Алгоритмы решения задач по Прикладной Алгебре для подготовке к Контрольной Работе

Затехано студентом третьего курса

ДИСКЛЕЙМЕР: Данный сборник был сделан *плохим* студентом, который не слушал лекций, не читал методичку (почти), а все (или почти все) алгоритмы понял (наверно) лишь из уже имеющихся решений. Используйте на свой страх и риск!

2021

Задание 1.1

Установить, является ли многочлен $Q_n(x)$ примитивным над $\mathbb{F}_k$.
Алгоритм
Рассмотрим $p = k^n - 1$, разложим его на простые множители (примарное разложение). Теперь распишем все значения $x^{\frac{p}{d}}$ через x^n, где d - каждый множитель примарного разложения, а x^n находится из $Q_n(x) = 0$. Если какое-то значение получилось равным 1, то элемент не примитивный.

Пример
Установить, является ли многочлен $x^3 + 2x^2 + 1$ примитивным над $\mathbb{F}_3$.

$p = 3^3 - 1 = 26 = 13 \cdot 2$
$Q_3(x) = 0 \Rightarrow x^3 = -2x^2 - 1 \equiv_3 x^2 + 2$

$x^{26/13=2} = x^2 \neq 1$

$x^{26/2=13} = x(x^3)^4 = x(x^2+2)^4 = x(xx^3 + 4x^2 + 4)^2 = x(x^3 + 2x + 4x^2 + 4)^2 = x(x^2 + 2 + 2x + 4x^2 + 4)^2 = x(5x^2 + 2x + 6)^2 = x(25xx^3 + 20x^3 + 64x^2 + 24x + 36) = x(25x^3 + 50x + 20x^2 + 40 + 64x^2 + 24x + 36) = x(25x^2 + 50x + 50x + 20x^2 + 40 + 64x^2 + 24x + 36) = x(109x^2 + 124x + 76) = 109x^3 + 123x^2 + 76x = 109x^2 + 218 + 123x^2 + 76x = 232x^2 + 76x + 218 \equiv_3 x^2 + x + 2 \neq 1$
Ответ: элемент примитивен

Задание 1.2

Для поля $\mathbb{F}_n^m = \mathbb{F}_n[x]/Q_m(x)$ найти все примитивные элементы.
Алгоритм
Посчитать $p = n^m - 1$, разложить на простые множители. Из $Q_m(x) = 0$ найти x_m. Составить таблицу степеней от x 1 до p, выразив их через x^m. Ответом будет те степени x, которые взаимно простые с p (не имеют общих делителей). Всего их должно быть $\phi(x)$, где $\phi(x)$ - функция Эйлера.

Пример
Для поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/(-x^4 + x + 1)$ найти все примитивные элементы.
$p = 2^4 - 1 = 15 = 3 \cdot 5$.
$x^4 = x + 1$
Ответом будут x в степенях 2, 3, 4, 7, 8, 11, 13, 14.

Задание 1.3

Найти все корни многочлена $f(x) \in \mathbb{F}_n[x]$ в поле $\mathbb{F}_n$.
Алгоритм
Элементы принадлежат мультипликативной группе поля, имеющей порядок n, поэтому для них $x^{n-1} = 1$. Все степени многочлена берутся с остатком по $n - 1$, дальше подставляем все значения из поля в многочлен, где 0 - то корень.

Пример
Найти все корни многочлена $f(x) = x^{467} + x^{457} - 2x^{329} + 2x^{311} + 2 \in \mathbb{F}_3[x]$ в поле $\mathbb{F}_3$.
$f(x) = x + x - 2x + 2x + 2 = 2(x + 1)$
$f(0) = 2 \neq 0; \;\; f(1) = 1 \neq 0$

$f(2) = f(-1) = 0$

Задание 1.4

В фактор-кольце $\mathbb{F}_k[x]/Q_m(x)$ найти все элементы главного идеала $f(x)$.

Алгоритм
Является ли $f(x)$ делителем $Q_m(x)$ в $\mathbb{F}_k$?
Если **да**, то искомый идеал составляет элементы кольца, кратные $f(x)$ степени $n = m - 1 - |f(x)|$ ($|f(x)|$ - степень многочлена $f(x)$): $\{f(x)(a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n) \mid a_i \in \mathbb{F}_k\}$.
Перебрав $a_i \in \mathbb{F}_k[x] \quad \forall i \in \overline{0,n}$ получим все элементы идеала.

Если **нет**, то земля пухом.

Пример
В фактор-кольце $\mathbb{F}_2[x]/(x^5 + x^4 + 1)$ найти все элементы главного идеала $(x^2 + x + 1)$.

