8.09.06.

Построение кодов переч. идеалов.

Ранее коды строились с помощью min идеалов, путём лин. комбинации примитивн. идемп.
Рассм-м идемп., постр-е на котор-я строк ФНС м-цы. Все они делятся на мин. многочлены кроме множителя
$(x+a^{-1}) = (x+b)$, где a элем. поля F_{2^m}, степени кот. образуют выбранную строку м-цы. Прибавим ед-цу к выбранному идемпту. Как показано ранее получим опять идемпот. Однако он уже не будет делиться на мин. многочлен на кот. делился исходный идемп-т. Остается проверить делимость на $x+b$, для этого запишем исходный идемп-т в виде.

$$b[x^{n-1}+bx^{n-2}+b^2x^{n-3}+\dots+b^{n-2}x+b^{n-1}] =$$
$$= bx^{n-1}+b^2x^{n-2}+b^3x^{n-3}+\dots+b^{n-1}x+1 \quad \text{т.к.}$$
$$b^n=1$$

Кол-во элем. в Σ нечетное. Прибавим к данному идемп-ту 1-цу и останется четное число элементов.

$$bx^{n-1}+b^2x^{n-2}+\dots+b^{n-1}x$$

подст. $x=b$, $\Rightarrow b^n=1$

И получим Σ четн. числа 1-цы.

$$1+1\dots+1=0$$

$\Rightarrow$ данный идемп-т $x+a^{-1}=x+b$

Для ФМС м-цы F_{2^3}

1) $x^6+x^5+x^4+x^3+x^2+x = x(x+1)(x^4+x^2+1)$
2) $7x^6+6x^5+5x^4+4x^3+3x^2+2x = x(x+7)(7x^4+5x^2+3)$
3) $6x^6+4x^5+2x^4+7x^3+5x^2+3x = x(x+6)(6x^4+2x^2+5)$
4) $5x^6+2x^5+6x^4+3x^3+7x^2+4x = x(x+5)(5x^4+6x^2+7)$
5) $4x^6+7x^5+3x^4+6x^3+2x^2+5x = x(x+4)(4x^4+3x^2+2)$
6) $3x^6+5x^5+7x^4+2x^3+4x^2+6x = x(x+3)(3x^4+7x^2+4)$
7) $2x^6+3x^5+4x^4+5x^3+6x^2+7x = x(x+2)(2x^4+4x^2+6)$

Ранее был получен код $g(x) = (x+2)(x-3)(x+4)$
Очевидно, что данный код может быть получен след. путем.
Каждый идеем-т явл. идем-м кода с образующ. элем-м $x + a^{-i}$. Данный код вкл. в себя и др. идеалы ⇒ искомый код может быть получен с пересеч. 3-х идеалов с идем-ми 5, 6 и 7. Примен-я правило пересеч.

$$g(x) = \text{НОД}\{ g_7(x)\, g_6(x)\, g_5(x) \}$$

А порожд-й идем-т кода

$$e_7(x)\, e_6(x)\, e_5(x)$$

$$(2x^6 + 3x^5 + 4x^4 + 5x^3 + 6x^2 + 7x)(3x^6 + 5x^5 + 7x^4 + 2x^3 + 4x^2 + 6x)$$
$$(4x^6 + 7x^5 + 3x^4 + 6x^3 + 2x^2 + 5x) = \underline{7x^6 + 6x^5 + 2x^4 + 4x^3 + 5x^2 + 3x}$$

Постр-е дуального кода

Рассм-м процесс формир-я прямого кода.
Пусть исх. полином $f(x)$ имеет степень a $\deg f(x) = a$

Выделим в табл. II $a+1$ строку, кот. будут участв-ть в формир. кодов. слова $C(x)$ ⇒ в получ-м коде будет
$n - (a+1) = n - a - 1$ нулей

Это нули $\underbrace{2, 3 \text{ и } 1}_{n-a-1}$

Элем обр-е к данным будут нулями дуального кода. Это в поле F_{2^3} ⇒ $\underbrace{7, 6 \text{ и}}_{n-a-1}$ элем-в.

Нули дуального кода $n - [n-a-1] = a+1$
Элем-т $\underbrace{1, 2 \text{ и}}_{a+1}$

(предполаг, что $f(x)$, $f_0 \not\equiv 0$).

