином $\sigma(z)$. Тогда он обратится в ноль.

Расш. Сократим полином через к-ты и после подстановки умножим лев. и пр. части на $Y_i X_i^{\nu+v-1}$.

В общем виде получим систему ур-ий, каждое из которых за скобки вынесем Y_i:

$$Y_i \left[\sigma_v X_i^{\nu-1} + \sigma_{v-1} X_i^{\nu} + .. + \sigma_1 X_i^{\nu+v-2} + X_i^{\nu+v-1} \right] = 0, \quad 1 \le i \le v.$$

Очевидно, что при фиксированном i можно каждое слагаемое умножить на Y_i и произвести по нему суммирование по всем i. Очевидно при этом не изменится:

$$\sigma_v \sum_{i=1}^{v} Y_i X_i^{\nu+1} + \sigma_{v-1} \sum_{i=1}^{v} Y_i X_i^{\nu} + .. + \sum_{i=1}^{v} Y_i X_i^{\nu+v-1} = 0.$$

Учитывая "исходную систему", заменим каждую сумму слагаемых на соответствующую. Получим систему:

$$\sigma_v s_j + \sigma_{v-1} s_{j+1} + \dots + \sigma_1 s_{j+v-1} + s_{j+v} = 0, \quad 1 \le j \le v.$$

Вернемся к исходной системе. В ней неизвестных: локаторы, величины, кол-во ошибок. Такая система неизвестна, поэтому наша решение задачи декодирования начинаем систему в исходном виде нецелесообразно. Приведем к новому виду системы, вычисления которых можно описать с помощью синдромов, которые будем представлять в виде:

$$\sigma_v S_1 + \sigma_{v-1} S_2 + \dots + \sigma_1 S_v = -S_{v+1}, \quad j = 1$$

$$\sigma_v S_2 + \sigma_{v-1} S_3 + \dots + \sigma_1 S_{v+1} = -S_{v+2}, \quad j = 2$$

$$\sigma_v S_v + \sigma_{v-1} S_{v+1} + \dots + \sigma_1 S_{2v-1} = -S_{2v}, \quad j = v, \quad v \le \frac{t}{2} m$$

Компоненты синдрома $S_1, S_2, \dots, S_{2v}$ являются, кратными к-ты полинома локаторов.

В зависимости от способа решения данной системы для нахождения к-тов σ_i, $0 \le i \le v$ получаются различные способы декодирования во временной обл-ти.

Существует традиционный способ анализа системы ур-й (Горенштейна - Цирлера)

Др. методы предполагают анализ особого вида матриц. Запишем данную левую часть системы в расширенную матрицу. Она имеет особый вид: элементы матрицы, стоящие на диагоналях, параллельных вспомогательной диагонали равны между собой. Такие матрицы называются Ганкелевыми матрицами. Если рассм. Ганкелеву матрицу, то они могут быть полностью описаны элементами, стоящими в первой строке и последнем столбце.

Расширение, продолжение ранговых матриц.

Часто вслед расширяемую матрицу, полученную на предыдущих шагах S., мы тоже заключаем "-" и дополняем до двойных полей. Тогда матрица X- со 2V параметрами.

Расш. полученную матрицу на базе 5 элементов

a_1 a_2 a_3 a_4

a_2 a_3 a_4 a_5

a_3 a_4 a_5 a_6

Расширим матрицу на один столбец вправо

Где мы получим свободный элемент a_6. Пусть матрица имеет заданный ранг. При таком расширении ранг может увеличиться или остаться прежним.

Расширение, продолжение, при которых ранг матрицы остается прежним называется особым.

Т.к. выбор a_6 произвольный, выберем его так, чтобы определитель на единицу больше разности, тем ранг, один равен нулю.

Будучи данную матрицу вниз на одну строку тогда мы новый элемент a_7, который может быть найден из усл-я чтобы определитель (1966) равнялся нулю

Матрицы можно расширять, продолжать до бесконечности каждый раз добавляя новую строку (столбец) новый элемент определяется из усл-я чтобы определитель. При этом ранг матрицы не менялся.

матрицу можно расширять расширяющую и продолжать до бесконечности с сохранением ранга.

Теорема о дробно-рациональных функциях.

Пусть a_i - i-ый Ганкелевой матрицы, на которых она построена.
При расширении последовательности новые i-ые, при добавлении бесконечной Ганкелева матрица имеет конечный ранг r тогда и только тогда, когда сумма формального ряда:

$$\sum_{i=1}^{\infty} \frac{a_i}{z} = \frac{W(z)}{B(z)} \quad \text{- дробно-рациональной ф-ии.}$$

Ранг r совпадает с числом n-ым $B(z)$ с учетом их кратности.

Бесконечный ряд

Пусть кол-во ошибок ν - максимальной равной n. Тогда Ганкелева матрица отлич $\neq 0$ на элементов

$$\frac{a_1}{z} + \frac{a_2}{z^2} + \dots + \frac{a_{2n}}{z^{2n}} + Q(z) = \frac{W(z)}{B(z)}, \text{ где}$$

$Q(z) = \frac{a_{2n+1}}{z^{2n+1}} + \frac{a_{2n+2}}{z^{2n+2}} + \dots$ - обладающая все те же, полученные расширением матрицы. Перенеся $Q(z)$ вправо и левую часть дробно-рациональной функции общему знаменателю

В числителе получится полином, который обозначим $A(z)$.

$$A(z) \cdot B(z) = z^{2n}[W(z) - Q(z) B(z)]$$

$$A(z) = a_1 z^{2n-1} + a_2 z^{2n-2} + \dots + a_{2n-1} z + a_{2n}.$$

Ключевое уравнение.

Разделим левую часть ур-я и правую часть на z^{-1}. Очевидно, степень полинома $\delta(z)$ равна n, а $W(z) - (n-1)$. Умножим левую часть на z^{2n-1}. Получим.

$$z^{2n-1} \cdot A\left(\frac{1}{z}\right) \delta\left(\frac{1}{z}\right) = \overleftarrow{A}(z)\ \overleftarrow{\delta}(z)$$

Тогда левая часть примет вид:

$$z^{2n-1}\ \frac{1}{z^{2n}}\left[W\left(\frac{1}{z}\right) - Q\left(\frac{1}{z}\right)\delta\left(\frac{1}{z}\right)\right] = z^{n-1} W\left(\frac{1}{z}\right) - z^{n-1}\delta\left(\frac{1}{z}\right)\left[q_{2n+1} z^{2n+1} + \dots\right]$$

$$= \overleftarrow{W}(z) - z^{2n}\overleftarrow{\delta}(z)\left[q_{2n+1} z + q_{2n+2} z^2 + \dots\right].$$

Возвращаемся к левой и правой части по модулю z^{2n}:

$$\overleftarrow{A}(z)\,\overleftarrow{\delta}(z) = \overleftarrow{W}(z) \mod z^{2n}.$$

Из расш. теоремы следует, что с помощью полинома $\overleftarrow{\delta}(z)$ можно построить, аналогично циклическим кодам, систему ур-я в неявном виде.

Обозначим $\overleftarrow{A}(z) = S(z) = S_1 + S_2 z + S_3 z^2 + \dots$

$$\overleftarrow{\delta}(z) = \sigma(z)$$

$\overleftarrow{W}(z) = \omega(z)$ - полином ошибок

Тогда получим ур-е, называемое ключевым ур-ем

$$\sigma(z)\, S(z) = \omega(z) \mod z^{2m}$$

Семинар.

Матрицы преобразований Фис. $2^{\alpha-k}$.

x \ u	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	1	3	5	7	9	11	13	15	2	4	6	8	10	12	14
3	1	4	7	10	13	1	4	7	10	13	1	4	7	10	13
4	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12
5	1	6	11	1	6	11	1	7	11	1	6	11	1	6	11
6	1	7	13	4	10	1	7	13	4	10	1	7	13	4	10
7	1	8	15	7	14	6	13	5	12	4	11	3	10	2	9
8	1	9	2	10	13	11	4	12	5	13	6	14	7	15	8
9	1	10	4	13	7	1	10	4	13	7	1	10	4	13	7
10	1	11	6	1	11	6	1	11	6	1	11	6	1	18	6
11	1	12	8	4	15	11	7	3	14	10	6	2	13	9	5
12	1	13	10	7	4	1	13	10	7	4	1	13	10	7	4
13	1	14	12	10	8	6	4	2	15	13	11	9	7	5	3
14	1	15	14	13	12	11	10	9	8	7	6	5	4	3	2

Построение основной матрицы Уолша.

В кач-ве умнож. рассм. сдвиг матрицы размерностью 8×8

$8 = 2^3$, поэтому разложим матрицу по базе трассы. Обычно в методе Уолша разлагают матрицу в прямую сумму Н2 матриц.

$$W_4(u) = \sum_{x \in V_n} (-1)^{\gamma(x,u)} \quad \gamma(x,u) = (-1)^{x_1 k_1} \cdot (-1)^{x_2 k_2} (-1)^{x_3 k_3}$$

Пусть рассм. умнож. Уолша реал. отображение 3-х одноразрядных чисел в поле квадратных к-ных из 1 в арифметических обозначениях $2^n - 1$ у всех чисел к-ных "-1".

x_0 \ x_1	000	001	010	011	100	101	110	111
000	1	1	1	1	1	1	1	1
001	1	-1	1	-1	1	-1	1	-1
010	1	1	-1	-1	1	1	-1	-1
011	1	-1	-1	1	1	-1	-1	1
100	1	1	1	1	-1	-1	-1	-1

101	1	-1	1	-1	-1	1	-1	1
110	1	1	-1	-1	-1	-1	1	1
111	1	-1	-1	1	-1	1	1	-1

Матрица преобразования Уолша-Адамара (Адамара)

Ключевое ф-е для нахождения максимального кол-ва ошибок.