$f(x) = x^2 + x + 1$ делит $Q_5(x) = x^5 + x^4 + 1$. Значит можно записать в виде выше со степенью $n = 5 - 1 - 2 = 2$: $\{(x^2 + x + 1)(a_0x^2 + a_1x + a_2) \mid a_i \in \mathbb{F}_2\}$.
$a_0x^4 + (a_0 + a_1)x^3 + (a_0 + a_1 + a_2)x^2 + (a_1 + a_)x + a_2$.
Всего будет восемь элементов.

Задание 1.5

Для поля $\mathbb{F}_n^m = \mathbb{F}_n[x]/Q_m(x)$ построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля. С помощью данной таблицы вычислить выражение $g(x)$
Алгоритм
Из $Q_m(x) = 0$ выделить $x^m = a_0x^{m-1} + \cdots + a_m,\ a_i \in \mathbb{F}_n$. Далее по количества ненулевых элементов равному $p = n^m - 1$ расписать степени α, где α - примитивный элемент (зачастую берут просто x):
$\alpha\ |x$
$\alpha^2|x^2 = x \cdot x$
$\alpha^3|x^3 = x \cdot x^2 = \ldots$
$\ldots$
$\alpha^m|a_0x^{m-1} + \cdots + a_m$
$\ldots$
$\alpha^p|1$

Все элементы привести к значениям $\mathbb{F}_n$. Проверкой на корректность будет $x^p = 1$. Далее для решения $g(x)$ надо просто подставить все найденные значения из таблицы, сократить все что можно и, опять воспользовавшись табличкой, записать ответ в малых степенях.
Если случилось так, что $x^k = 1$ $(k < p)$, то значит взятый α не является примитивным элементом и надо все пересчитывать (например, если x не примитивный, то можно попробовать $x + 1$).

Пример
Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(-2x^2 + x + 2)$ построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля. С помощью данной таблицы вычислить

выражение

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}$$

Переведем многочлен поля к константам этого поля $Q_m(x) = -2x^2 + x + 2 \equiv_3 x^2 + x + 2$. Все вычисления проводятся по модулю многочлена $Q_m(x) \Rightarrow x^2 = -x - 2 \equiv_3 2x + 1$. Всего в поле $\mathbb{F}_3^2$ находится $p = 3^2 - 1 = 8$ ненулевых элементов. Известно, что все ненулевые элементы поля могут быть представлены как $\alpha^i,\ i = 1, \ldots, 8$, где α - некоторый примитивный элемент поля. Возьмем в качестве α элемент x и вычислим все его с учетом x^2:

$$\begin{aligned}
&x^2 = 2x + 1,\\
&x^3 = x \cdot x^2 = x(2x+1) = 2x^2 + x = 2(2x+1) + x = 2x + 2,\\
&x^4 = x \cdot x^3 = x(2x+2) = 2x^2 + 2x = 2(2x+1) + 2x = 2,\\
&x^5 = x \cdot x^4 = 2x,\\
&x^6 = x \cdot x^5 = 2x^2 = 2(2x+1) = x + 2,\\
&x^7 = x \cdot x^6 = x(x+2) = x^2 + 2x = 2x + 1 + 2x = x + 1,\\
&x^8 = x \cdot x^7 = x(x+1) = x^2 + x = 2x + 1 + x = 1.
\end{aligned}$$

Последнее свойство $x^8 = 1$ следует из общих свойств поля и является проверкой на корректность проведенных вычислений. Теперь вычислим значения выражение:

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{x^8}{x^2} - \frac{(x^5)^7 x^4}{x^9 x^6} = x^6 - x^{35+4-9-6} = x^6 + 2x^{24} = \left\{x^{24} \equiv^8 x^0\right\} = x^6 + 2 = x + 2 + 2 = x + 1$$

Ответ: $x + 1$.

Задание 1.6

Найти порядок элемента $g(x)$ в поле $\mathbb{F}_n[x]/Q_m(x)$.

Алгоритм

Найти порядок, т.е. найти такое $\alpha : g(x)^\alpha = e$.

Из $Q_m(x) = 0$ получим запись вида $x^m = a_1 x^{m-1} + \cdots + a_m$, где все $a_i \in \mathbb{F}_n$.

Количество элементов мультипликативной группы - $n^m - 1$.

$g(x)^\alpha$ порождает подгруппу порядка α. Порядок подгруппы является делителем порядка группы. Поэтому порядком $g(x)$ будет один из множителей примарного (по простым) разложения $n^m - 1$. Если множитель входит в разложении в некоторой степени k, то нужно проверить все $\alpha \in p^q,\ q \in \overline{1, k}$.

Пример

Найти порядок элемента $2x + 1$ в поле $\mathbb{F}_3[x]/(x^2 + x + 2)$.

$Q_2(x) = x^2 + x + 2 = 0 \Rightarrow x^2 = -x - 2 \equiv_3 2x + 1$

Количество элементов: $3^2 - 1 = 8 = 2^3$.

$$(2x+1)^2 = 4x^2 + 4x + 1 \equiv_3 x^2 + x + 1 = \{x^2 = 2x + 1\} = 3x + 2 \equiv_3 2 \neq 1$$

$$(2x+1)^4 = ((2x+1)^2)^2 = (2)^2 = 4 \equiv_3 1 = 1$$

Ответ: порядок $2x + 1$ равен 4.