Идем рассмотрение корней кодового слова $c(x)$ ⇒ степень порожд-го полинома циклич-го дуального кода $r_1 = a+1$ ⇒ $k = n - r_1 = n - a - 1$.

Опред-м min кодовое расст-е, для этого проанализир-м полином $f(x)$.

Т.к. 1-ца явл. корнем циклич. кода ⇒ 1-я строка в табл. I, II нетождественны ⇒ полином $f_1(x)$ имеет $f_{0_1} \equiv 0$.

Вынесем за скобки в $f_1(x)$ → x, тогда в скобках останется полином $a_1 = n - a - 2$.

Найдем d_1

$$d_1 = n - a_1 = a + 2$$

Имеем дуальный код с пар-ми

$$[n, n-a-1, a+2]_q$$

Кодирование дуального кода

Для код-я можно можно использ. ФМС м-цу у кот. удалена 1-я строка, или же кодир-ть полином в скобках, а затем каждую получ. коорд. умнож. соотв-но 1, 2, 3 и n.

Поэтому дуальный код при кодир-ии не имеет никаких существ-х отличий от кодир. полинома $f(x)$ для прямого кода ⇒ будем относить и дуальный код в коды РС.

Спектральный анализ.

Построим из коэф-ов $f(x)$ вектор длиной $a+1$, дополним его нулями в напр. старших разрядов до max длины n. Возьмем полную ФМС м-цу и осуществим ФМС преобр-е данного вектора. Получим век-р соотв-го полиному $c(x)$ циклич. РС кода.

Т.О. РС коды можно получ. 2-мя способами: 1) вычисление значения полинома $f(x)$ при всех значениях мультипликат. группы поля; 2) умножением информац. полинома на порожд. полином $g(x)$.

Эти 2 способа не явл. независимыми, они связаны через спектральное ФМС преобр-е.

$\exists$ св-во ФМС преобр-я.

Если α^j, где α образ-й элем мультипл. группы поля, корень полинома $f(x)$ $\Rightarrow$

$f(x) = \sum_{i=0}^{n-1} f_i x^i$, то элем-ы $c_j = 0$, где

$c(x) = \sum_{i=0}^{n-1} c_i x^i$ и наоборот, если α^{-j} корень полинома $c(x)$, тогда $f_j = 0$

Т.О. дополняя нулями исходный вектор мы обеспеч-ем корни всех полиномов $c(x)$.

Это один взаимосв. способ ↑

Использование преобраз-е Θ_{-1}

Идемп-т дуального кода можем получ. 2 спос-ми: 1) Σ-ем ~~старой 2,3~~ идемп-ов 2),3),4)

$7x^6+6x^5+5x^4+4x^3+3x^2+2x+1$
$6x^6+4x^5+2x^4+7x^3+5x^2+3x+1$
$5x^6+2x^5+6x^4+3x^3+7x^2+4x+1$

$3x^6+5x^5+4x^4+2x^3+6x^2+7x+1$

Наиболее самое простое получение применяя преобр-е.

$e_1 = 1 + \Theta_{-1}[7x^6+6x^5+2x^4+4x^3+5x^2+3x]$

идемп-т прямого кода.

$\Theta_{-1} = \Theta_6$

Группа. преобр. D_{-1} можно интерпр. след. образом, если степени x считать вычисл-ми то после применения D_{-1} кодо-е слово инвертируется.

Тривиальные коды.

Цепочка-е расш-го метода позволяет выделить следующие 3 кода

1. Пусть полин $f(x)$, $f_0 \neq 0$ и $a = n-1$

Тогда $k = a-1 = n$, $d = n - a = 1$

$[n, n, 1]_q$ – безызбыточный код.

2. Допустим, что $f(x) = f_0 \Rightarrow a = 0$,

$k = a+1 = 1$, $d = n - a = n$

$[n, 1, n]_q$ – код с повторениями

Каждое слово имеет вид

$(f_0, f_0, \ldots, f_0)$

3. Пусть полин. $f(x)$ имеет max степень $a = n-1$ и $f_0 \equiv 0$ (см. II)

$\Rightarrow$ Все кодовые слова делятся на $x+1$

$\Rightarrow$ Σ всех компонент кодового слова $= 0$

Для ост-я кор-ов выносим за скобки x в скобках получится полином в степени $a' = n-2$, тогда $k = a'+1 = a = n-1$

$d = n - a' = 2$

$[n, n-1, 2]_q$ – тривиальные и имеют код $q = 0$.