Пусть $V < n$. В этом случае $B(z)$ имеет степень V, а $W(z)$ - $(V-1)$.

Перемножение $A(z)$ и $B(z)$ приводит к полу-ю выражению:

$$A(z)\,B(z) = z^{2m}\left[W(z) - Q(z)\,b(z)\right]$$

Поскольку максимально степень $V = n$ заменяем z на $(1/z)$.

Но делителей 1, и n часть не на z^{2n+V-1}, а на z^{2n+V-1}.

Т.о. получаем ф-е, аналогичное основному случаю и под ее замену:

$$\overleftarrow{A(z)} \Rightarrow S(z);$$
$$\overleftarrow{B(z)} \rightarrow b(z),$$
$$\overleftarrow{W(z)} \rightarrow \omega(z)$$

Приводим ф-е к ключевому ф-ю, Т.о.

Вид ключевого ф-я не зависит от кол-ва ошибок.

В ключевой ф-ии один полином неизвестен, $S(z)$, т.к. он образуется на известном векторе-синдроме.

Два члена полинома $b(z)$, $\omega(z)$.

Если $b(z)$ ранее определен, а его к-ты входят в систему ф-й с коэффициентами синдрома, то полином ошибок $\omega(z)$ также не определен.

Очевидно, что ключевое ф-е несет полную инф-цию об ошибках $b(z)$ - ошибочные позиции, $\omega(z)$ - величины ошибок

Подаешь, чтобы из них $G(z)$ и $\omega(z)$ имеют ошибочные позиции, а разработав дополнит. алгоритм и внесешь ошибок.

Существует 2 метода решения кольцевого ур-я.

Метод 8 Метод Сугиямы.

Использует св-во алгоритма Евклида до нахождения наиб общего делителя двух полиномов.

Пусть даны 2 полинома $f(z)$ и $g(z)$.
Степень $g(z)$ меньше степени $f(z)$.

Всегда можно записать, что:

$$f(z) = g(z) q_1(z) + R_1(z)$$

$R_1(z)$ - остаток от деления, его степень меньше $g(z)$.
$q_1(z)$ - неполное частное.

Далее

$g(z) = R_1(z) q_2(z) + R_2(z)$, причем степень $R_2(z)$ меньше степени $R_1(z)$.

$R_1(z) = R_2(z) q_3(z) + R_3(z)$ и т.д.
на $(k-2)$ шаге.
Если $R_{k-2}(z) = R_{k-1}(z) q_k(z) + R_k(z)$

$R_{k-1}(z) = R_k(z) q_{k+1}(z)$. * - допустим, что возникла такая ситуация, что $R_{k-1}(z)$ нацело делится $R_k(z)$.

В теории чисел существов. теорема, которая может быть перенесена и на полиномиальный случай.
Если $R_k(z)$ является наиб. общим делителем $f(z)$ и $g(z)$, то найдутся и такие ф-ции $U(z)$ и $V(z)$, что.

$$f(z) U(z) + g(z) V(z) = R_k(z)$$

$U(z)$ и $V(z)$ Следовательно рекуррентности (пошагового выполнения алгоритма Евклида) также могут вычисляться пошагово.
Т.е. на каждом шаге можно вычислять $U_i(z)$ и $V_i(z)$, причем:

$$U_i(z) = q_i(z)\, U_{i-1}(z) + U_{i-2}(z)$$

$$V_i(z) = q_i(z)\, V_{i-1}(z) + V_{i-2}(z)$$

Используется следующ. нач. условия:

$U_{-1} = 0 \qquad V_{-1} = 1$

$U_0 = 1 \qquad V_0 = 0$.

Рассм. цепно-дробную дробь:

$$h(z) = \frac{f(z)}{g(z)}$$

Тогда:

$h(z)$ можно представить в виде цепной дроби:

$$h(z) = g_1(z) + \cfrac{1}{g_2(z) + \cfrac{1}{g_3(z) + \cfrac{1}{g_4(z) + \ldots + \cfrac{1}{g_k + \cfrac{1}{g_{k+1}}}}}}$$

или:

$$h(z) = g_1(z) + \left(g_2(z) + \left(g_3(z) + \ldots + \left(g_k + g_{k+1}^{-1}\right)^{-1} \ldots\right)^{-1}\right)^{-1}$$

Обычно цепную дробь усекают и рассм. частичные суммы.

1) Усекаем до $x-z_0$ члена, тогда: $h_1(z) = g_1(z)$.

2) до $2-z_0$, тогда: $h_2(z) = g_1(z) + \cfrac{1}{g_2(z)}$

3) до $3-z_0$, тогда: $h_3(z) = g_1(z) + \cfrac{1}{g_2(z) + \cfrac{1}{g_3(z)}}$

4) $h_4 = g_1 + \left[g_2 + (g_3 + g_4^{-1})^{-1} \right]^{-1}$

Анализ данных подходящих сумм показывает, что

$h_1 = \frac{g_1}{1} = \frac{u_1}{v_1}$,

$h_2 = g_1 + \frac{1}{g_2} = \frac{g_2 g_1 + 1}{g_2} = \frac{u_2}{v_2}$,

$h_3 = g_1 + \frac{1}{g_2 + \frac{1}{g_3}} = \frac{u_3}{v_3}$

$h_4 = \frac{u_4}{v_4}$.

Данное св-во удовлетворяется по индукции.

Эйлер изучал подходящие суммы рассмотрел общее выражение вида: $(h_i - h_{i-1})$ и получил:

$h_i - h_{i-1} = \frac{u_i v_i - u_{i-1} v_{i-1}}{v_i v_{i-1}} = \frac{(-1)^i}{v_i v_{i-1}}$ — соотношение Эйлера.

Предоставим полученное значение u_i, v_i в векторном виде. Тогда

$$\begin{pmatrix} u_i(z) \\ v_i(z) \end{pmatrix} = \begin{pmatrix} u_{i-1}(z) & u_{i-2}(z) \\ v_{i-1}(z) & v_{i-2}(z) \end{pmatrix} \begin{pmatrix} g_i(z) \\ 1 \end{pmatrix}$$

Расширим левую и правую матрицы:

$$\begin{pmatrix} u_i(z) & u_{i-1}(z) \\ v_i(z) & v_{i-1}(z) \end{pmatrix} = \begin{pmatrix} u_{i-1}(z) & u_{i-2}(z) \\ v_{i-1}(z) & v_{i-2}(z) \end{pmatrix} \begin{pmatrix} g_i(z) & 1 \\ 1 & 0 \end{pmatrix}$$

Используя правую часть выражения получаем его подобное с индексами.

Очевидно, что:

$$\begin{pmatrix} u_{i-1}(z) & u_{i-2}(z) \\ v_{i-1}(z) & v_{i-2}(z) \end{pmatrix} = \begin{pmatrix} u_{i-2}(z) & u_{i-3}(z) \\ v_{i-2}(z) & v_{i-3}(z) \end{pmatrix} \begin{pmatrix} g_{i-1}(z) & 1 \\ 1 & 0 \end{pmatrix}$$

Любое ф-ции Ui D на i-ом шаге можно записать через набор Qi двигаясь от i = 1 до конкретного значения i

Т.е.:

$$\begin{pmatrix} U_i(z) & U_{i-1}(z) \\ D_i(z) & D_{i-1}(z) \end{pmatrix} = \prod_{i=1}^{i} \begin{pmatrix} q_i(z) & 1 \\ 1 & 0 \end{pmatrix}$$

Обозначим левую матрицу, как Qi найти ее определитель: $|Q| = (-1)^i$ - из соотношения Эйлера.

След-но, обратная матрица опр-ся как:

$$Q^{-1}_i = (-1)^i \begin{pmatrix} D_{i-1}(z) & -U_{i-1}(z) \\ -D_i(z) & U_i(z) \end{pmatrix}$$

Из алгоритма Евклида для двух последних строк можно записать:

$$\begin{pmatrix} R_{k-2}(z) \\ R_{k-1}(z) \end{pmatrix} = \begin{pmatrix} q_k(z) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_{k-1}(z) \\ R_k(z) \end{pmatrix}$$

Аналогично, двигаясь "вверх" можно получить:

$$\begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q \\ R_1 \end{pmatrix}; \begin{pmatrix} q \\ R_1 \end{pmatrix} = \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

Следовательно:

$$\begin{pmatrix} f \\ g \end{pmatrix} = \prod_{i=1}^{i} \begin{pmatrix} q_i(z) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_{i-1}(z) \\ R_i(z) \end{pmatrix}$$, i - текущий шаг.

Всегда f и g можно определить зная совокупность строк в алгоритме Евклида.

~~Непрерывной дробью~~

Пр-ние и есть матрица Qi

Но нужность матрица, обратная ей. Возьмем две левых остатка R_{k-1}, R_k. Используя обратную матрицу можно записать:

$$\begin{pmatrix} R_{k-1} \\ R_k \end{pmatrix} = Q_k^{-1} \begin{pmatrix} f(z) \\ g(z) \end{pmatrix}$$

Последнее выражение позволяет, формируя матрицы Q_k^{-1} и зная f и g, определять остатки на любом шаге

Запишем выражение для остатка $R_k(z)$:

$$\begin{pmatrix} R_{k-1}(z) \\ R_k(z) \end{pmatrix} = (-1)^k \begin{pmatrix} V_{k-1}(z) & -U_{k-1}(z) \\ -V_k(z) & U_k(z) \end{pmatrix} \begin{pmatrix} f(z) \\ g(z) \end{pmatrix}$$

$$R_k(z) = (-1)^k [-V_k(z) f(z) + U_k(z) g(z)]$$

Выберем остаток $R_k(z)$ так, чтобы его степень была меньше n, а степень предыдущего остатка больше или равна

Выберем в кач-ве g-ции $f(z) = z^{2n}$, $g(z) = S(z)$

Далее идем с основанием д. Горо "-" обеспечивают знакопеременность:

$$R_k = z^{2n} V_k(z) + U_k(z) S(z).$$

Возьмем выражение по $\mod z^{2n}$; тогда,

$$R_k = U_k(z) S(z) \mod z^{2n}.$$

Сравним данное выражение с ключевым ур-ем:

$$\omega(z) = \sigma(z) S(z) \mod z^{2n}.$$

Т.к. левые части совпадают, то должны совпадать и правые части:

$\sigma(z) = \xi U_k(z)$, ξ - постоянный множитель.