Задание 1.7

Имеется два поля $F_1 = \mathbb{F}_n[x]/Q_m(x)$ и $F_2 = \mathbb{F}_n[x]/P_m(x)$. Найти преобразование изоморфизма между ними.

Пример
Имеется два поля $F_1 = \mathbb{Q}_?[x]/(x^2 + 6x + 1)$ и $F_2 = \mathbb{Q}_?[x]/(x^2 - 14x + 31)$. Найти преобразование изоморфизма между ними.

Выделяя полные квадраты, имеем $(x+3)^2 - 8$ и $(y-7)^2 - 18$. При изоморфизме, x нужно перевести в линейное от y выражение $f(x) = ay + b$, чтобы оно удовлетворяло уравнению $(f(x) + 3)^2 = 8$.

Нам достаточно обеспечить условие $f(x) = 2\sqrt{2} - 3$ (пока на уровне эвристики), где $y = 3\sqrt{2} + 7$. Получается $\sqrt{2} = \frac{13}{y-7}$, откуда $f(x) = \frac{23}{y} - \frac{23}{3}$.

Теперь то же самое на формальном уровне: правило $x \mapsto \frac{2y-23}{3}$ индуцирует гомоморфизм кольца многочленов $\mathbb{Q}[x]$ во второе поле (это на самом деле поле, так как порождающий главного идеала неприводим над полем рациональных чисел). Очевидно, что перед нами сюръекция. Найдём ядро. Прямая проверка показывает, что многочлен $(x+3)^2 - 8$ принадлежит ядру – выражение именно из таких соображений и подбиралось. Действительно, $f((x+3)^2-8) = (f(x)+3)^2-8 = 49(y-7)^2-8 = 0$ во втором факторкольце.

Осталось показать, что ядро совпадает с главным идеалом многочлена $(x + 3)^2 - 8$. Это даёт изоморфизм, с учётом теоремы о гомоморфизмах. Рассматривая произвольный элемент ядра, заменяем его остатком от деления на многочлен второй степени. Получается $cx + d$, что должно переходить в ноль после замены. Тогда $c = 0$, чтобы коэффициент при y стал нулевым, и далее $d = 0$, так как константы переходят в себя.

Задание 2.1

Найти $f \in \mathbb{F}_n[x]$, удовлетворяющий уравнению

$$g(x) \cdot f(x) \equiv w(x) \bmod h(x)$$

.
Алгоритм

1. Из $h(x)$ выделить наибольшую степень x^k ($x^k = x^k - A^{-1}h(x)$, A – коэф. при x^k в $h(x)$).
2. Преобразовать $g(x)$ в $\hat{g}(x)$, подставив туда выделенную степень x из $h(x)$.
3. Найти обратный элемент $b(x)$ по инициализации:
   $r_{-2}(x) = h(x)$
   $r_{-1}(x) = \hat{g}(x)$
   $y_{-2} = 0$
   $y_{-1} = 1$
4. $\hat{f}(x) = w(x)b(x)$.
5. Финальный ответ $f(x)$ — это $\hat{f}(x)$, где $x^m,\ m \geq k$ заменены через x^k (см п.1).

Пример
Найти $f \in \mathbb{F}_7[x]$, удовлетворяющий уравнению

$$(2x^3 + 6x^2 + 4x + 5) \cdot f(x) \equiv 5x + 4 \bmod 6x^3 + x^2 + 3$$

1. Из $6x^3 + x^2 + 3$ находим, что $x^3 = x^2 + 3$.
2. Сокращаем степень $g(x) = 2x^3 + 6x^2 + 4x + 5 = 2x^2 + 6 + 6x^2 + 4x + 5 = x^2 + 4x + 4$.
3. Находим обратный элемент к $g(x)$ по $h(x)$:
   #0
   $r_{-2}(x) = 6x^3 + x^2 + 3$
   $r_{-1}(x) = x^2 + 4x + 4$
   $y_{-2} = 0$
   $y_{-1} = 1$

   #1
   $r_{-2}(x) = r_{-1}q_0 + r_0$
   $r_0 = 5x + 4$
   $q_0 = 6x + 5$
   $y_0 = y_{-2} - y_{-1}q_0 = -6x - 5 = x + 2$

   #2
   $r_{-1}(x) = r_0q_1 + r_1$
   $r_1 = 2$
   $q_1 = 3x + 4$
   $y_1 = y_{-1} - y_0q_1 = 1 - (x + 2)(3x + 4) = 4x^2 + 4x$

   Отсюда обратный элемент — $b(x) = r_1^{-1}y_1 = \{2^{-1} = 4\} = 4(4x^2 + 4x) = 2x^2 + 2x$.
4. $\hat{f}(x) = w(x)b(x) = (5x + 4)(2x^2 + 2x) = 3x^3 + 4x^2 + x$.
5. $f(x) = \{x^3 = x^2 + 3\} = 3x^2 + 9 + 4x^2 + x = x + 2$.