Укороченные РС коды

Пусть задано мн-во полиномов $f(x)$ степени не выше a, образ. подмн-во $a+1$, опред. кол-во элем-в, подст-х в полином $f(x)$. $n < 2^m - 1$ т.е. длина получ-гося кода будет < примитивной длины.

Расположим все элем-ы использ-е для вычисл-я в естеств-м порядке упорядоч-м полю. Получим (очевидно)

$$[n, a+1, n-a]_q$$

Кодировать укороченные коды можно также с пом. ФМС м-цы, кот. усечена до $a+1$ строки и из кот. вырезаны столбцы соотв. отсутств-м элементов в поле, в котор. использ-м для вычисления.

Полученные кодовые слова не образуют циклич. код т.к. в общем случае все они не делятся на общий полином.

Дуальный укороченный код

Его нельзя построить рассм-м ранее способом (т.к. он циклич-й). Поэтому рассм-м метод. Пусть $f(x)$ некий полином, образ-й прим. код при подст-ке множ-ва элем-в поля. Опред-м ф-цию $\varphi(x)$ соотв-но дуальному коду.

В функц-ом анализе можно опред-ся скалярное произв.

$$\int_{-\infty}^{\infty} f(x)\cdot\varphi(x)\, dx$$

Если ф-ии ортогональны (что необх. для дуального кода), то интеграл $= 0$

Обозн. $F(x) = f(x)\varphi(x) \Rightarrow$

$$\int_{-\infty}^{\infty} F(x)\,dx$$

Пусть $P = \{P_1, P_2, \dots, P_n\}$ мн-во точек, нули-й $\varphi(x)$. Образуем полином

$$Q(x) = (x+P_1)(x+P_2)\dots(x+P_n)$$

Опред. ф-цию $\varphi(x)$ как отнош. полиномов

$$\varphi(x) = \frac{h(x)}{Q(x)}$$ при этом $h(x)$ – "инфорн." полином

множ-во его коэфф. обр. инф. блок дуального кода. Тогда

$$F(x) = \frac{f(x)\,h(x)}{Q(x)} = \frac{P(x)}{Q(x)}$$

Рассмотр. интегр - л

$$\int_{-\infty}^{\infty} \frac{P(x)}{Q(x)}\,dx$$

Вычисление данных интегралов часто проводится с использованием аналитич. продолжения $F(x)$ в расширенной комплексной плоскости. При этом обычно расм-т $Q(z)$ точкой, что все полюса $F(z)$. В нашем случае все полюсы $F(z)$ лежат на вещест. оси $\Rightarrow$ реализуем аналитич. вырожд $F(x)$ на всю расшир-ю компл-ю плоскость. Рассмотрение данного инт-ла заменим аналогом

$$\oint_c F(z)\,dz$$, где c - окр-ть с рад-ом $R \to \infty$

Введем дополнит. ограничения, пусть степень полинома $\deg P(x) = n$, а $\deg Q(x) = m$

Потребуем $m - n \geq 2$

Степень числ-ля как мин на 2 ед-цы < степ-и знам-ля. Оценим модуль $|F(z)|$.

$$|F(z)| \le \left| \frac{P_n z^n + P_{n-1} z^{n-1} + \dots + P_0}{Q_m z^m + Q_{m-1} z^{m-1} + \dots + Q_0} \right| \le$$

$$\le \left| \frac{P_n}{Q_m z^{m-n}} \cdot \frac{\left(1 + \dots + \frac{P_0}{P_n z^n}\right)}{\left(1 + \dots + \frac{Q_0}{Q_m z^m}\right)} \right|$$

Обозначим $|z| = R$, тогда $|F(z)| \le \frac{C}{R^2}$ при $R \to \infty$, тогда $\left| \oint_C F(z)\,dz \right| \le \frac{C}{R^2} \cdot 2\pi R = \frac{2\pi C}{R}$

$C = const$; $C = \left| \frac{2P_n}{Q_m} \right|$

т. о. при $R \to \infty$ интеграл $\to 0$

С др. стороны

$$\oint_C F(z)\,dz = 2\pi i \sum_{p_i} \operatorname{Res}_{p_i} F(z) = 0$$

$$\Rightarrow \sum_{p_i} \operatorname{Res}_{p_i} F(z) = 0$$

Мы опред. ф-цию $F(z)$ т. о. что все полюса у нее простые.