Аналогично,

$$\omega(z) = \xi R_k(z)$$

След-но, $\omega_0(z)$ можно получить из алгоритма Евклида, получив остаток $R_k(z)$.

Определяют из полинома $\sigma(z)$ и $\omega(z)$.

Особенности применения метода рекуррентных продолжений.

Ранее была получена система ур-й для компонент синдромов с к-ыми из полинома $\sigma(z)$.

Анализ бесконечных особых продолжений Ганкелевой матрицы показывает, что можно сформулировать следующие условия:

1) Бесконечная Ганкелевая матрица имеет конечный ранг r тогда и только тогда, когда существуют r чисел $\sigma_1, \sigma_2, \ldots, \sigma_r$ таких, что:

$$-a_{u+1} = \sigma_1 a_u + \sigma_2 a_{u+1} + \ldots + \sigma_r a_{u-r+1} = \sum_{i=1}^{r} \sigma_i a_{u-i+1} \quad (*)$$

При этом определитель матрицы $(r \times r)$ будет неравен нулю, а $(r+j \times r+1)$ будет равен нулю.

Метод Ш. Метод Грин - Берлекэмп - Месси (ГБМ)

Данный метод основан на использовании теории продолжения

Рассм. систему ур-й для компонент синдрома

$$\sigma_n S_1 + \sigma_{n-1} S_2 + \sigma_{n-2} S_3 + \ldots + \sigma_2 S_{n-1} + \sigma_1 S_n + S_{n+1} = 0$$

$$\sigma_n S_2 + \sigma_{n-1} S_3 + \sigma_{n-2} S_4 + \ldots + \sigma_2 S_n + \sigma_1 S_{n+1} + S_{n+2} = 0$$

$$\sigma_n S_n + \sigma_{n-1} S_{n+1} + \sigma_{n-2} S_{n+2} + \ldots + \sigma_2 S_{2n-2} + \sigma_1 S_{2n-1} + S_{2n} = 0$$

Очевидно, что $\sum_{k=0}^{n} S_{u+j-k} \sigma_k = 0$

Последняя сумма, полученная ранее (*) совпадает с данной, если положить $r = n$ и переобозначить: $u = j+u-1$.

Т.к. каждое ур-е обрисовывается в том смысле, что к-ый σ_i „связывает" компоненты синдрома каждой строки.

Г.О. к-ой ячейки $\sigma(8)$ являются с равной вероятностью, построенной на комплексах синдромов, особое продолжение, начинающее ранее матрицей.

Расположение контрольных символов в шифре:

Расположение под контрольными символами ячейки к-ой ячейки $\sigma(8)$, начиная с левого края перемещения числа, начиная символов двух фаз в двух шифрах; получаем первое ур-е системы.

Если все к-ые σ подобраны правильно по перемещению с нулевой фазой 0.

Сдвинем шифр σ на одну позицию вправо и проделаем по ним самое получим 2-е ур-е и в результате 0

Сдвигая вправо ~~ур~~ начальные символы так-то ошибок n в последней ур-ии достигнем правого края шифра S_1.

Пусть так-то ошибок $V < n$. Сл-но матрица будет иметь меньшую размерность. Продолжаем те же операции с шифрами. Когда после некоторого ур-я шифра σ не достигнет правого края.

Если же продолжать сдвигать шифр вправо, то будут получаться одни нули.

Если обычно обе ~~подобные~~ последовательности $S_{2V+1}, S_{2V+2}, \ldots, S_{2n}$, то их можно было определить с начального связи.

Семинар

Метод Сугиямы.

В методе Сугиямы используется ф-ция $e^{\frac{2\pi}{n}}$, где в случае кольцевого кода РС можно записать, $\alpha^{n/n-k}$

Для кода БЧХ $(n-k)=6$.

Г.О. В методе Сугиямы вычисляем полиномиальную ф-цию z^6 и S(z).

Вектор синдром: 10, 10, 8, 1, 2, 1.

Для получения слова можно и иначе "вокруг" поворотной матрицы можно получить вектор-синдром.

Вычисляем деление в векторной форме.

$+1\,0\,0\,0\,0\,0\,0$ $1\,2\,1\,8\,10\,10$	$1,2,1,8,10,10 = S$
$+2\,1\,8\,10\,10\,0$ $2\,3\,2\,9\,11\,11$	$1,2 = g_1$

$8, 15, 13, 14, 11 = R_1 \quad \deg R_1 = 4 > 3$

Находим U_1

$d \neq 0$

$U_1 = g_1 U_0 + U_{-1} = S(1,2) = 2+2$

$+1\,2\,1\,8\,10\,10$ $1\,2\,5\,6\,3$	$9, 15, 13, 14, 11$
$+12\,2\,14\,12\,10$ $12\,3\,1\,2\,14$	$8, 4 = g_2$

$6+7+11 = R_2 \quad \deg R_2 = 3 = 3$

$U_2 = g_2 U_1 + U_0 = g(1,2) + U(8z+4)(z+2) + 1 =$

$= 8z^2 + 9z + 4z + 5 = 8z^2 + 13z + 2 = (8, 13, 2)$

$$+\begin{array}{r} 9\ 15\ 13\ 14\ 11 \\ 9\ 10\ 10\ 14 \\ \hline 5\ 9\ 0\ 14 \\ 5\ 6\ 6\ 10 \\ \hline 5\ 6\ 14 = R_3 \end{array} \quad \begin{array}{|l} 6\ 8\ 8\ 11 \\ \hline 4\ 15 = g_3 \end{array}$$

$\deg R_3 = 2 < 3.$

$U_3 = g_3 U_2 + U_1 = (4z+15)(8z^2+14z+2) + (z+2) =$

$= 11z^3 + 2z^2 + 5z + 7z^2 + 13z + 1 + z + 2 =$

$= 11z^3 + 12z^2 + 14z + 5 = (11, 12, 14, 5)$

, некоприв. б.

$\Delta = 11z^3 + 12z^2 + 14z + 5$

$\Omega = 5z^2 + 6z + 14$ - некоприв. 3

Удобно д-т Вектора также образом, чтобы

$\nabla_0 = 1$

ξ^{-12}

$\Phi(z) = z^2 + 9z + 10$

$\Theta(z) = 7z^3 + 8z^2 + 10z + 1$

Следствие из произведения полиномов 6 и 5.

$7z^6 + 5z^6 + z^2 + 2z + 10;$

$7z^6 + 0z^7 + 5 \cdot z^6 + 0z^5 + 0z^4 + 0z^3 + z^2 + 2z + 10$

В нашем случае макс кол-во ошибок $n = 3$.

И макс степень $(3 \cdot n - 1) = 8$

Обозначим проверочный полином $\Psi(z)$ Следствие уравнение - $Q(z) = 0$;

$P(z) = 7z^2 + 0z + 5$

$\Theta z = z^6 P(z) + R(z)$

Чтобы убедиться в том, что данное выражение универсально ко всех полиномов $\sigma(z)$ и $S(z)$, и разделим ур-ние на пункты.

Возьмем $\sigma \cdot S$ по z^{2n}, т е

$$\sigma S = h \bmod z^{2n} \quad (n=3).$$

Сравним данное выражение с ключевым ур-ем и увидим, что $h = \omega(z)$.

Т о, зная σ и S, можно найти вектор ω.

Запишем полиномы $R(z)$, $Q(z)$ и $P(z)$ в общем виде:

$$R(z) = S_1\sigma_0 + (S_1\sigma_1 + \sigma_0 S_2)z + (S_1\sigma_2 + S_2\sigma_1 + S_3\sigma_0)z^2 + \ldots +$$

$$+ (S_1\sigma_{n-1} + S_2\sigma_{n-2} + \ldots + S_{n-2}\sigma_2 + S_{n-1}\sigma_1 + S_n\sigma_0)z^{n-1}.$$

$$Q(z) = (S_n\sigma_n + S_{n+1}\sigma_{n-1} + \ldots + S_{2n-1}\sigma_1 + S_{2n}\sigma_0)z^{2n-1} +$$

$$+ (S_{n-1}\sigma_n + S_n\sigma_{n-1} + \ldots + S_{2n-2}\sigma_1 + S_{2n-1}\sigma_2)z^{2n-2} + \ldots +$$

$$+ (S_1\sigma_n + S_2\sigma_{n-1} + \ldots + S_n\sigma_1 + S_{n+1}\sigma_0)z^n.$$

Анализ общего выражения $Q(z)$ показывает, что каждая скобка перед степенью - строка в исходных ур-ниях для компонент синдрома. Но каждая строка равна нулю, следов и $Q(z) \equiv 0$.

$$z^{2n}\cdot P(z) = S_{2n}\sigma_n z^{3n-1} + (S_{2n}\sigma_{n-1} + S_{2n-1}\sigma_n)z^{3n-2} + \ldots +$$

$$+ (S_{2n}\sigma_1 + S_{2n-1}\sigma_2 + \ldots + S_{n+1}\sigma_n)z^{2n}$$

. . . . . .

Нахождение к-тов полинома $\sigma(z)$.