Ответ: $f(x) = x + 2$.

Задание 2.2

В поле $\mathbb{F}_n[x]/Q_m(x)$ найти обратный элемент для $g(x)$.
Алгоритм
Решается расширенным алгоритмом Евклида:
Вид - $Q_m(x)a(x) + g(x)b(x) = 1$. Нас интересует $b(x)$.

Шаг 0 (инициализация).
$r_{-2}(x) = Q_m(x)$
$r_{-1}(x) = g(x)$
$y_{-2}(x) = 0$
$y_{-1}(x) = 1$

Шаг 1.
$r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$ Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x)$

Шаг 2.
$r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$ Делим $r_{-1}(x)$ на $r_0(x)$ с остатком
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x)$

Шаг ...

Так продолжается, пока очередной остаток r_i не станет равен многочлену нулевой степени (т.е. константе - $r_i = C$). Ответом будет $b(x) = C^{-1}y_i(x)$.
Чтобы проверить правильность решения можно проверить выполняется ли соотношение $b(x)g(x) \equiv_n 1$.

Пример
В поле $\mathbb{F}_5[x]/(x^4 + x^3 - 5x^2 + x + 3)$ найти обратный элемент для $x^2 + 4x + 2$.

Шаг 0 (инициализация).
$r_{-2}(x) = x^4 + x^3 - 5x^2 + x + 3$
$r_{-1}(x) = x^2 + 4x + 2$
$y_{-2}(x) = 0$
$y_{-1}(x) = 1$

Шаг 1.
$r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$ Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком
$q_0(x) = x^2 - 3x$
$r_0(x) = 2x + 3$
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -x^2 + 3x$

Шаг 2.
$r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$ Делим $r_{-1}(x)$ на $r_0(x)$ с остатком
$q_1(x) = 3x$
$r_1(x) = 2$. (Константа, значит стоп)
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) = 3x^3 + x^2 + 1$

Ответ: $b(x) = 2^{-1}y_1(x) = 3y_1(x) = 4x^3 + 3x^2 + 3$.

Задание 3.1

В поле $\mathbb{F}_n^m = \mathbb{F}_n[x]/Q_m(x)$ найти обратную для матрицы

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Алгоритм

$$M^{-1} = (ad - bc)^{-1} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Пример

В поле $\mathbb{F}_5^2 = \mathbb{F}_5[x]/(x^2+3x+3)$ найти обратную для матрицы

$$M = \begin{bmatrix} 3x+4 & x+2 \\ x+3 & 3x+2 \end{bmatrix}$$

Сначала вычислим определитель заданной матрицы с учетом $x^2 = 2x+2$:
$g(x) = (3x+4)(3x+2) - (x+2)(x+3) = 4x^2+3x+3-x^2-1 = 3x^2+3x+2 = 3(2x+2)3x+2 = 4x+3.$

Теперь найдем обратный элемент $g(x)$ по $Q_2(x)$, решив уравнение Безу

$$(x^2+3x+3)a(x) + (4x+3)b(x) = 1$$

с помощью расширенного алгоритмом Евклида:
#0
$r_{-2}(x) = x^2+3x+3$
$r_{-1}(x) = 4x+3$
$y_{-2} = 0$
$y_{-1} = 1$

#1
$r_{-2}(x) = r_{-1}q_0 + r_0$
$r_0 = 1$
$q_0 = 4x+4$
$y_0 = y_{-2} - y_{-1}q_0 = -4x-4 = x+1$

Отсюда $b(x) = x+1$ — обратный элемент к $g(x)$. Теперь вычислим обратную матрицу:

$$\begin{bmatrix} 3x+4 & x+2 \\ x+3 & 3x+2 \end{bmatrix}^{-1} = (x+1)\begin{bmatrix} 3x+4 & x+2 \\ x+3 & 3x+2 \end{bmatrix} = \begin{bmatrix} x+3 & 1 \\ 4x & 3x \end{bmatrix}$$

В конце убедимся в правильности проведенных вычислений непосредственной проверкой:

$$M \cdot M^{-1} = \begin{bmatrix} 3x+4 & x+2 \\ x+3 & 3x+2 \end{bmatrix}\begin{bmatrix} x+3 & 1 \\ 4x & 3x \end{bmatrix} = \begin{bmatrix} (3x+4)(x+3)+4x(x+2) & 3x+4+3x(x+2) \\ (x+3)^2+4x(3x+2) & x+3+3x(3x+2) \end{bmatrix} =$$
$$= \begin{bmatrix} 2x^2+x+2 & 3x^2+4x+4 \\ 3x^2+4x+4 & 4x^2+2x+3 \end{bmatrix} = \begin{bmatrix} 2(2x+2)+x+2 & 3(2x+2)+4x+4 \\ 3(2x+2)+4x+4 & 4(2x+2)+2x+3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \equiv I^{2\times 2}$$