Изв-но что

$$\operatorname{Res}_{p_i} F(z) = \lim_{z \to p_i} (z + p_i) F(z)$$

Используем данную формулу для вычисл. вычетов.

$$\operatorname{Res}_{p_i} \frac{f(x)\,h(x)}{(x+p_1)(x+p_2)\dots(x+p_n)} = \frac{f(p_i)\,h(p_i)}{(p_i+p_1)\dots(p_i+p_n)}$$

Тогда Σ всех рассм. вычетов также будет $= 0$

запишем вычет для вычетов в виде

$$f(p_i) \operatorname{Res}_{p_i} \frac{h(p_i)}{(p_i+p_1)\dots(p_i+p_n)}$$

p_i – текущее значение, тогда получим вектор неизв. кот. будут все возм. вычеты.

Если каждую комп. $*f(P_i)$, то напр. скалярн. произв. полин. на полин. $F(x)$ и век-ра с коорд. в виде вычита.

Очевидно что скалярн. произв. $= 0$ и вектор постр-й на основе вычетов ортогонален исходному вектору.

Тогда обозначим ф-цию

$$\frac{h(x)}{(x+p_1)(x+p_2)\ldots(x+p_n)} = \varphi(x) \Rightarrow \text{дуальный код}$$

образуется как отображение

$$\varphi(x) \to (\mathrm{Res}_{p_1}\varphi(x), \mathrm{Res}_{p_2}\varphi(x), \ldots, \mathrm{Res}_{p_n}\varphi(x))$$

Введем век. простр-во.

Пусть $g_0(x) = \frac{1}{(x+p_1)(x+p_2)\ldots(x+p_n)}$ т.к.

степень $= \deg$

$\deg Q(x) - \deg P(x) \geq 2$

$\deg f(x) = a$, то степень $\deg f(x)\,h(n) \leq n-2$

где степень $\deg Q(x) = n$

$\Rightarrow \deg h(x) = n-a-2$, тогда построим векторы $g_e(x) = x^e g_0(x)$ $0 \leq e \leq n-a-2$

$\Rightarrow$ Данные векторы будут базисными для данного кода

15.11.06.

Укороченные коды Р-С

Определив базис $x^{l} g_0(x)$ можно получить ф-цию в виде полинома $h(x)$
Найдем величины опред-но всех полюсов опред-х набором элем- нулевыми гр. поля получим кодовое слово.

$$y_i = \prod_{(j \neq i)} \frac{1}{(P_i + P_j)}$$

На множестве элем. произведем кодирование $h(x)$ и каждую коорд. получ. слова умножим на соотв. y_i. Если дополнить мн-во элем-в поля, то все нулевыми. группы

$$y_i \in \{1, 2, 3, .., n\}$$

Кодирование можно также производить с помощью усеч-й, вырож-й м-цы ФНС, с помощью которой производим кодирование по полиному $h(x)$ предварительно умножив каждый столбец на соотв-ее y_i

Определение циклич-х кодов РС

Известно опред. кодов РС как подкласс более широкого класса кодов БЧХ. При этом предполагается что порождающий многочлен $g(z)$ разлагается на множители и имеет корни

$\alpha, \alpha^2, .., \alpha^{d-1}$

α - образ-й элем. примитив-й гр. поля F_{2^r}

d - мин кодовое расстояние.

тогда

$$g(z) = (z+\alpha)(z+\alpha^2) \cdot .. (z+\alpha^{d-1})$$

Очень суженное и старое определение

Рассмотрим

$\alpha, \alpha^{\nu+1} .., \alpha^{\nu+d-2}$

$\nu = 0, 1, 2 ..$

Коды построенные по данным корням ~~...~~ порожд-х полиномах при разные ν практически не отлич-ся в методах кодир-я и декодир-я.
В наст. время $\exists$ тенденция считать кодами Р-С коды корнями которых явл.
$\alpha^{\nu}, \alpha^{\nu+1}, ..., \alpha^{\nu+m-2}$ (недвоичные коды)

Когда говорят о более широком классе БЧХ кодов, то предполаг-т 2-е коды.