Для нахождения к-тов используем св-во полинома $Q(z)$ обращаться в ноль, когда к-ты σ выбраны правильно

Необходим алгоритм, позволяющий итерационно вычислять новые к-ты $\sigma(z)$, уточняя старые. Когда все к-ты будут определены, то при заданном ранге (кол-ве ошибок) ранжировой матрицы S^k, наш. членов к-тов при дальнейш. продвижении

Чтобы убедиться в том, что данное выражение универсально всех характеристик $G(z)$ и $S(z)$, и доказать р-ние по индукции

Возьмем $G \cdot S \bmod z^{2n}$, т е

$$GS = R \bmod z^{2n} \quad (n=3)$$

Сравним данное выражение с исходным ур-ем и увидим, что $R = \Phi(z)$

Т о, зная G и S, можно найти вектор Φ.

Запишем полиномы $R(z)$, $Q(z)$ и $P(z)$ в общем виде.

$$R(z) = S_1 G_0 + (S_1 G_1 + G_0 S_2) z + (S_1 G_2 + S_2 G_1 + S_3 G_0) z^2 + \ldots +$$

$$+ (S_1 G_{n-1} + S_2 G_{n-2} + \ldots + S_{n-2} G_2 + S_{n-1} G_1 + S_n G_0) z^{n-1}.$$

$$Q(z) = (S_n G_n + S_{n+1} G_{n-1} + \ldots + S_{2n-1} G_1 + S_{2n} G_0) z^{2n-1} +$$

$$+ (S_{n-1} G_n + S_n G_{n-1} + \ldots + S_{2n-2} G_1 + S_{2n-1} G_2) z^{2n-2} + \ldots +$$

$$+ (S_1 G_n + S_2 G_{n-1} + \ldots + S_n G_1 + S_{n+1} G_0) z^n$$

Анализ общего выражения $Q(z)$ показывает, что каждая скобка перед степенью - строка в исходных ур-ниях для коэффициентов синдрома. Но каждая строка равна нулю, следов и $Q(z) \equiv 0$.

$$z^{2n} \cdot P(z) = S_{2n} G_n z^{3n-1} + (S_{2n} G_{n-1} + S_{2n-1} G_n) z^{3n-2} + \ldots +$$

$$+ (S_{2n} G_1 + S_{2n-1} G_2 + \ldots + S_{n+1} G_n) z^{2n}$$

Исполнение к-тов полинома $G(z)$.

Для исполнения к-тов используем св-во полинома $Q(z)$ обращаться в ноль, когда к-ты G будут найдены правильно

Необходим алгоритм, позволяющий итерационно вычислять новые к-ты $G(z)$, уточняя старые. когда все к-ты будут найдены с нулевой, но при задании ранее числа ошибок) Наименьшей матрицы S', полученные к-ты при указанной они правильными

Описывает обеспечение программного управления операциями.

Разработан алгоритм, который для позиции нахождения к-ра записан $G(z)$, сравнивает между к-рой G будет вычитан к-р S с тем возможным состоянием (программными сигналами):
пусто с помощью заданного алгоритма направляет к к-ру G. Возвращает команду на запуск к к-ру.

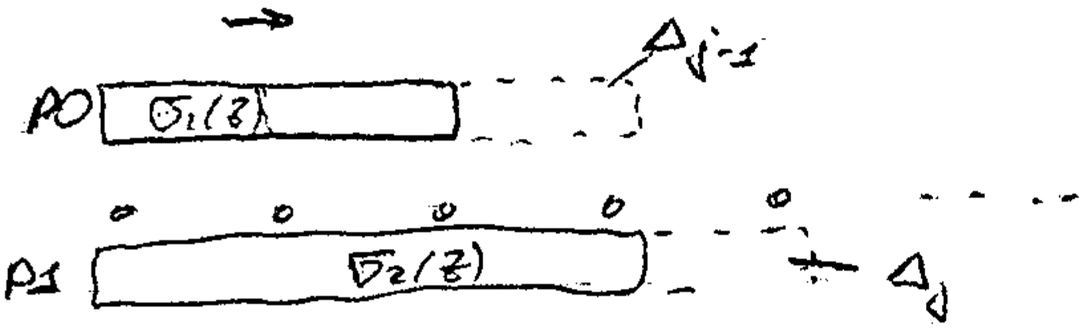
Если это команда определенно удовлетворяет, то:
$S_1 G_2 + S_2 G_1 + S_3 G_0 = 0$. Сравнивает команду с кодом, описывающим в общем виде о не получении. Допустим, что произошла ошибка команды в одном разряде, в котором разность сигнала по-иному отличается от нуля. Вычитание команды из кода Δ. В этой ситуации необх. сформировать условие, с помощью которого или во к-ре G модифицируется или подключается с дополнением нового к-ра, где отмечена позиция $G(z)$ возможна.
Данный данный задачи производится методом d-х регистров, основного и вспомогательного.
Допустим существует промежуточная ситуация, запоминающая переходит до к-ра командой синхронизации, по которой пришел команда. С помощью этого сигнала регистр P_1, который имеет код неправильно к-ра, или дополнительно Δ по обычному циклу производится кодом команды с кодом до не один из, где каждый будет отмечен единицей в своей соответствующей ему, основной регистр. Путь каждого отмечен на нуле. Ну одно возможно Δ не совпадает нулю. Если

– ремонтер подходит с пакетом готовых сообщений с правой стороны, щелкает левой, но все сами, кнопки нет щелкает левой

Вспомогат. ремонтер имеет два формирования основного ремонтера. Допустим, что по вспомогательному алгоритму с помощью вспомогат. ремонтер получает новый основной, при этом вспомогат. модифицируется.

Самым простым способом модификации вспомогат. ремонтера является его замена на основной ремонтер из предыдущ. шага (до смены).

Исходя из этого рассм. пронумеровались шаг:



Основной ремонтер после модификации должен подвинуться, когда об на один шаг и выдаст нужные команды.

Из общих нужных команд продвинем P0 и P1 на шаг, получив Δ_j и Δ_{j-1}, отличные от нуля.

Назовем сумму т-ний при протягивании ремонтера по S связок, если команда равна нулю

При совместном продвижении ремонтеров основной подвигается вперед данные. При этом к-ты б с одинак. индексами будут совпадать.
В пояснительной записке у ремонтеров будут разные состояния & Выровняем индексы 7 памятников. Для того $\sigma_1(7)$ умножим на 2. Тогда состояния у памятников будут одинаковые.
Умножим все к-ты σ_1 на Δ_j, а все к-ты σ_2 на Δ_{j-1}
Тогда команды для обоих ремонтеров будут одинаковыми.

Предполагается подключение подключающего
ОЗ следующим образом после окончания
счета ЭВМ и появления — подается новый
импульс, который сдвигает на один
шаг вправо цифровой код

Новый импульс подвигается на один шаг вправо
в кон-ве модификации РО (ячейки 62(8)). Аналогично
продвигается вперед по шагу общей модификации
ваше РО и РД. Процесс останавливается, когда
скорректированный код сдвинется на нужное
кол-во.

Скорректированный основной массив подключается
показаний для этого нужно решение не только
предыдущего вычитания, но и накопленное уче-
ное. Для этого необходимы СчО + показания
пошагового, с которого корректир. основ
ной пошаг.

В С хранятся границы ячеек для Б, Б
Ф-ция Ф. Алгоритм удобно производить, если осущ.
корректировку вычитания пошагово тут его значение
на предыдущем шаге Тогда на этом шаге его
невязка будет равна единице.

Логика детектирования пошагов Б заключается в
детектировании пошагов предыдущего шага с модификацией, связанной с вычитанием пошагов:

$$\Phi_j(z) = \Phi_{j-1}(z) + \Delta z \; C_{j-1}(z)$$

В ячейке $C_{j-1}(z)$ записаны вычитаемые
пошаги.

Основная задача состоит решая вычитания
невязки по заданным начальным условиям x Бы
Если невязка равна нулю, то основной пошаг
продвигается вперед, а вычитаемый увеличивается на Δz.
Если невязка отлична от нуля, то вычитаемый
вычитаемый пошаг

$$A_j(z) = \Phi_{j-1}(z) + A_j \; z \; C_{j-1}(z).$$

Необходимо проверить, обеспечивает ли данный алгоритм
основной пошаговый интегрирования заданные условия
погрешности

Если обнаружат, что длина регистра достаточна, если нет - то она увеличивается

Номер синдрома S_j определяет макс кол-во ошибок $2t$. Если длина регистра $(L+1)$, то определяется с вводится в вычисление $2L$ и $(L-1)$ для того, чтобы их сравнить

$2L$ - удвоенное кол-во ошибок, связанных с основным регистром.

j - кол-во компонент синдрома, необх. для опр-я $2t$ ошибок.

Сравнивая их приходим к выводу, что если $2L > (j-1)$, то регистр модифицировать не нужно, иначе нужна модификация.

Пусть модификация нужна, тогда рассчит новые полиномы C и D, нормированные по длине уже вычислен новую длину регистра L Тем этом имеем вверху нужные сущ модифик. ции, кот: $2L = j - 1$;

$$L_j + L_t = j - 1;$$
$$L_{j+1} = j - L_j$$

Определение полинома ошибок $\omega(z)$

Полином $\omega(z)$ может быть найден в конце, когда известен полином $\sigma(z)$, по удобной и описанной итерации. Возьмем пр-е для σ_j и данный процесс. получ. полином умножим на вектор S тогда получим структуру аналогичную пр-ию. $\sigma(z)S(z)$. Очевидно:

$$\underbrace{\sigma_j(z)\cdot S}_{\omega_j(z)} = \underbrace{\sigma_{j-1}(z)S}_{\omega_{j-1}(z)} + \Delta_j z\, C_{j-1}(z) S$$

Когда $\sigma(z)$ будет определено точно, то $\sigma_j(z)\, S(z)$ делится $\omega_j(z) \bmod z^{2v}$, v - кол-во ошибок. На практических систем вычисление делают проще делится по модулю - по наименьшему модулю

Нахождение $G(z)$ и $\omega(z)$ методом ФБМ.

