4.11.06.

Разложение $x^n - 1$ (полинома)
разл. в поле F_{2^m}
обычно рассм-т коды с $n = 2^m - 1$
(коды примитивной длины).
В данном поле $x^n + 1$ раскладывается на линейные множители т.е.

$$x^n + 1 = (x+1)(x+2)\dots(x+n)$$

Пусть α – образующий элемент $F_{2^m}^*$ мультипликативной группы поля.

$$x^n + 1 = \prod_{i=1}^{n-1} (x + \alpha^i)$$

Объединим все индексы i в одно мн-во I

$$I = \{0, 1, 2, \dots, n-1\}$$

Выделим из этого мн-ва подмножество
$I_1 \subset I$

$g(x) = \prod_{i \in I_1} (x + \alpha^i)$ делит мн-н $x^n + 1$

$\Rightarrow$ они явл. образующими для соотв-го идеала (кода).

Полиномов $g(x)$ будет столько, ск-ко подмножеств I_1. Среди них будут полиномы у кот. мн-во степеней пробегает полностью 1 или неск-ко смежных. классов.
У таких полиномов коэфф принадл. полю F_2

2. разложение в поле F_2
В F_2, $x^n + 1$ разлагается произведение тех же полиномов. Каждый из них образует свой идеал.

Кодирование циклических кодов.

Пусть степенной полином $g(x)$ кон. степени делит x^n+1 и его степень $= r$, тогда с пом. этого полинома получим код длины n, где $k = n-r$ (k - число инф. симв.)
Рассм. блок инф. символов k.
Поставим ему в соответ. инф. полином
$f(x) = f_0 + f_1 x + \dots + f_{k-1} x^{k-1}$.

Степень полинома не выше $k-1$
Опред. кодовое слово $c(x)$ как

$$c(x) = f(x)\,g(x)$$

Данное кодирование явл. несистематическим.
В общем случае коэфф. $c(x)$ из поля F_{2^m} и код явл. недвоичным. Однако, если $g(x)$ т/к полином, а инф-е слово записано в алфавите из символов F_2, то $c(x)$ становится двоичным кодом. Двоичные коды имеют особенности при анализе. Для них строим спец-ые алгоритмы.

Пусть все кодовые слова делятся на $1+x$
$c(x) = (1+x)\varphi(x)$

Такой код наз. кодом с пров-кой на четность.
Пусть $x=1 \Rightarrow c(1)=0$
с др. стор. $c(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1}$
И $c(1)=0 \Rightarrow$ единичных коэфф-в в кодовом слове будет четное число $\Rightarrow$ будут обнаруж. все ошибки с нечетным весом вектора ошибки.

Пусть c - циклический код, а c_1 код такой, что $c_1 \subset c$
$c \leftrightarrow g(x)$, $c_1 \leftrightarrow g_1(x)$ - порожд-й полиномы
тогда $g_1(x)$ делит $g(x)$ ($g_1(x) \mid g(x)$)

Несистематическое кодирование

Рассмотрим $c(x) = f(x)\,g(x)$

$c(x) = (f_0 + f_1 x + f_2 x^2 + \dots + f_{k-1} x^{k-1})\,g(x) =$

$= f_0 g(x) + f_1 x g(x) + f_2 x^2 g(x) + \dots + f_{k-1} x^{k-1} g(x)$

Рассм-м векторы соотв-е данному

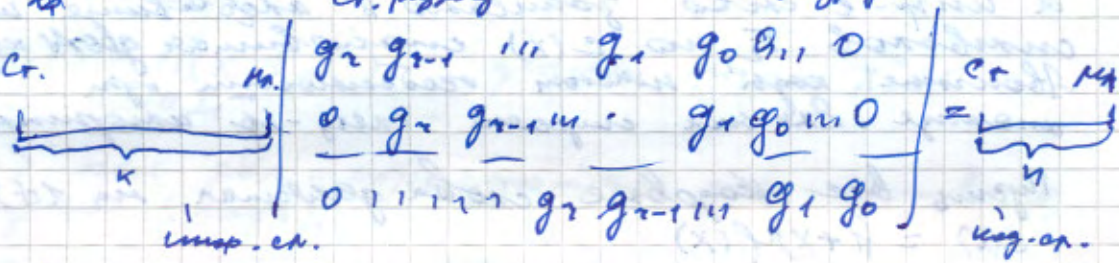
$g(x)$, $x\,g(x)$, $x^2 g(x)$, $\dots$, $x^{k-1} g(x)$

Очевидно, что $c(x)$ образ-ся как лин. комбинация этих векторов с коэф. $f_0, f_1, \dots, f_{k-1}$

Возьмем эти век. (лин. независ.) в качестве базиса $\Rightarrow$ нам нужно построить порожд-ю матрицу G

Матрицу G можно записать 2-я способами.