Обычно α принимают $=2$
Кодир-е и декодир-е кодов Р-С производят во временой или частот-ой обл-ти. порожд.
Во врем-й обл. кодир. произв-т полиномом $g(z)$, а опред. синдрома с помощью проверочной матрицы H.
В частотном методе использ-ся ФНС преобр-я.

Временой метод.

Примен порожд. полином.

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

$\nu = 0, 1, 2, ...$

F_{2^r}

$m = n - k = d - 1 = 2t$

t - кол-во ошибок, кот. исправляет код.
обычно $\nu = 0, 1$.

Но иногда выбирают >1, если надо получить заданный вид полинома или матрицу.
m - выбир. четным.
Провер. м-ца - это вырезка из ФНС м-цы

1-я её строка опред-ся пар-ом ϑ, а последн. m,

$$H = \begin{pmatrix} 1 & \alpha^{\vartheta} & \alpha^{2\vartheta} & \alpha^{3\vartheta} & \dots & \alpha^{(n-2)\vartheta} & \alpha^{(n-1)\vartheta} \\ 1 & \alpha^{\vartheta+1} & \alpha^{2(\vartheta+1)} & \dots & \dots & & \alpha^{(n-1)(\vartheta+1)} \\ \dots & & & & & & \dots \\ 1 & \alpha^{\vartheta+m-1} & \alpha^{2(\vartheta+m-1)} & \dots & & & \alpha^{(n-1)(\vartheta+m-1)} \end{pmatrix}$$

В завис-ти от того, с какого многочлена начинается $g(z)$, $z+\alpha^{\vartheta}$, производится сдвиг нач. строки ФМС м-цы.

Анализ структуры компонент синдрома.

Для разраб. алгоритмов декодир-я необх. проанализировать компоненты в-ра синдрома. Обычно кодир-е произв. в несист-м виде и после прохождения сообщ. через канал, получаем слово U искаж. ошибками.

Пусть S в-р синдрома

$S_1, S_2, \dots, S_m$

$S = U H^T$

вектор строка

Пусть в слове U имеется v ошибок где i номер ошибки $0 \le i \le v$

Пусть ℓ_i – номера позиций в ком. имеющих ошибки $\ell_i = 0, 1, 2, \dots, n-1$

e_i – вел-на ошибки в позиции ℓ_i

Учитывая вид провер-й м-цы можно записать для j-й компоненты синдрома

$$\sum_{i=1}^{v} e_i \alpha^{\ell_i(\vartheta+j-1)} = S_j$$

Т.к. компон-ы синдрома опред. лишь конфигур. в-ра ошибок, а не передав-м сообщ., то S_j зависит от e_i, ℓ_i

Где $j = 1, 2, \ldots, n$

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

Вместо α возьмем $\alpha = 2$

Тогда $\alpha^{e_i} = X_i$ – нах. локатором ошибки

$e_i = 1, 2, \ldots, n$

Вел-на ошибки характеризуется

$$Y_i = e_i \alpha^{e_i v}$$

множителем $\alpha^{e_i v}$

Это нужно учесть при вычислении e_i, тогда S_j перепишем в виде

$$\sum_{i=1}^{v} Y_i X_i^{j-1} = S_j$$

Данное ур-е порождает систему при всех j

$$\sum_{i=1}^{v} Y_i X_i^0 = Y_1 X_1^0 + Y_2 X_2^0 + \ldots + Y_v X_v^0 = S_1 \quad j = 1$$

$$\sum_{i=1}^{v} Y_i X_i = Y_1 X_1 + Y_2 X_2 + \ldots + Y_v X_v = S_2 \quad j = 2$$

$$\sum_{i=1}^{v} Y_i X_i^2 = Y X_1^2 + Y_2 X_2^2 + \ldots + Y_v X_v^2 = S_3 \quad j = 3$$

$$\sum_{i=1}^{v} Y_i X_i^{m-1} = Y_1 X_1^{m-1} + Y_2 X_2^{m-1} + \ldots Y_v X_v^{m-1} = S_m \quad j = m$$

Данная сист. явл. нелин. отн-но неизв-х X_i Y_i известным можно построить синдром S_i, поэтому используем доп. приемы

Введем полином локатора, кот. имеет корни X_i^{-1}; $\sigma(z) = (1 + X_1 z)(1 + X_2 z) \ldots (1 + X_v z)$

v – кол-во ошибок.