0 шаг. $S_1 = 10$, $S_2 = 10$, $S_3 = 8$, $S_4 = 1$, $S_5 = 2$; $S_6 = 1$

$q = 0$, $L_0 = 0$, $\sigma_0 = 1$, $\omega_0 = 0$; $C_0(z) = 1$, $Q(z) = 1$

$n = n - K = 6$

1 шаг. $j = 1$

$$\Delta_1 = \sum_{i=0}^{0} \sigma_i \cdot S_{1-i} = \sigma_0 \cdot S_1 = 1 \cdot 10 = 10 \neq 0$$

$A_1(z) = \sigma_0(z) + \Delta_1 z\, C_0(z) = 1 + 10 \cdot z \cdot 1 = 10z + 1$

$B_1(z) = \omega_0(z) + \Delta_1 Q_0(z) = 0 + 10 = 10$

$2 \cdot 0 > 1 - 1$ — неверно

$C_1(z) = \Delta^{-1}\, \sigma_0(z) = \frac{1}{z} \cdot 1 = \frac{1}{z}$

$\sigma_1(z) = A_0(z) = 10z + 1 \rightarrow \sigma_0 = 1$; $\sigma_1 = 10$.

$Q_1(z) = \Delta^{-1}\, \frac{1}{z}\, \omega_0(z) = \frac{1}{z} \cdot 0 = 0$

$\omega_1(z) = B_0(z) = 10$

$L_1 = q - L_0 = 1$

$\sigma_0 \neq \sigma_1 \neq 0$

2 шаг. $j = 2$

$$\Delta_2 = \sum_{i=0}^{1} \sigma_i S_{2-i} = \sigma_0 S_2 + \sigma_1 S_1 = 1 \cdot 10 + 10 \cdot 10 = 10 + 4 = 2$$

$A_2(z) = \sigma_1(z) + \Delta_2 z\, C_1(z) = 10z + 1 + 2z \cdot \frac{1}{z} = 10z + 1 + 2z = z + 1$

$B_2(z) = \omega_1(z) + \Delta_2 Q_1(z) = 10 + 2 \cdot 0 = 10$

$2 \cdot 1 > 2 - 1$ — ОК

$\sigma_2(z) = A_2(z) = z + 1 \rightarrow \sigma_0 = 1$, $\sigma_1 = 1$

$\omega_2(z) = B_2(z) = 10$ ч.т.д.

$C_2(z) = z\, C_1(z) = z \cdot \frac{1}{z} = 1z$

$Q_2(z) = z\, Q_1(z) = z \cdot 0 = 0$

$L_2 = L_1 = 1$

3 шаг $j = 3$

$$\Delta_3 = \sum_{i=0}^{1} \sigma_i S_{3-i} = \sigma_0 S_3 + \sigma_1 S_2 = 1 \cdot 8 + 1 \cdot 10 = 1 \neq 0$$

$$A_3(z) = \sigma_2(z) + \Delta_3 z C_2(z) = 8 + 1 + 1 \cdot 2 \cdot 2z = 7z^2 + 2 + 1$$
$$B_3(z) = \omega_2(z) + \Delta_3 Q_2(z) = 10 + 1 \cdot 0 = 10$$

$2 \cdot 1 > 3 - 1$ Нет.

$$C_3(z) = \Delta_3^{-1} \sigma_2(z) = 1 \cdot (2z + 1) = 2z + 1$$
$$\sigma_3(z) = A_3(z) = 7z^2 + 2z + 1 \rightarrow \sigma_0 = 1, \sigma_1 = 1, \sigma_2 = 7.$$
$$Q_3(z) = \Delta^{-1} z \, \omega_2(z) = 1 \cdot 10 = 10z$$
$$\omega_3(z) = B_3(z) = 10$$
$$L_3 = 3 - L_2 = 2$$

4 шаг. $j = 4$

$$\Delta_4 = \sum_{i=0}^{2} \sigma_i S_{4-i} = \sigma_0 \cdot S_4 + \sigma_1 S_3 + \sigma_2 S_2 = 1 \cdot 1 + 1 \cdot 8 + 2 \cdot 10 = 10 + 1 = 8 \neq 0$$

$$A_4(z) = \sigma_3(z) + \Delta_4 z C_3(z) = 7z^2 + 2 + 1 + 8z(2z+1) = 7z^2 + 8 + 1 + 8z^2 + 8z =$$
$$= 11z^2 + 10z + 1$$

$$B_4(z) = \omega_3(z) + \Delta_4 Q_3(z) = 10 + 8 \cdot 10z = 2z + 10$$

$2 \cdot 2 > 4 - 1$ Да

$$\sigma_4(z) = A_4(z) = 11z^2 + 10z + 1 \rightarrow \sigma_0 = 1; \sigma_1 = 10, \sigma_2 = 11$$
$$\omega_4(z) = B_4(z) = 2z + 10$$
$$C_4(z) = z C_3(z) = z^2 + 7$$
$$Q_4(z) = z Q_3(z) = 10z^2$$
$$L_4 = L_3 = 2.$$

Определение полинома ошибок $\omega(z)$ (продолжение)

Т.к. для приведенного значения $\sigma_4(z)$, то оно исправит не все связки кратности 3, а только часть α_4, поэтому средняя ошибка часто увеличивается. След-но для текущего j нужно определить такую минимальную e, что $\sigma_j(z)$ S будет равно $A_4(z)$ mod z^e.

Аналогично $\sigma_{j-1}(z)$, но рассматривается следующий случай, когда степень полинома увеличивается равномерно на одну единицу

Тогда $\sigma_{j-1}(z)\,S$ будет иметь на единицу меньшую и равную степени $\sigma_j(z)\,S$ но, если возвести $\sigma_{j-1}(z)\,S$ по модулю не модуло z^e, то получим

$$\sigma_{j-1}(z)\,S = \Omega_{j-1}(z) \bmod z^e.$$

Т.к. если "нулевая область" уже, то всё равно остаток тот же $\Omega_{j-1}(z)$.

В третьем слагаемом заменим $C_{j-1}(z)$ его модификацией и получим,

$$\sigma_j(z)\,S = \sigma_{j-1}(z)\,S + \frac{\Delta_j}{\Delta_{j-1}} z\,\sigma_{j-2}(z)\,S$$

$$C_{j-1}(z) = \frac{\sigma_{j-2}(z)}{\Delta_{j-1}}$$

Здесь $\sigma_{j-2}(z)\cdot S$ также имеет структуру некой текущей Ω. Причем всё второе слагаемое имеет степень такое же, как первое или на единицу больше

Т.е. и во втором слагаемом использование того же модуля, что и для первых двух приведет к получению $\Omega_{j-2}(z)\cdot z$. Аналогично рассуждая получаем заключение следующее ур-е для нахождения Ω в том же виде, что и для δ.

Если ввести вновь, которую назовем

$$\Omega_{j-1}(z) = \frac{1}{\Delta_{j-1}} z\,\sigma_{j-2}(z)\,S.$$

Тогда к исход. ур-ю для отр-я δ, добавим ур-е для отр-я ω:

$$\omega_j(z) = \omega_{j-1}(z) + \Delta_j \Omega_{j-1}(z)$$

Их отличие заключается в том, что вычисление ω текущего шага второе слагаемое от z не умножается. Также вводим вспомогат. регистр $Q(z)$ для вычисления $\omega(z)$. Данный алгоритм показывает, что изменение степени полинома во вспомогат. регистре производится не на шаге итерации, а

при модификации вспомогат. регистра.

Начальные условия для алгоритма

Начальное условие отр-ся исходя из того существования полинома $G(z)$ имеет единств известный к-т $G_0 = 1$. При этом $G(z) - G_0 = 1$ Есть самый минимальный полином, который возможен При этом начальные условия для r следует положить нулевыми

Определение ошибочных позиций.

Номера ошибочных позиций извлекаем из полинома - локатора $G(z)$. Для этого нужно найти корни $G(z)$. В зависимости от кол-ва ошибок $G(z)$ может иметь различные степени. Наиболее часто используются полиномы 2-й и 3-й степеней. Для них разработаны отдельные алгоритмы нахождения корней Более существ. алгоритмы и для полиномов 4-й, 5-й степеней Для большего кол ва ошибок существ общий универсальный алгоритм нахождения корней.

Самый универсальный для конечных полей это есть алгоритм Чена или метод полного перебора. Он заключается в последовательной подстановке в $G(z)$ всех n-го конечного поля $\overline{1}, \overline{\alpha}, \overline{\alpha^2}, \dots, \overline{\alpha^{n-1}}$, для которых $G(z) = 0$ - корни полинома

Решение квадратного уравнения в конечных полях Галуа.

Пусть имеется ур-е

$$A_2 x^2 + A_1 x + A_0 = 0 \quad | : A_2;\ A_2 \neq 0$$

$$x^2 + Ax + B = 0, \quad A = \frac{A_1}{A_2},\ B = \frac{A_0}{A_2}$$

Границами являются $x = A^2$, тогда

$$z^2 + z + Q = 0, \quad \text{где } Q = \frac{B}{A^2}$$

В работе Берлекэмпа установлено, что данное ур-е будет иметь 0 к-ня в конечном поле Галуа, если след эл-та Q в данном поле равен нулю.

$$Sp\,Q = Q + Q^2 + Q^4 + \ldots + Q^{2^{r-1}} = 0, \quad Q = \alpha^{2^r - 1}, \quad GF(2^r)$$

Для получения конкретного вида решения нет понятие нормального базиса поля.

Нулевой элемент. базиса, состоящего из "0" и "1" существует как нормальный, в кач-ве которых выступают элементы. Правило отр-я нормального базиса как элемента требует, чтобы след эл-тов в элементе был равен „1".