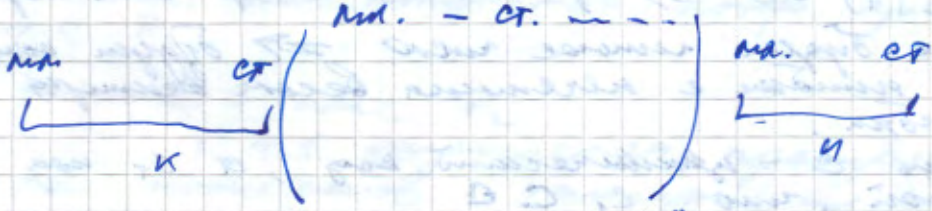
1.



k – строк и n – столбцов.

При такой записи инф. и кодовое слово имеют расположение, указ-е выше.

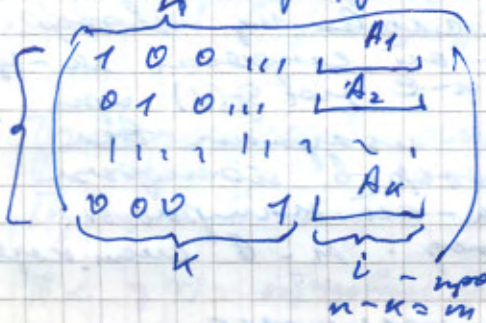
2.



Матрица несистематическая.

Кодирование систематич. n-цы.

Рассм-м стр-ру систем. матрицы:



Поставим в соотв. каждой строке n-цы полином, тогда e-ую строку начиная сверху запишем в виде:

$$x^{n-e} + A_i(x)$$

A_i - полином соотв-й i-й последов-сти символов в подматрице A

Разделим x^{n-e} на $g(x)$

$e = 1, 2, \dots, k$

$$\frac{x^{n-e}}{g(x)} = q(x) + \frac{R_e(x)}{g(x)} \qquad (7.1)$$

$q(x)$ - частное, $R_e(x)$ - остаток от деления. $g(x)$ имеет степень $n = n - k$ $\Rightarrow$ остаток $R_e(x)$ имеет степень ~~на~~ меньше $n-k$ $\Rightarrow$ кол-во символов не превышает m.

Умножим 7.1 на $g(x)$

$$x^{n-e} = q(x)\,g(x) + R_e(x)$$

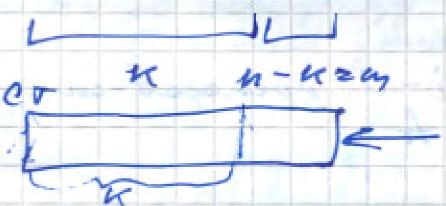
Перенесем $R_e(x)$ влево

$$x^{n-e} + R_e(x) = q(x)\,g(x) \qquad (7.2)$$

(7.2) в правой части $g(x)\, q(x)$ соотв. вектор для слова соотв. циклич. кода ~~слову~~.
=> и в левой части слово цикл. кода.
Очевидно что это слово из коэфф полинома соотв. l-ой строки м-цы.
Произведя деление x^{n-l} на $g(x)$ при всех $l = 1, 2, \ldots, k$ получим все остатки $R_l(x)$ из коэфф-в которых получаем A_l систем-ой матрицы.
Т.к. получили порожд. м-в систем. коде.

Сист. кодирование полинома.

Представим слово цикл. кода в систем-м виде, для этого возьмем регистр длиной n, ввод справа, ст. раз слева.



Введем регистр инф.

Продвинем инф. слово до левой границы регистра (на $n-k = m$ шагов, или ячеек). Данному слову будет соотв. $x^{n-k} f(x)$.
Разделим эту вел-ну на $g(x)$

$$\frac{x^{n-k} f(x)}{g(x)} = q(x) + \frac{R(x)}{g(x)} \qquad (7.3)$$

$q(x)$ — частн., $R(x)$ — остаток от деления

Каков порядок полинома
Очевидно что степень полинома $R(x) < m$
Умножим 7.3 на $g(x)$ и перенесем $R(x)$ влево.

$$x^{n-k} f(x) + R(x) = q(x)\, g(x) \qquad (7,4)$$

кодовое слово из кода => и слева ↑

Запишем в регистр символ соотв. полиному $R(x)$ на своб. с разряды справа т.к. кол-во коэф $R(x)$ не превыш. r, то остаток и коэф. символы в регистре не перекр-ся.