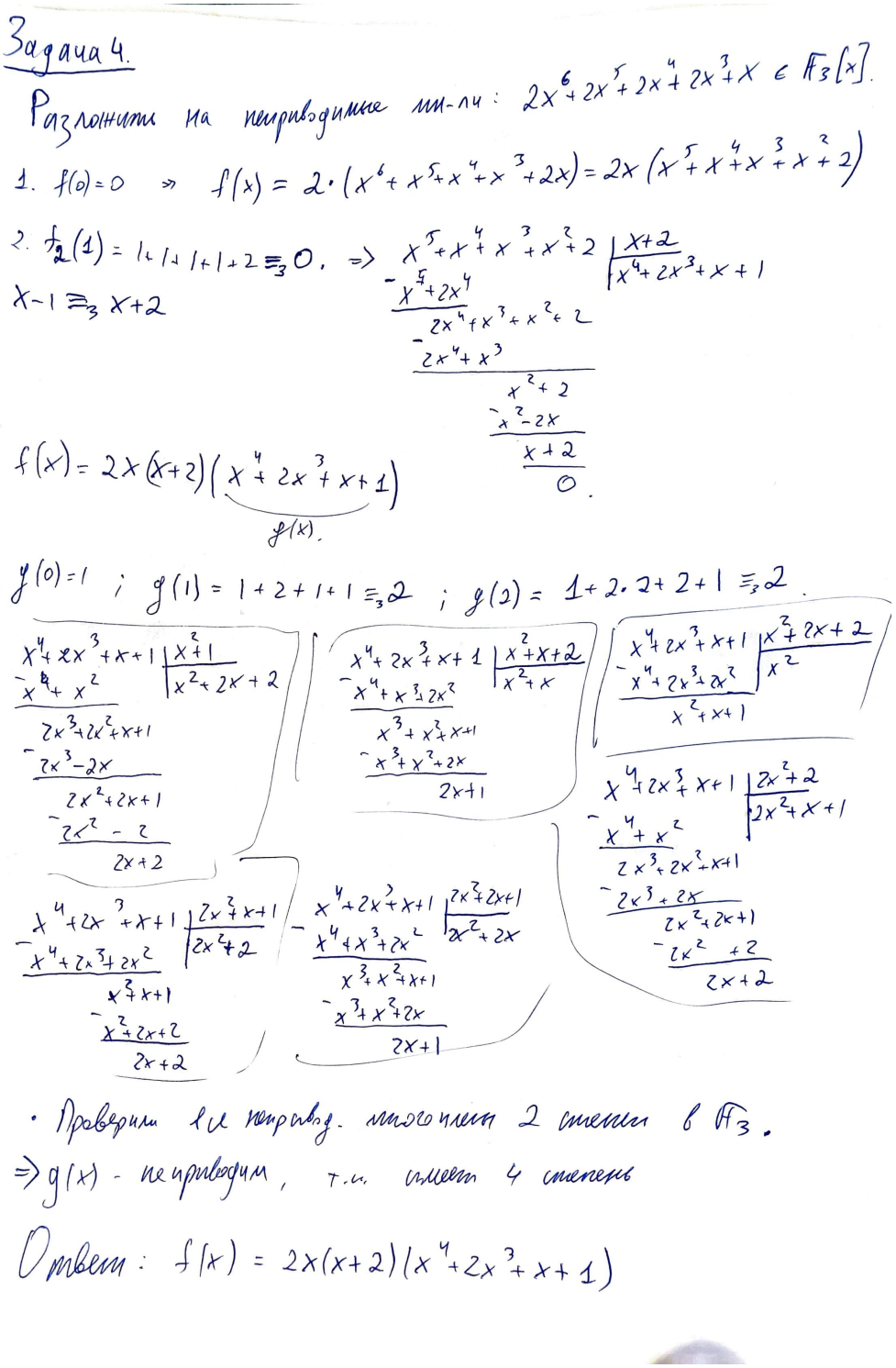
Задание 3.2

В поле $\mathbb{F}_n^m = \mathbb{F}_n[x]/Q_m(x)$ решить следующую СЛАУ:

$$\begin{aligned} \mathrm{m}_{00}a + m_{01}b &= s_0, \\ \mathrm{m}_{10}a + m_{11}b &= s_1. \end{aligned}$$

Алгоритм
$M \cdot \begin{bmatrix} a \\ b \end{bmatrix} = s \quad \Rightarrow \quad M^{-1} \cdot M \cdot \begin{bmatrix} a \\ b \end{bmatrix} = M^{-1} \cdot s \quad \Rightarrow \quad \begin{bmatrix} a \\ b \end{bmatrix} = M^{-1} \cdot s$
Таким образом достаточно просто найти обратную матрицу к M и домножить на s.