Так в GF(2^4) широко исп. базис: 12; 14, 15; 8

Пусть эл-ты базиса $\gamma^1, \gamma^2, \ldots, \gamma^0$. Тогда Q разложается в этом базисе,

$$Q = d_0\gamma^1 + d_1\gamma^2 + \ldots + d_{r-1}\gamma^0,$$

где $d_0, d_1, \ldots, d_{r-1}$ - к-ты разложения

Обозначим z', z'' - два эл-та пр-а. Тогда,

$$z' = \sum_{i=0}^{r-1} z_i \gamma^{2^i}, \quad z'' = \sum_{i=0}^{r-1} \bar{z}_i \gamma^{2^i},$$

$$\bar{z}_i = 1 + z_i; \quad z_i \in \{0, 1\},$$

Тогда к-т z_i находится по ф-ле

$z_0 = 0$; $z_1 = d_1$, $z_2 = d_1 + d_2$, ..., $z_{r-1} = \sum_{i=1}^{r-1} d_i$, т.е.

$$z_j = z_{j-1} + d_j, \quad j = 1, 2, \ldots, r-1.$$

Тогда решение ур-я записывается в виде строки:

$z' = (z_{r-1}, z_{r-2}, \ldots, z_1, z_0)$,

$z'' = (\bar{z}_{r-1}, \bar{z}_{r-2}, \ldots, \bar{z}_1, \bar{z}_0)$.

по данным векторам и таблице к-ов порождающего базиса определ. коэф. в поле a^7.

Рассмотрим порождающий базисный a^4: 8, 15, 14, 12

Рассмотрим метод составления к-ов таблиц для базиса

	8	15	14	12		
0	0	0	0	0	→	0
1	0	0	0	1	→	12
2	0	0	1	0	→	14
3	0	0	1	1	→	5
4	0	1	0	0	→	15
5	0	1	0	1		
6	0	1	1	0		
"	"	"	"	"	"	"

По найден все к-ты разложения векторов в порождающем базисе. Справа получаем столбец из решетов поля a^4. Обычно данную таблицу перестраивают в соответ. с порядком к-ов поля и располагают столбцы в порядке степеней базисного решета

$r = 2$

#	A^3	A^4	A^2	A^1
0	0	0	0	0
1	1	1	1	1
2	0	0	1	1
3	0	1	1	0
4	1	1	0	1
5	1	1	0	0
6	0	1	0	1
7	1	0	1	1
8	0	0	0	1
9	1	0	0	1
10	1	1	1	0
11	1	0	1	0
12	1	0	0	0
13	0	1	1	1
14	0	1	0	0
15	0	0	1	0

Кубическое уравнение

$$A_3 x^3 + A_2 x^2 + A_1 x + A_0 = 0 \quad , A_3 \neq 0$$

$$x^3 + A x^2 + B x + C = 0,$$

Для решения ур-я Кардано и Виет предложили замену $x = y - \frac{A}{3}$, позволяющую избавиться от члена с y^2

$$y^3 + \alpha y + \beta = 0 \quad , \text{где} \quad \alpha = B - \frac{1}{3}A^2, \; \beta = C + \frac{2}{27}A^3 - \frac{1}{3}AB$$

$y = \sqrt{a}\, V$, получим:

$$V^3 + V + E = 0 \quad , \text{где} \quad E = \frac{\beta}{a^{3/2}}$$

В качестве x можно взять:

$$x = y + A \quad , a = B + A^2, \; b = C + AB$$

Получили ур-е, в которое единственным входящим параметром является E, так и в случае четного ур-я, но могут и здесь удалить путем подстановки $\frac{1}{w}$

$$P_t(E) = 0 \quad , \text{где} \quad P_1(E) = E, \; P_2(E) = E,$$

$$P_t(E) = P_{t-1}(E) + E^{2t-3} P_{t-2}(E)$$

Получение ур-я можно заменить последовательностью Ганке Бано - это сделано для общего ур-я и квадратного. Для этого сперва можно перейти: $V = U + \frac{1}{U}$, $U^6 + EU^3 + 1 = 0$,

$$U^3 = v \Rightarrow v^2 + Ev + 1 = 0$$

$$v = Ew \Rightarrow w^2 + w^2 + 0 \cdot w + 0 = 0; \quad v = \frac{-E \pm \sqrt{E^2 - 4}}{2}$$

Получили квадратное ур-е, которое умеем решать.
Далее производим обратный процесс.
Пусть ω_1 и ω_2 найдены и соотв λ_1 и λ_2.
Для дальнейшего нахожд. к-ей достаточно возвести
любое из λ. Извлекаем кубич. корень из $\lambda \to$ получаем
$\omega', \omega'', \omega'''$. Далее находим V_1, V_2, V_3 и окончательно X_1, X_2, X_3.
Для опр-я полных позиций ошибок необх. большого знания, обратим
с использованием подстановок. к-ей ур-я.

Определение величин ошибок.

Пусть ошибочные позиции известны. Введем новые обозначения: e

Имеем, что $\sum_{i=1}^{v} e_i \alpha^{e_i j} \alpha^{e_i (j-1)} = S_j$, v - кол-во ошибок, e_i - величина ошибки

Зная, что кол-во ошибок известно можно составить систему:

$$e_1 \alpha^{e_1 0} + e_2 \alpha^{e_2 0} + e_3 \alpha^{e_3 0} + \dots + e_v \alpha^{e_v 0} = S_1$$

$$e_1 \alpha^{e_1 0} p_1 + e_2 \alpha^{e_2 0} p_2 + \dots + e_v \alpha^{e_v 0} p_v = S_2 \qquad p_i = \alpha^{e_i}$$

$$e_1 \alpha^{e_1 0} p^{v-1} + e_2 \alpha^{e_2 0} p^{v-1} + \dots + e_v \alpha^{e_v 0} p^{v-1} = S_v$$

В полученной системе неизвестными являются величины ошибок.
Расширенную матрицу к-тов левой части системы.
Из первого столбца вынесли $\alpha^{e_1 0}$, из второго - $\alpha^{e_2 0}$ и т.д. - $\alpha^{e_v 0}$. Эти к-ты, т.е их ур-ние, образуют
полином н-й степ. матрицей $p_1^0 p_2^0, p_v^0$.
После выполнения этой операции получаем матрицу Вандермонда.

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ p_1 & p_2 & p_3 & \dots & p_v \\ p_1^2 & p_2^2 & p_3^2 & \dots & p_v^2 \\ \dots & \dots & \dots & \dots & \dots \\ p_1^{v-1} & p_2^{v-1} & p_3^{v-1} & \dots & p_v^{v-1} \end{pmatrix} \cdot p_1^0 p_2^0 p_3^0$$

Семинар

Решение квадратных и кубических ур-ий.

Найдем к-ии ур-я $G(Z) = 8X^3 + 8X^2 + 10X + 1 = 0$ | $\cdot 10$

$X^3 + 2X^2 + 4X + 10 = 0$; $A = 2$, $B = 4$; $C = 10$

$X = y + A = y + 2$

$y^3 + ay + b = 0$, $a = B + A^2 = 4 + 2^2 = 4 + 3 = 7$

$b = C + AB = 10 + 2 \cdot 4 = 10 + 5 = 15$

$y^3 + 7y + 15 = 0$

$y = \sqrt{a}\, V = 4V$

$E = \frac{b}{a^{3/2}} = \frac{15}{7^{3/2}} = \frac{15}{4^3} = \frac{15}{10} = 6$

$V^3 + V + 6 = 0$

$P_1(E) = 6$, $P_2(E) = 6$

$P_3(E) = P_2(E) + 6^{2^{3-3}} P_1(E) = 6 + 6 \cdot 6 = 6 + 11 = 1$

$P_4(E) = P_3(E) + 6^{2^{4-3}} P_2(E) = 1 + 6^2 \cdot 6 = 1 + 1 = 0$

В данном поле сложатся 3 решения данного ур-я.
Сведем его к квадратному

$V = w + \frac{1}{w}$

$w^6 + 6w^3 + 1 = 0$

$w^3 = y$ $\quad y^2 + 6y + 1 = 0$

$y = 6W$

$D = \frac{1}{6^2} = \frac{1}{11} = 6$

$W^2 + W + 6 = 0$

Решим квадратное ур-е. Для этого найдем к-ии разложения 2 в нормальном базисе по таблице 1.

$6 \to \gamma^3 \cdot 0 + \gamma^4 \cdot 1 + \gamma^2 \cdot 0 + \gamma 1 = 6_\gamma$

Вектор $d_0 = 1$, $d_1 = 0$; $d_2 = 1$, $d_3 = 0$.

$$D = \sum_{i=0}^{3} d_i = 0.$$

Вычисляем z_i,

$z_0 = 0$; $z_1 = d_1 = 0$; $z_2 = d_1 + d_2 = 1$, $z_3 = d_1 + d_2 + d_3 = 1$

$z' = (1, 1, 0, 0)$,

$z'' = (0, 0, 1, 1)$.

Находим n-ый член — k-ый др-р, которые обоб дающие др-р, $z' = 5$

$z'' = 2$

(В Q 3 $\in$ = 6 имм 11.)

$D_1 = 6\ 5 = 10$

$D_2 = 6\ 2 = 7$

Берем $D_1 = 10$,

$u = \sqrt[3]{D} = \sqrt[3]{10} =$; $u_1 = 4$

$u_2 = 9$

$u_3 = 14$

$V_1 = u_1 + \frac{1}{u_1} = 4 + \frac{1}{4} = 4 + 13 = 11$

$V_2 = u_2 + \frac{1}{u_2} = 9 + \frac{1}{9} = 9 + 8 = 12$

$V_3 = u_3 + \frac{1}{u_3} = 14 + \frac{1}{14} = 14 + 3 = 15$

$y = 4V$

$y_1 = 4\ 11 = 14$

$y_2 = 4\ 12 = 15$

$y_3 = 4\ 15 = 3$

$X = y + 2$

$X_1 = 14 + 2 = 13$

$X_2 = 15 + 2 = 8$

$X_3 = 3 + 2 = 6$

Т.е $(x+13)(x+8)(x+6) = x^3 + 8x^2 + 10x + 1 = 0$

Найдем номера ошибочных подуцил.