Проверочный полином

Пусть C код с порожд-м полиномом $g(x)$

Т.к. $g(x)$ образован произв-ем лин. множителей, то он имеет n-корней, где n - степень полинома. Все корни наз. нулями кода. Корни принадлежат коду K_{2^m}. Все остальные элем. кода наз. ненулевыми.

Т.к. $g(x)$ делит x^{n+1}, то $h(x) = \frac{x^n+1}{g(x)}$

наз. проверочным полиномом кода.

$n-r = k$. С помощью полинома $h(x)$ тоже можно кодировать, однако получаемый код наз дополнительным кодом C (не дуальным, а дополнительным).

$h(x)\,g(x) = 0$ по модулю x^n+1 (7,5)

Полиномы $h(x)$ и $g(x)$ орт. ортогональными

$\Rightarrow$ орт и $x^i h(x)\, x^j g(x)$ (7,6)

Однако векторы сост. из ~~векторов~~ коэф. полиномов 7.5 и 7.6 орт. лишь в том случае если коэф. одного из полиномов инверсировались.

Возьмем коэф. полинома $h(x)$ и построим на полуш. векторе n-ку $(n-k)$ нулей (слева старшие разряды!)

Инвертируем каждую строку и получим след-ю матрицу.

$$\begin{pmatrix} 0,\dots,0\, h_0 \dots h_{k-1}\, h_k \\ 0,\dots,0\, h_0 \dots h_{k-1}\, h_k\, 0 \\ \dots \\ h_0\, h_1 \dots h_k\, 0,\dots,0 \end{pmatrix}$$

Данная м. наз. проверочной м-й для кода C с порождающим полиномом $g(x)$.
При умножении кодового слова строки на транспонир-ю м-цу получаем синдром.
Данная м. несистематическая.
Сист-ю м. можно получить из сист. м-цы G кот. приведена выше.
Для циклического кода наличие ошибки можно опред-ть делением слова на полином $g(x)$. Наличие остатка говорит о ошибке в слове.

Идемпотенты.

Прим. для цикл. кода.
Полином $K(x)$ также как и $g(x)$ будет порождать идеал и соотв. ему код если наибольший общий делитель

$$НОД[K(x), x^n+1] = g(x)$$

Полином $e(x)$ наз. идемпотентом если $e^2(x) = e(x)$. Иногда его так же наз. проектором.
Пусть C код с порожд. и провер-м полиномами $g(x)$ и $h(x)$, тогда для идеала порожд-го $g(x)$ сущ. единств. идемпот. $e(x)$, кот. также порожд. этот идеал.
Полин. $h(x)$ и $g(x)$ взаимно просты т.к. имеют различные коды. (нули одного не нули др-го).

$\exists\ a(x)$ и $b(x)$ т. что $a(x)g(x) - b(x)h(x) = 1$

Рассм-м полином $e(x) = a(x)g(x)$ тогда

$a(x)\cdot g(x) = a(x)g(x)[a(x)g(x) + b(x)h(x)] =$

$= a^2(x)g^2(x) + a(x)g(x)h(x)b(x) =$

$0 \mod x^n + 1$

$= a^2(x)g^2(x)$

$\Rightarrow \quad e(x) = g(x)a(x)$ — идемпотенты.

Если $\neq$ не равен 0 или 1 то такой идемп. наз. собств-м.

Единств-й идемпотент идеала выполняет в нем роль единицы.

Т.к. $e(x)$ порожд. идеал (код) то любое слово может быть представ. в виде

$c(x) = \varphi(x)e(x)$

Умножим идемпотент на кодовое слово

т.е. $e(x)*c(x) = e^2(x)\cdot\varphi(x) = e(x)\cdot\varphi(x) = c(x)$

$\Rightarrow$ Идемпотент выполняет роль единицы

Каждому коду можем пост в соотв порожд. полином и порожд. идеал.

Сопряженный полином и дуальный код.

Пусть $h(x)$ — провер-й полином кода C, тогда

$h^*(x) = x^{\dim h(x)}\, h(x^{-1})$

— сопряж. полином.

Он явл. порожд-м для дуального кода $C_\perp$

Если B_1, B_2 и B_n идут тогда C, то B_1^{-1}, B_2^{-1} и B_n^{-1} это строки дуального $C_\perp$

Идемпотенты двоичных кодов.