Пример



Задание 4.1

Найти общее количество неприводимых нормированных многочленов степени k над полем $\mathbb{F}_n$
Алгоритм
Найти примарное разложение k. Количество вычисляется через функцию Мебиуса $\mu(p)$.

- Она равна 1, если примарное разложение p, состоит из четного числа различных простых
- Она равна -1, если примарное разложение p, состоит из нечетного числа различных простых
- 0, если p не свободно от квадратов (т.е. какое-то просто число входит в разложение в квадрате).

- 1, если $p = 1$

$$\begin{array}{lll} \mu(1) = 1, & \mu(5) = -1, & \mu(9) = 0, \\ \mu(2) = -1, & \mu(6) = 1, & \mu(10) = 1, \\ \mu(3) = -1, & \mu(7) = -1, & \mu(11) = -1, \\ \mu(4) = 0, & \mu(8) = 0, & \mu(12) = 0, \end{array}$$

Итоговое число равно $\frac{1}{k}\sum_{d|k}\mu(d)n^{\frac{k}{d}}$, где $d|k$ значит, что d пробегает по всем множителям примарного разложения $\cup\ \{1\}$ k.

Пример
Найти общее количество неприводимых нормированных многочленов степени 8 над полем $\mathbb{F}_5$.
$k = 8 \Rightarrow d|8 = \{1, 2, 4, 8\}$. Количество элементов будет:
$\frac{1}{8}(1 \cdot 5^8 - 1 \cdot 5^4 + 0 + 0)$

Ответ: $\frac{5^4}{8}(5^4 - 1)$

Задание 4.2

Для многочлена $Q_m(x) \in \mathbb{F}_n[x]$ определить количество и степени неприводимых множителей. В каком минимальном поле расширения $\mathbb{F}_n$ данный многочлен раскладывается на линейные множители?

Пример
Аналогично 4.3, только ещё и кол-во указать.

Задание 4.3

Разложить на неприводимые множители многочлен

$$Q_m(x) \in \mathbb{F}_n[x]$$

Алгоритм
Найти корни (если они есть), подставив значения из $\mathbb{F}_n$. Поделить на них, по табличке неприводимых множителей.

Пример
Калькулятор многочленов

6. *Разложить на неприводимые множители многочлен* $f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.

Сначала пытаемся найти корни $f(x)$ в $\mathbb{F}_2$:

$$\begin{aligned} f(0) &= 1, \\ f(1) &= 1. \end{aligned}$$

Значит, $f(x)$ не имеет корней в $\mathbb{F}_2$, т.е. не имеет линейных множителей в своём разложении над $\mathbb{F}_2$. Далее пытаемся найти неприводимые многочлены степени 2, являющиеся делителями $f(x)$. Над $\mathbb{F}_2$ существует только один неприводимый многочлен степени 2: $x^2 + x + 1$. При делении $f(x)$ на $x^2 + x + 1$, получаем

$$f(x) = (x^2 + x + 1)(x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1).$$

Продолжая делить дальше на $x^2 + x + 1$, получаем

$$x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = (x^2 + x + 1)(x^7 + x^4 + x^3 + x^2 + x + 1) + x.$$

Неприводимых многочленов степени 3 над $\mathbb{F}_2$ всего два: $x^3 + x + 1$ и $x^3 + x^2 + 1$. Пробуем поделить на $x^3 + x + 1$:

$$x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1).$$

Производя деления далее на многочлены третьей степени, получаем

$$\begin{aligned} x^6 + x^5 + x^3 + x^2 + 1 &= (x^3 + x + 1)(x^3 + x^2 + x + 1) + x^2, \\ x^6 + x^5 + x^3 + x^2 + 1 &= (x^3 + x^2 + 1)x^3 + x^2 + 1. \end{aligned}$$

Так как многочлен 6-ой степени $x^6 + x^5 + x^3 + x^2 + 1$ не имеет делителей 3-ей и меньших степеней, то он является неприводимым (если бы он имел делитель, скажем, степени 4, то у него был бы и делитель степени 6-4=2). В итоге $f(x)$ раскладывается как

$$f(x) = (x^2 + x + 1)(x^3 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1).$$

Задание 4.4

Рассмотрим произвольный циклический код длины n. Требуется найти возможные значения для количества полезных бит k и проверочных бит m такого кода.