$m_i = \frac{1}{X_i}$

$$m_1 = \frac{1}{13} = 4$$

$$m_2 = \frac{1}{8} = 9$$

$$m_3 = \frac{1}{6} = 11$$

Использование правила Крамера:

Ранее было установлено, что в качестве ур-я для оценки ошибок измерения можно взять Δ можно было определить через матрицу Вак дер Монда

Определитель матрицы Вак дер Монда совпадает как по-иное Вандермонтовский множителей вида.

$$\Delta = \prod_{1 \le j \le i \le n} (p_i - p_j)$$

$$\Delta = (p_2 + p_1)(p_3 + p_2)(p_3 + p_1)(p_4 + p_3)(p_4 + p_2)(p_4 + p_1) \dots (p_n + p_{n-1}) \dots (p_1 + p_0)$$

Пример матрицы 3-го порядка:

$$\begin{pmatrix} 1 & 1 & 1 \\ p_1 & p_2 & p_3 \\ p_1^2 & p_2^2 & p_3^2 \end{pmatrix}, \quad \Delta = (p_2 + p_1)(p_3 + p_1)(p_3 + p_2)$$

Использование правила треугольников вида матрицы для определения ошибок целесообразно выразить определителем через матрицу порядка 6×6

Определение многочлена Δ.

Рассм. многочлен $\sigma(z)$

Его корни, тогда:

$$\sigma(z) = (x+\rho_1 z)(x+\rho_2 z)\dots(x+\rho_\nu z)$$

$$\overleftarrow{\sigma}(z) = (z^\nu+\rho_1)(z^{\nu-1}+\rho_2)\dots(z+\rho_\nu) = z^\nu + (\rho_1+\rho_2+\dots+\rho_\nu)z^{\nu-1} + (\rho_1\rho_2+\rho_1\rho_3+\dots+\rho_{\nu-1}\rho_\nu)z^{\nu-2} + \dots + \rho_1\rho_2\dots\rho_\nu$$

Пример.

$$\sigma(z) = (x+\rho_1 z)(x+\rho_2 z)(x+\rho_3 z) =$$

$$\overleftarrow{\sigma}(z) = (z+\rho_1)(z+\rho_2)(z+\rho_3) = z^3 + (\rho_1+\rho_2+\rho_3)z^2 + (\rho_1\rho_2+\rho_1\rho_3+\rho_2\rho_3)z + \rho_1\rho_2\rho_3$$

Вычислим пр-ную $\overleftarrow{\sigma}(z)$ по z.

$$\overleftarrow{\sigma}'(z) = (z+\rho_2)(z+\rho_3)\dots(z+\rho_\nu) + (z+\rho_1)\left[(z+\rho_3)\dots(z+\rho_\nu) + \dots + (z+\rho_2)\dots(z+\rho_{\nu-1})\right]$$

Подставим в это выражение $z=\rho_x$, тогда каждое слагаемое кроме одного будет нулем:

$$\overleftarrow{\sigma}'(\rho_x) = (\rho_x+\rho_1)(\rho_x+\rho_2)\dots(\rho_x+\rho_\nu)$$

Т.о. произведение в x-ом ρ_x равно произведению множителей, куда входит ρ_x.

С помощью этого выражения Δ можно представить в виде:

$$\Delta = \rho_1^\nu \rho_2^\nu \dots \rho_\nu^\nu \prod_{\substack{i,j \\ i\neq k}} (\rho_i+\rho_j)\,\overleftarrow{\sigma}'(\rho_k)$$

Следующее и последнее Δ

Рассмотрим $\sigma(z)$

Свободный член,

$$\sigma(z) = (1+\rho_1 z)(1+\rho_2 z)\dots(1+\rho_\nu z)$$

$$\overleftarrow{\sigma}(z) = (z+\rho_1)(z+\rho_2)\dots(z+\rho_\nu) = z^\nu + (\rho_1+\rho_2+\dots+\rho_\nu)z^{\nu-1} + (\rho_1\rho_2+\rho_1\rho_3+\dots+\rho_1\rho_\nu)z^{\nu-2} + \dots$$

$$+ \rho_1\rho_2\dots\rho_\nu$$

Пример.

$$\sigma(z) = (1+\rho_1 z)(1+\rho_2 z)(1+\rho_3 z)$$

$$\overleftarrow{\sigma}(z) = (z+\rho_1)(z+\rho_2)(z+\rho_3) = z^3 + (\rho_1+\rho_2+\rho_3)z^2 + (\rho_1\rho_2+\rho_1\rho_3+\rho_2\rho_3)z + \rho_1\rho_2\rho_3$$

Вычислим пр-ную $\overleftarrow{\sigma}(z)$ по z.

$$\overleftarrow{\sigma}'(z) = (z+\rho_2)(z+\rho_3)\dots(z+\rho_\nu) + (z+\rho_3)\left[(z+\rho_3)\dots(z+\rho_\nu)\right] + \dots + (z+\rho_2)\left[(z+\rho_2)\dots(z+\rho_\nu)\right]$$

Подставим в это выражение $z=\rho_1$, тогда правая часть суммы равна нулю.

$$\overleftarrow{\sigma}'(\rho_1) = (\rho_1+\rho_2)(\rho_1+\rho_3)\dots(\rho_1+\rho_\nu)$$

Т.о. произведение в т-ме ρ_1 равна произведению множителей, куда входит ρ_1.

С помощью данной Ф-ции определитель Δ можно записать в виде,

$$\Delta = \rho_1^0\rho_2^1\dots\rho_\nu^{\nu-1}\prod_{\substack{i,k\\ i\neq k}}(\rho_i+\rho_j)\,\overleftarrow{\sigma}'(\rho_k)$$

Вычисление определителя для малого алгоритма.

Возьмем матрицу системы ур-й для вычисления ошибок и вычислим все определители, получим коэффициенты каждого столбца по Крамеру.

без ущерба для общности можно взять 1-ый столбец

Раскроем определитель по 1-му столбцу.

Для матрицы размерности (4×4):

$$\Delta_1 = \begin{vmatrix} S_1 & S_2 & S_3 & S_4 \\ S_2 & P_2 & P_3 & P_4 \\ S_3 & P_2^2 & P_3^2 & P_4^2 \\ S_4 & P_2^3 & P_3^3 & P_4^3 \end{vmatrix} = (P_2+P_3)(P_3+P_4)(P_2+P_4)\Big[S_4 + S_3(P_2+P_3+P_4) + S_2(P_2P_3+P_3P_4+P_4P_2) + S_1 P_2 P_3 P_4 \Big]$$

1/3 примера видно, что алгоритм вычисления Δ в выражении для Δ_1 получается путем вычеркивания из произведения всевозможных сумм P_i, P_j, в которых отсутствует буквенная часть P_k (данного k-го столбца) без вычеркнутых получается Σ_k в выражении для Δ матрицы (4×4), если $P_k = P_i$ добавляется этот множитель:

$$B = \prod_{i,j \neq k} (P_i + P_j)$$

Алгоритм (3) в общем виде

Для Алгоритма производится путем вычисления k-того б и ш, путем из k-ых и получается из пр-ния б·ш.

k-ый опр-ся через предыдущий P_{k-1}

$\Sigma_0 = 1$ $\quad \Sigma_2 = P_1P_2 + P_1P_3 + \dots + P_{k-1}P_k$

$\Sigma = P_1 + P_2 + \dots + P_N$ $\quad$ и т.д.

$\omega_0 = S_1$

$\omega_1 = S_2 + \sigma_1 S_1$

$\omega_2 = S_3 + \sigma_1 S_2 + \sigma_2 S_1$

$\omega_3 = S_4 + \sigma_1 S_3 + \sigma_2 S_2 + \sigma_3 S_1$

- - - - - - - -

Умножим каждую строку ω на соотв. к-т. Получаем

P_k^{v-1}

P_k^{v-2}

P_k^{v-3}

P_k^{v-4}

Видим, что каждый к-т ω зависит от к-тов P, через к-ты σ

После умножения сложим все строки ω_i, при этом вынесем каждую ω_i без S и σ, приведем подобные и получим значение полинома $\overleftarrow{\omega}(P_k)$:

$$\overleftarrow{\omega}(P_k) = S_1 [P_k^{v-1} + \sigma_1 P_k^{v-2} + \sigma_2 P_k^{v-3} + \dots + \sigma_{v-2} P_k + \sigma_{v-1}] +$$

$$+ S_2 [P_k^{v-2} + \sigma_1 P_k^{v-3} + \sigma_2 P_k^{v-4} + \dots + \sigma_{v-3} P_k + \sigma_{v-2}] +$$

$$+ S_3 [P_k^{v-3} + \sigma_1 P_k^{v-4} + \sigma_2 P_k^{v-5} + \dots + \sigma_{v-4} P_k + \sigma_{v-3}] + \dots$$

$$\dots + S_{v-1}(P_k + \sigma_1) + S_v$$

Замечание

Из выражения для $\overleftarrow{\omega}(P_k)$ видно, что этот полином при P_k полностью совпадает с выражением, получающимся при раскрытии определителя по каждому из столбцов с полиномом до последнего к-та B

Теперь при вычислении расширенного определителя достаточно к-т, вычисленный ранее в определителе Δ и использовавшийся с нулевой строкой, $S_1 1 1$. В действительности, нужно добавить к-т, который будет отражать вычисленный ранее полином из $\deg 0, 3-го$ и $5-го$ столбцов, т.к. из $1-го$ столбца этот к-т вычислить не можем,

Т.о. определитель Δ_i можно записать в виде:

$$\Delta_i = P_1^0 P_2^0 \cdot P_{i-1}^0 P_{i+1}^0 \cdots A^0 B \overleftarrow{\omega}(P_i)$$

А определяется Δ:

$$\Delta = P_x^{\nu} P_i^{\rho} \dots P_j^{\rho} B \overline{\sigma}'(P_i)$$

Полная ошибка:

$$e_i = \frac{1}{P_e^{\rho}} \frac{\overline{\omega}(P_i)}{\overline{\sigma}(P_i)}$$ - Формула Форни

Код Рида - Маллера.