Пусть F_{2^m} построим для него циклотомические классы, тогда идемпотент-ты идеала в соответ-м кольце многочленов явл. полиномы вида

$$e(x) = \sum_{s \in S} \cdot \sum_{i \in C_{n,s}} x^i$$

S - подмн. множ-ва представ-й циклот-х классов Π_n.

i - пробегает полностью циклот. классы из подмножества S

Пусть α образующий элемент поля F_{2^m} тогда $e(\alpha^0) = 0,1$

Пусть $j = 0,1,\dots,n-1$

Если $e(x)$ идемпотентен то $e(x)+1$ тоже, причем дополн. Кодов.

Рассмотрим полином $a(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$

Тогда обозначим

$$\overline{a}(x) = a_0 + a_{n-1} x + a_{n-2} x^2 + \dots + a_2 x^{n-2} + a_1 x^{n-1}$$

Если $e(x)$ идемпот-т то $\overline{e}(x)$ тоже.

Выражение $\overline{1 + e(x)}$ - идемп-т дуального кода.

С помощью идемп-та можно построить матрицу порождающую идеал (код

СТ — МА

$$\begin{pmatrix} e_{n-1} & e_{n-2} & \dots & e_1 & e_0 \\ e_0 & e_{n-1} & \dots & e_2 & e_1 \\ e_1 & e_0 & \dots & e_3 & e_2 \\ \hline e_{k-2} & e_{k-3} & \dots & e_k & e_{k-1} \end{pmatrix}$$

07.11.06.

Отображение кодов

Пусть дано поле F_{2^m} и $n = 2^m - 1$

Рассм-м числа $0, 1, 2, \dots, n-1$

Выберем из них число d т.ч.

$НОД(d, n) = 1$

Введем отображ числа

$\Theta_d = i^d \bmod n$

i – любое из данных чисел.

Применение данного отобр-я ко всей поля-ти набор-я чисел приводит к их перест-ке. Распространим данное отобр. на полиномы

$\Theta_d [a(x)] = a(x^d)$

$\Theta_d [a(x) + b(x)] = \Theta_d [a(x)] + \Theta_d [b(x)]$

$\Theta_d [a(x)\, b(x)] = \Theta_d [a(x)] \Theta_d [b(x)]$

св-ва

Если каждое слово кода C двоичного примитивной длины отображать Θ_d то получится тоже код

При этом идентичность исх. кода пресер-ся в идент. нового.

Отображение Θ_2 не нулев. циклотом. класса поля. Θ_2 не меняет идентичности кода. Если d нули двоичного кода прим. длины c, то d – нули кода $\Theta_d C$.

Пусть c дв. к. пр. дл – с порожд. полин. $e(x)$.

c' дополнит. код. $C_\perp$ – двойств. код

$C_\perp = \Theta_{-1} \cdot c'$

$e_\perp(x) = 1 + \Theta_{-1}\, e(x)$

Минимальные идеалы циклических кодов (поле F_2)

Пусть $\exists F_{2^m}$, $\exists \alpha \in F_{2^m}$

α - образующий элемент мультипликативной группы

$\alpha \in F_{2^m}^*$

$\alpha = \alpha^s$

Найдем циклотомический класс, в который входит s

Очевидно, что этот циклотомический класс определяется полиномом – тот для числа α возьмем в этом циклотомическом тот элемент, который является представителем этого класса: S_1

Полином $m_{S_1}(x)$.

Определим полином:

$$\hat{m}_{S_1}(x) = (x^n+1) / m_{S_1}(x)$$

Получ. полином – порождающий для тех идеала поля F_2

Найдем всех представителей циклотомических классов $S_1, S_2 \dots$

Найдем все образующие полиномы.

$m_{S_1}(x)$, $\hat{m}_{S_2}(x)$

$\Rightarrow$ получили все тех идеалы в кольце R_n над F_2

Найдем для каждого идеала его идемпотент.

Св-ва тех идеалов

Применив идемпотенты всего набора тех идеалов обр-ть ортогональ. систему т.е.

$$e_i \cdot e_j = 0, \quad i \neq j$$

Кольцо разложили в прямую сумму всех ненулевых идеалов.

Пусть $a \in R_n$, тогда a можно представить в виде лин. комбинации ненулевых идемпотентов.

$$a = a_1 e_1 + a_2 e_2 + \dots + a_k e_k$$

$a_1, a_2, \dots a_k$ – элементы поля в общем случае.