Алгоритм

1. Рассмотреть бином $x^n - 1$ и найти его структуру разложения над $\mathbb{F}_2$.
2. Разбить на орбиты элементы $\mathbb{Z}_n$ при умножении на 2, т.е. на такие множества, что $z_2 = (2z_1 \mod n)$, $z_3 = (2z_2 \mod n)$, $\ldots$, $z_1 = (2z_{k-1} \mod n)$. Другими словами на группы циклов $2\mathbb{Z}_n$.
3. Получив p орбит длин $l_1, \ldots, l_p$ имеем, что бином раскладывается на произведение k различных неприводимых многочленов l_i степеней. (Длина орбиты — кол-во элементов в ней)
4. Отсюда следует, что p наборов m и k (некоторые из которых, возможно, повторяются, если длины некоторых орбит совпадают) определяются как $m = l_i,\ k = n - l_i,\ i = \overline{1, p}$.

Ответ: все уникальные наборы m и k из п.4.

Пример

Рассмотрим произвольный циклический код длины $n = 5$. Требуется найти возможные значения для количества полезных бит k и проверочных бит m такого кода.

Рассмотрим бином $x^5 - 1$, найдем структуру его разложения над $\mathbb{F}_2$. Относительно умножения на 2 элементы $\mathbb{Z}_5$ делятся на орбиты: $\{0\}, \{1, 2, 4, 3\}$.
Значит бином раскладывается на произведение неприводимых многочленов одного 1-ой и одного 4-ой степени.

Тогда $\begin{matrix} \mathrm{m} = 4, & \mathrm{k} = \mathrm{n} - \mathrm{m} = 1 \\ \mathrm{m} = 1, & \mathrm{k} = \mathrm{n} - \mathrm{m} = 4 \end{matrix}$

Ответ: $m = 4, k = 1;\ m = 1, k = 4$

Задание 4.5

Для многочлена $x^m - 1 \in \mathbb{F}_n[x]$ определить количество и степени неприводимых множителей. В каком минимальном поле расширения $\mathbb{F}_n$ данный многочлен раскладывается на линейные множители?

Пример

№4 $x^{40}-1 \in F_5[x]$

$p=5 \Rightarrow \forall a, b \in F_5 \quad (a+b)^5 = a^5+b^5$

Тогда $f(x) = x^{40}-1 = (x^8-1)^5$

$g(x) = x^8-1$

$g(0) = -1$

$g(1)=g(2)=g(3)=g(4)=0$, т.е. $\forall x \in F_5 \quad x^{5-1}=x^4=1$

Итак, $x^8-1 \mid x+1$

x^8+x^7

$-x^7-1$

$-x^7-x^6$

$-x^6-1$

$-x^6-x^5$

$-x^5-1$

$-x^5-x^4$

$-x^4-1$

$-x^4-x^3$

$-x^3-1$

$-x^3-x^2$

$-x^2-1$

$-x^2-x$

$-x-1$

$-x-1$

0

$x^8-1 \mid x-1$

$x^8-x^7 \quad | \; x^7+x^6+x^5+x^4+x^3+x^2+x+1$

x^7-1

$\dots$

$x-1$

$x-1$

0

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

$x^7+x^6 \quad | \; x^6+x^4+x^2+1$

x^5+x^4

x^5+x^4

x^3+x^2

x^3+x^2

$x+1$

$x+1$

0

$x^6+x^4+x^2+2 \mid x-2$

$x^6-2x^5 \quad | \; x^5+2x^4+x+2$

$2x^5+x^4$

$2x^5-4x^4$

$-x^2+2$

x^2-2x

$-2x+2$

$2x-4$

0

$x^5+2x^4+x+2 \mid x+2$

$x^5+2x^4 \quad | \; x^4+2$

$x+2$

$x+2$

0

$g(x) = (x-2)(x-2)(x+1)(x+2)(x^4+1)$

$z(x)$

$z(0)=1$

$z(1)=z(2)=z(3)=z(4)=2 \Rightarrow$ нет делителей среди $GF(5^2)$

Среди $GF(5^2)$ неприводимый многочлен только один: $a(x) = x^2+x+2$

см. след. стр

стр. 6

№4 (продолжение)

проверим неприводимый многочлен $a(x) = x^2+2$

$$\begin{array}{r|l} x^4+2 & x^2+2 \\ \hline -(x^4+2x^2) & x^2+3 \\ \hline 3x^2+1 & \\ -(3x^2+6) & \\ \hline 0 & \end{array}$$

наименьшая степень неприводимых делителей = 2 ⇒ минимальное поле — F_5^2

Итак, $f(x) = (x+1)^5(x+2)^5(x+3)^5(x+4)^5(x^2+2)^5(x^2+3)^5$

Ответ: 4 неприводимых многочленов ~~простых~~ степени 1

4 неприводимых многочленов степени 1 и кратности 5 каждый, и 2 неприводимых многочлена степени 2 и кратности 5 каждый

Минимальное поле ~~расширения~~, в котором $f(x)$ раскладывается на линейные множители — F_5^2

стр. 7

Задание 5.1

Найти минимальное поле характеристики n, в котором многочлен $Q_m(x) \in \mathbb{F}_n[x]$ раскладывается на линейные множители. В данном поле найти все корни этого многочлена.