$= \sigma_\nu z^\nu + \sigma_{\nu-1} z^{\nu-1} + \dots + \sigma_1 z + \sigma_0$

$\sigma_0 = 1$

Степень полинома опред-ся кол-ом ошибок ν, кот. в общем случае $<$ max значения.

Подставим в $\sigma(z) \to z = X_i^{-1}$

тогда

$\sigma(X_i^{-1}) = 0$

Умножим левую и правую часть выражения на $Y_i X_i^{j+\nu-1}$ тогда получим.

$$\sigma_\nu Y_i X_i^{j-1} + \sigma_{\nu-1} Y_i X_i^{j} + \sigma_{\nu-2} Y_i X_i^{j+1} + \dots + \sigma_1 Y_i X_i^{j+\nu-2} + Y_i X_i^{j+\nu-1} = 0$$

Просуммируем по i каждый член выражения.

$$\sigma_\nu \sum_{i=1}^{\nu} Y_i X_i^{j-1} + \sigma_{\nu-1} \sum_{i=1}^{\nu} Y_i X_i^{j} + \sigma_{\nu-2} \sum_{i=1}^{\nu} Y_i X_i^{j+1} + \dots + \sigma_1 \sum_{i=1}^{\nu} Y_i X_i^{j+\nu-2} + \sum_{i=1}^{\nu} Y_i X_i^{j+\nu-1} = 0$$

Под Σ – и есть компоненты в-ра синдрома

Тогда получим

$$\sigma_\nu S_j + \sigma_{\nu-1} S_{j+1} + \sigma_{\nu-2} S_{j+2} + \dots + \sigma_1 S_{j+\nu-1} + S_{\nu+\nu} = 0$$

$1 \le j \le \nu$

Последн. ур. определяет систему при различных j

$$\sigma_\nu S_1 + \sigma_{\nu-1} S_2 + \sigma_{\nu-2} S_3 + \dots + \sigma_1 S_\nu + S_{\nu-1} = 0$$
$$\sigma_\nu S_2 + \sigma_{\nu-1} S_3 + \sigma_{\nu-2} S_4 + \dots + \sigma_1 S_{\nu+1} + S_{\nu+2} = 0$$
$$\sigma_\nu S_\nu + \sigma_{\nu-1} S_{\nu+1} + \sigma_{\nu-2} S_{\nu+2} + \dots + \sigma_1 S_{2\nu-1} + S_{2\nu} = 0$$

Эта система неоднородных лин. ур-й относ. коэф-в полинома локаторов. $\sigma_1, \sigma_2, \dots \sigma_\nu$

Лекция 15.11.06 (нет начала)

$$\sigma_v S_1 + \sigma_{v-1} S_2 + \sigma_{v-2} S_3 + \ldots + \sigma_1 S_v + S_{v+1} = 0$$

$$\sigma_v S_2 + \sigma_{v-1} S_3 + \sigma_{v-2} S_4 + \ldots \sigma_1 S_{v+1} + S_{v+2} = 0$$

$$\vdots$$

$$\sigma_v S_v + \sigma_{v-1} S_{v+1} + \sigma_{v-2} S_{v+2} + \ldots + \sigma_1 S_{2v-1} + S_{2v} = 0$$

Эта система неодн. лин. ур. относит. коэф. полинома локаторов $\sigma_1, \sigma_2 \ldots \sigma_v$. Если перенести столбец свободных членов вправо, то получим матрицу коэф. из компон. вектора синдрома.

Данную систему можно решить обычными методами, однако кол-во ошибок заранее не известно и не известен порядок системы. Кроме того кол-во ошибок м.б. большим, поэтому используются другие методы для нахождения эф-го решения.

Рассмотрим квадр. матрицу коэф. при σ_i. Проведём в матрице побочн. диагональ. Тогда на всех прямых, пар. этой диагонали, будут на всех элементах, а значит элементы равными между собой. Такие матрицы назыв. Ганкелевыми.

Ганкелевы матрицы

Рассмотрим произв. Ганкелеву матрицу A с элементами a_{ij} и будем её сравнивать с матрицей из компонентов синдрома.

Если матрица Ганкелева, то

$a_{ij} = a_{kl}$, если $i+j = k+l$.