Идемпотенты образуют полную систему ортогональных.

$\exists e_i \otimes a \Rightarrow \underline{e_i a = a_i e_i}$

Образование новых кодов

Рассм. на примере 2 цикл. кодов C_1 и C_2 с порожд. полиномами $g_1(x), g_2(x)$ и с порожд. идемпот. $e_1(x), e_2(x)$.

1. Объединение кодов

$$C_\Sigma = C_1 + C_2$$

Если $c \in C$, то $\exists a_1 \in C_1, c_2 \in C_2 \Rightarrow$

$\Rightarrow \exists c = c_1 + c_2$, причем

$$g(x) = НОД[g_1(x), g_2(x)]$$

$$e(x) = e_1(x) + e_2(x) + e_1(x) e_2(x)$$

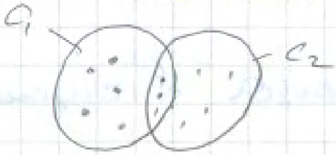
2. Пересечение кодов.

$$C = C_1 \cap C_2$$

Если $c \in C$, то $c \in C_1$ и $c \in C_2$

Порождающий $g(x) = НОК[g_1(x), g_2(x)]$
$g(x) = e_1(x) \cdot e_2(x)$

Рассм-м усл-но геом. интерпр. объед-ия (·) пересеч-е идемпотентных или идеалы, входящих в коды



Коды Рида – Соломона

∃ разн. опр-я РС кодов, кот. не всегда совпад-ся между собой.
Одни осн-ны на форм-м опр-ии кодов, другие на практике опер-ий с этими кодами =>
рассм. различ. опр-я, уст-м соотн-я дан. кодов с другими, опр-м св-ва этих кодов и с учетом этого дадим опр-е

Рассм. пр-во полиномов от 1й перем., степень кот-х $\le a$.
Пр-во имеет разм-ть $(a+1)$

Рассм-м все эл-ты поля F_{2^m} и в их уст-м порядке $b_1, b_2, \dots b_n$.
Рассм. отобр-е пр-ва полиномов в афин. пр-во F_{2^m} в виде

$(f(b_1), f(b_2) \dots f(b_n))$, $f(x)$ – полином из рассм. поле

Мн-во слов для $f(x)$ обр-т код. РС

Очевидно, что $k = a+1$, т.к. своб-й эл-т в полиноме не обяз-но $= 0$.
Коэф. полинома – блок инф-го сообщ-я, сост-й из k символов.

Кол-во 0 в код слове $\le$ степени пол-на
=> min код. расст-е $d = n - a$
=> код с пар-ми $[n, a+1, n-a]_q$
Проверим нер-во синглтона:
$n - k \ge d - 1$.

$n - k = n - a - 1$.
$d - 1 = n - a - 1$ => нер-во переходит в рав-во => код явл-ся кодом с максим. достиж. расст-ем (МДР) (код рода ноль).

Трактовка в терминах $[n,k,d]_q$ систем

Пусть полином $f(x)$ тожд. $= 0$ ∀ полиномов. => опр-м (·) a с коорд-ми
$x_1 = b_i$, $x_2 = b_i^2$, ... $x_a = b_i^a$

∀ всех b_i получаем n точек, кот-е обр-т $[n,k,d]_q$ систему.

Задавая различ. формы, преобр. (·), получаем все коорд. слова кода РС

Предположим, $f(x)$ содерж. не 0й своб-й член.
Вложим пр-во V^a в проектив. пр-во с коорд-ми $(1 : x_1 : x_2 : \dots : x_a)$ => получаем n (·) – принадлеж. в проектив. пр-ве, кот-е обр-т проектив-ю $[n,k,d]_q$ систему.
Задавая форму, получ. все коорд. слова РС.

Кодирование кодов РС

Составим таблицу из векторов столбцов, сост-х из коорд. $\beta^{(i)}$

$(1, \beta_i, \beta_i^2, \dots \beta_i^a)$

$\Rightarrow$ такая таблица будет ученик. маш-й преобр-я РМС.

Сост-м вектор строку из коэф. полинома $f(x)$, где слева – младший разряд

$\Rightarrow$ код-е кода РС свободен к перемен. $(f_0, f_1, \dots, f_a) \cdot$ (РМС маш-ное) $= (c_0, c_1, \dots c_n)$

Будем рассм-ть код-е на примере F_2^3

РМС маш-ка примет вид

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

↳ степени эл-в.