Вспомогательные замечания.

Пусть задано множество булевых ф-ций. Обозначим пр-во всех булевых ф-ций как F_n, n-мер-во переменных. Очевидно, что если $f \in F_n$, то

$$f = f(x^1, x^2, \dots, x^n).$$

Существует множество способов представления булевых ф-ций. Рассм. алгебраич. представление булевых ф-ций.

Каждая булева ф-ция может быть представлена единств. образом в виде полинома, степень которого не больше n.

$$f(x^1, x^2, \dots, x^n) = C_0 + \sum_{i=1}^{n} C_i x_i^i + \sum_{1 \le i < j \le n} C_{ij} x^i x^j + \dots + C x^1 x^2 \dots x^n$$

Где булева ф-ция - представима в виде суммы полного различного числа. Слагаемое называется членом.

Расстояние

Рассм пр-во булевых ф-ций размерности n. Тогда в нем базисом в некотором условно любые n-мерные векторы, которые обозначим $e_0^0, e_1^1, \dots, e^{2^n-1}$

Вектор булевой ф-ции в форме полинома представляет собой вектор

К эту ф-цию и она примет некоторое значение
Сам поиск порождающего вектора $v^0, v^1, \dots$, по
которым строку M_f значения ф-ции на всех
векторах.
Аксиоматическое сетевое ф-ции в форме полиномов
Минимальный вес. длина минимального полинома,
входящего в данную ф-цию. Обозначим $\deg f$ -
степень ф-ции.
Пусть $C(n,k)$ - код Рида - Маллера порядка
r и длины n^m называется множество всех строк
M_f всех булевых ф-ций, степень которых
не превышает r. Он обозначается $RM(r,m)$

$$RM(r,m) = \{ M_f \mid f \in F_m, \deg f \le r \}.$$

Чтобы построить порождающую к данного кода
постр. рассм. все задающих ф-ций и множество
возможных таких функций полиномов степ-но
$k = 1 + \binom{m}{1} + \binom{m}{2} + \dots + \binom{m}{r}$.
Минимальное кодовое расст. кода больше
и равно 2^{m-r}

Минимальное кодовое расстояние кода Рида -
Маллера - (2^{m-r}), т.е. код имеет параметры:

$$(2^m, k, 2^{m-r})$$

Код РМ может быть получен при известной
порождающей матрице с помощью перестановки
координат. Порождающая матрица G имеет
блочную структуру

$$G = \begin{pmatrix} G_0 \\ G_1 \\ G_r \end{pmatrix}$$

Он получен из блока полной матрицы
входящих в данный код. Каждому
Коду кроме этих будет строка состоящая из
2^m единиц

Введем в рассмотрение последовательность $(x_1, x_2, \ldots, x_m)$ блок построим ~~последовательность~~ вида

$u_0\ u_1 \ldots u_{2^m-1}$

Будем рассм. некоторую перестановку мож. построить по ф-ле, когда подставляя в них i всех i от $0, \ldots, u_{2^m-1}$, выпишем строку значений этих ~~ф-ций~~ ф-ций.

~~Обозначим~~ Обозначим этот блок G_x и добавим к блоку G_0

$$G_1 = \begin{pmatrix} \Omega_{x_m} \\ \Omega_{x_{m-1}} \\ \cdots \\ \Omega_{x_1} \end{pmatrix}$$

Аналогично построим блок G_2, образованный строками

$$G_2 = \begin{pmatrix} \Omega_{x_m x_{m-1}} \\ \cdots \\ \Omega_{x_1 x_3} \\ \Omega_{x_1 x_2} \end{pmatrix}$$

Т.о. можно формировать блоки для наборов, степень которых не превосходит t.

Объединив все эти блоки, получим порождающую матрицу.

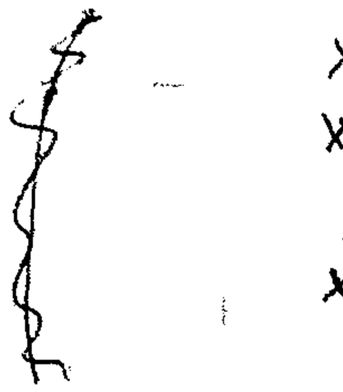
Для всех $0 < r < (m-1)$ справедливо:

$$RM^{-1}(r, m) = RM(m-r-1, m).$$

Двойственный код

Для любых $0 < r < (m-1)$ выполнимость кодом $RM(r, m)$ совпадает с кодом $RM(m-r-1, m)$ ~~совпадает~~ состоящим из всех возможных всех возможных слов координат, где

Введем в пространстве признаков $(x_1, x_2, \ldots, x_m)$ блок



Будем рассм. каждую переключательную как компоненту ... функ-ции, могут подключаться к них блоки $U_0, \ldots, U_{2^m-1}$, выходы которых являются значениями этих функ-ций.

Обозначим этот блок G_x и подключим к блоку G_0

$$G_1 = \begin{pmatrix} \Omega_{x_m} \\ \Omega_{x_{m-1}} \\ \cdots \\ \Omega_{x_1} \end{pmatrix}$$

Аналогично на второй блок G_2, образованный строками:

$$G_2 = \begin{pmatrix} \Omega_{x_m x_{m-1}} \\ \cdots \\ \Omega_{x_1 x_3} \\ \Omega_{x_1 x_2} \end{pmatrix}$$

т.о. можно формировать блоки для произвольного числа которых не превосходит 2^r.

Объединяя соответствующие блоки, получаем порождающую матрицу

Для всех $0 < r < (m-1)$ аналогично:

$$RM^{-1}(r, m) = RM(m-r-1, m).$$

Двойственный код

Для любых $0 < r < (m-1)$ двойственный коду Рида-Маллера порядка r, длины 2^m имеет параметры $[2^m, 2^m - \sum_{i=0}^{r} C_m^i, 2^{r+1}]$ и G_{r+1} — его порождающая матрица

значимо. Булевых ф-ций на нулевом векторе.

Восхолящий код РМ порядка r $RM^*(r, m)$ об. на сл. циклическим кодом длины 2^m-1, нули которого интерпретированы эл-тами α^S, удовл. условиям:

$$1 \le W_2(S) \le m-r-1;$$
$$1 \le S \le 2^m-2;$$

$W_2(S)$ – вес двоичного числа S.

Порождающие и проверочные полиномы кода имеют вид:

$$g(x) = \prod_{\substack{S \in \Omega_m \\ 1 \le W_2(S') \le m-r-1}} m_{\alpha^{S'}}(x)$$

$m_{\alpha^S}(x)$ – минимальный полином α^S.

Семинар

Частотный метод кодирования и декодирования кодов РС.

Рассм. информ. слово A.

ст. мл.

13, 5, 2, 13, 12, 7, 7, 4, 6

Сформируем слово, дополнив информ. сообщение справа "0", недостающими до полной длины кодового слова.

Реализуем обратное преобр. ФМС. При этом используем его св-во:

$$(V_0, V_1, .., V_{n-1}) \Phi^{-1} = (V_0, V_{n-1}, .., V_1) \Phi.$$

Φ – прямое ФМС.

Φ' – обратное ФМС.

Отправляем слово в канал, в котором появилась ошибка. Удаляем слово из канала и начинаем процесс декодирования.

Реализуем прямое ФПС преобразование.

Если ошибок в канале не было, то после прямого ФПС получаем исходную строку с нулями на всех дополнит. позициях. Если же ошибки в канале были, но на дополнит. позициях появились значения. Поэтому дополнит. позиции можно рассм. как вектор-синдром любым методом (Сугиямы, ФБМ) находим только b.

Берем синдром и с помощью к-ов полинома $G(x)$ строим продолжение данного синдрома, построив $(n-r)$ продолжения позиции ко слово

Синдром опр-ет только ошибки в слове, поэтому построив его полное продолжение позиции слова, являющееся самой конфигурацией ошибок. Прибавив данное слово к полученному из канала. Тогда избыточная разряды обнулятся и останется только информационное слово.

$B, 5, 7, 13, 12, 7, 7, 4, 6, 0, 0, 0, 0, 0, 0$
$V_0\ V_1 \dots$ V_{14}

$13, 0, 0, 0, 0, 0, 0, 6, 4, 8, 7, 12, 13, 7, 5$

Дополним слово до ФПС находим и получим

$13, 11, 13, 4, 6, 5, 5, 1, 10, 0, 0, 0, 11, 14, 11$ кодовое слово
$+ \ 0\ 0\ 0\ 4\ 0\ 0\ 0\ 0\ 7\ 0\ 3\ 0\ 0\ 0$ ошибка
$13, 11, 13, 0, 6, 5, 5, 1, 6, 0\ 3, 0, 11, 14, 11$

Производим прямое ФПС преобр над полученным:

$13, 15, 6, 9, 9, 14, 12, 15, 9, 14, 15, 3, 1, 6, 11$

Находим b и ϕ методом

$S = 14, 15, 3, 1, 6, 11$ - Сугиямы

```
  1 0 0 0 0 0 0 | 14 15 3 1 6 11
+ 1 2 5 3 8 13 |  3  4
-----------------
    2 5 3 8 13 0
    2 1 4
```