Запишем произв. Ганкелеву матрицу

$a_1 \; a_2 \; a_3 \ldots a_n \; a_{n+1}$

$a_2 \; a_3 \; a_4 \ldots a_{n+1} \; a_{n+2}$

$a_3 \; a_4 \; a_5 \ldots a_{n+2} \; a_{n+3}$

$\ldots$

$a_n \; a_{n+1} \; a_{n+2} \ldots a_{2n}$

опред. элементами первой строки и последнего столбца

Данная матрица явл. постр. по компонентам синдрома, если $v = n$ (расширенная)

Расширение матрицы. Продолжение.

Пусть имеется простая Ганкелева матрица. Дополним её одним столбцом и строкой чтобы она и ост. последовательной.

$a_1 \; a_2 \; a_3 \; a_4$
$a_2 \; a_3 \; a_4 \; a_5$
$a_3 \; a_4 \; a_5 \; a_6$
$a_4 \; a_5 \; a_6 \; a_7$

Расширение первое матрицы можно получить второе и т.д. расширение.

Пусть матрица $n \times n+1$ и $n \times n$

При расширении матрицы ранг может ост. неизменным или же увеличится на 1.

Рассмотрим такие расширения, при к. ранг остается неизменен.

Рассмотрим расширение матрицы $n \times (n+1)$

$a_1 \; a_2 \; a_3 \; a_4$
$a_2 \; a_3 \; a_4 \; a_5$
$a_3 \; a_4 \; a_5 \; a_6$
$a_4 \; a_5 \; a_6 \; a_7$
$a_5 \; a_6 \; a_7 \; a_8$

Неизв. элемент a_7 и т.д. могут продолжение виду, а по ним формировать новые расшир. квадр. матрицы.
ср. с матрицей комп. синдрома

$S_1 \; S_2 \; S_3 \ldots S_v \; S_{v+1}$

$S_2 \; S_3 \; S_4 \ldots S_{v+1} \; S_{v+2}$

$\ldots$

$S_v \; S_{v+1} \; S_{v+2} \ldots S_{2v-1} \; S_{2v}$

Из ур. приведенных ранее видим что для каждой строки существ. параметры

$\sigma_v \; \sigma_{v-2} \; \sigma_{v-1} \ldots \sigma_1 \; \sigma_0 = 1$
к. связывают все компоненты одной строки

Для произв. ганкелевой матрицы ранга r, в L при бесконечном продолжении сохраняем ее ранг, существует r таких чисел, что выполняется $-a_{n+1} =$

$$= b_1 a_n + b_2 a_{n-1} + \dots + b_r a_{n-r+1} =$$

$$= \sum_{k=1}^{r} a_{n-k+1} b_k$$

можно опр. новые членов элемент (при расширении вниз) с помощью данного соотношения. Для матриц на компонентах синдрома при $v=n$, каждая строка имеет вид $\sum_{k=0} S_{n+j-k} b_k$. Данное выражение совпадает с предыдущим, если положить $r = n$, $n = n+j-1$

⇒ для матриц, постр. на компонентах синдрома, можно использовать теорию ее продолжения вниз. Схем-но это можно представить в след. виде

b_3	b_2	b_1	b_0
a_1	a_2	a_3	a_4
a_2	a_3	a_4	a_5
a_3	a_4	a_5	a_6
a_4	a_5	a_6	a_7

При продолжении вниз также связаны с помощью коэф. $b_3\ b_2\ b_1\ b_0$.

$$b_3 a_1 + b_2 a_2 + b_1 a_3 + b_0 a_4 = 0$$

$$\dots$$

$$b_3 a_4 + b_2 a_5 + b_1 a_6 + b_0 a_7 = 0$$

$b_0 = 1 \longrightarrow a_7$

Подобным образом можно расширить матрицу и получить коорд. бесконечно.

Допустим, что max значение ошибок равно n. Тогда прям. матрица на синдр. имеет ранг n и размер $n \times n+1$. Опр. комп. $S_1, S_2 \dots S_{2n}$. Если кол-во ошибок < max, то получ. , при этом можно исп. $2v$ компонент синдромов. Будем расширять матрицу размера v на $v+1$. Тогда сначала вычисляем оставшиеся компон. синдрома, а далее вычисляем новые компоненты матрицы. В таком случае за основу возьмем матрицу постр. на всех комп. синдрома. Продолжение, не изм. ранг матрицы будет линейн. особым