Каждая стр-ка – степень эл-та поля

Отличие этих эл-тов поля – по строку

Циклическое представ-е кода

Пост-м в соотв. код. слову полином

$c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1}$

Пусть $f(x) \equiv 1$ $\Rightarrow$ код-й полином имеет все единич. коэф-ты.

$l_i = 1$ $\Leftrightarrow$ полиному, соотв-му на $i^{\text{й}}$ строке РМС маш-и.

Пусть $f(x) = f_0 \neq 1$, $\Rightarrow$ все коэф. полин. $l_i = f_0$

Пусть $f(x) = x$ $\Rightarrow$ полином, соотв-й на коэф-х $d^{\text{й}}$ строки.

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

Если $f(x) = f_1(x)$ $\Rightarrow$ все коэф полинома надо $\otimes f_1$

Пусть $f(x) = f_0 + f_1 x^{\frac{1}{3}}$ $\Rightarrow$ код полином сост-ся как лин. комб-я 2^x 2^x строк

Убедимся далее, убедимся, что для произв-го сек. полинома код. слово сост-ся лин. комб. полинома, соотв-го на строках РМС маш-и

Структура полиномов-строк РМС маш-ны.

Ранее было уст-но, что полиномы, коэф-е на строках делят $(x^n + 1)$

Если a – обр-й эл-т коэф-в строки, то произв-й полином имеет вид

$a^{-1} \frac{x^n + 1}{x + a^{-1}} = \beta \frac{x^n + 1}{x + \beta}$, $\beta = a^{-1}$

След-но каждый полином получается на лин. ком-ции след. вида:

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

* — одночлены, отсутств. у разложения

Сопоставляя дан. таблицы удобно анализ. комбинаторн. стр-ру кода.

Пусть $a = 3$, тогда полином код. слова форм-ие лин-й комб-ей $1^х$ $4^х$ строк таблицы

=> НОК кажд. полинома $(x+2)(x+3)(x+1)$ => каждое код слово будет делиться на этот полином => получаемый код — циклический с образ-им полиномом $g(x) = (x+2)(x+3)(x+1)$

Минимальн-е идеалы — образующие кода.

Рассм. полиномы, постр. на строках ГМС мат-цы. Кажд. из них имеет макс. степень $(n-1)$ и делит полином x^n+1. Т.к. степень их максимальна, то дан. полиномы не делят ни какого другого полинома => эти полиномы порожд-т идеалы, в кот-х нет никаких других идеалов — min идеалы =>

=> каждое $g(x)$ кода имеет НОД нескольк. полиномов min идеалов. Мы ищем объедин-е кодов.

Примитивные идемпотенты

Рассм-м произв-й полином, постр. на строке ГМС мат-цы в виде

$$a^{n-1}x^{n-1} + a^{n-2}x^{n-2} + \dots a^2x^2 + ax + 1.$$

Возведем в квадрат этот полином. В поле F_2^m кв-т Σ = Σ кв-в, т.к. удвоен. произв-е = 0.

1 ост-ся без изменения, а ост-е мономы возв-ся в квадрат, причем степени x от 1 до $(n-1)/2$ при возведении в 2 дают все чет.-е степени. Все степени x от $(n+1)/2$ до $(n-1)$ при возвед-ии в степень должны привод-ся по мод-ю полинома по степени (x^n+1), т.е. $x^{n+k} = x^k$

=> получим все нечет. степени

$$(x^{n+1/2})^2 = x \dots x^{n-1} \cdot x^{n-2}$$

Рассм. коэф. при степенях x. Из исх. выр-я видно, что степени a такие же, что и у x. При этом как и для x необх. учит-ть соотн. $a^{n+k} = a^k$, т.к. $a^n = 1$.

=> при возвед-ии в кв-т полинома мономы просто перест-ся => кв-т полинома = самому полиному =>

=> Полиномы, постр-е на строках ГМС мат-ы явл. образ-ми пол. примит. обр-е мат-цы и являет идемпотентами.

=> идемпот-т рассм-го кода = Σ примитив. идемпотентов.

$e(x) = e_1(x) + e_2(x) + e_3(x) + e_4(x) =$

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

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

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

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

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

Из возведения в кв-т видно, что 1. явл-ся неизменной $\Rightarrow$ $e(x) + 1$ – идемпотент.

Из дан. примера видно, что Σ идемпотентов $\Rightarrow$ идемпот.

При рассм. компрес. кодов исходим из след. принципов: для дан. кода анализ. дуальн. код, кот-й доп-т св-ва прямого кода