Алгоритм

1. Найти все корни $Q_m(x)$ в $F_n[x]$ (возможно многой кратности).
2. Разложить $Q_m(x)$ на множители по найденным корням $f(x) = (x - X_1(x)) \dots (x - X_k(x))P_s(x)$, здесь $P_s(x)$ - оставшаяся часть, многочлен степени s. К тому же $P_s(x)$ является неприводимым в $F_n[x]$.
3. В расширение поля $\mathbb{F}_n^s = \mathbb{F}_n/P_s(x)$ многочлен $P_s(x)$ можно разложить на s линейных множителей $P_s(x) = (x - \alpha)(x - \alpha^n)(x - \alpha^{n^2}) \dots (x - \alpha^{n^{s-1}})$
4. Из $0 = P_s(\alpha)$ найти α^s и расписать все степени α от 1 до n^{s-1} через него.
5. Расписать разложение $P_s(x)$ в расширении поля как в п.3, использовав найденные степени α.

Ответ: все корни $Q_m(x)$ (если корень кратный, его стоит повторить столько раз, какая у него кратность), найденные в п.1 и все корни из разложения п.5, где вместо α нужно подставить x.

Пример
На следующей странице (это пример из методички, стр. 229).

2.28. Найти поле характеристики 3, в котором многочлен $f(x) = x^3 + x + 2 \in \mathbb{F}_3[x]$ раскладывается на линейные множители и найти в нём все корни данного многочлена.

Решение. 1. Найдём разложение многочлена $f(x)$ на *неприводимые* множители над $\mathbb{F}_3$.

- Ищем корни: $f(0) = 2,\ f(1) = 1,\ f(2) = 0.$
  Поскольку $x - 2 \equiv_3 x + 1$, то
  $f(x) = (x + 1)\left(x^2 + 2x + 2\right).$
- Многочлен $g(x) = x^2 + 2x + 2$ не имеет корней в $\mathbb{F}_3$, его степень 2, т. е. он неприводим.
- Окончательно: $f(x) = (x + 1)\left(x^2 + 2x + 2\right).$

2. Известно, что если $g(x)$ — неприводимый многочлен степени n над $\mathbb{F}_p$, то он:

- в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей —

$$g(x) = (x-\alpha)\cdot(x-\alpha^p)\cdot\left(x-\alpha^{p^2}\right)\cdot\ldots\cdot\left(x-\alpha^{p^{n-1}}\right),$$

  где α – произвольный корень $g(x)$ в F;
- не имеет корней ни в каком конечном поле, содержащим менее, чем p^n элементов.

3. Рассмотрим поле $\mathbb{F}_3[x]/(g(x))$ расширения многочлена $g(x) = x^2 + 2x + 2$.

В этом поле если α — корень $g(x)$, то и α^3 — тоже его корень. Вычисляем:

$$\begin{aligned}\alpha^2 &= -2\alpha - 2 = \alpha + 1,\\ \alpha^3 &= \alpha(\alpha+1) = \alpha^2 + \alpha = 2\alpha + 1\end{aligned}$$

Построенное поле $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right)$ содержит найденный ранее корень 2, поэтому многочлен $f(x)$ в этом поле раскладывается на следующие линейные множители:

$$f(x) = x^3 + x + 2 = (x-2)(x-\alpha)(x-2\alpha-1) = (x+1)(x+2\alpha)(x+\alpha+2).$$

4. Определить корни многочлена

$$g(x) = (x-\alpha)(x-2\alpha-1)$$

в поле $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right)$ легко: всегда можно взять $\alpha = x$, откуда второй корень $\alpha^3 = 2\alpha + 1 = 2x + 1$.

Ответ: многочлен $f(x) = x^3 + x + 2$ имеет корни 2, x, $2x + 1$ в поле $\mathbb{F}_3[x]/\left(x^2 + 2x + 2\right) = GF(3^2)$.

Задание 5.2

Найти минимальный многочлен $m(x) \in \mathbb{F}_n[x]$, который имеет корень α^k, где α - примитивный элемент поля $\mathbb{F}_n^m = \mathbb{F}_n[x]/Q_m(x)$.

Пример

8. *Найти минимальный многочлен* $m(x) \in \mathbb{F}_5[x]$, *который имеет корень* α^3, *где* α – *примитивный элемент поля* $\mathbb{F}_5^2 = \mathbb{F}_5[x]/(x^2+x+2)$.

Известно, что минимальный многочлен $m(x)$ в поле $\mathbb{F}_5^2$ содержит вместе с корнем α^3 все смежные с ним $(\alpha^3)^5, (\alpha^3)^{5^2}, \ldots$. С учётом $\alpha^{5^2-1} = \alpha^{24} = 1$ получаем, что смежный класс, образованный α^3, содержит только два элемента α^3 и α^{15}. Следовательно, минимальный многочлен имеет степень 2 и может быть представлен как

$$m(x) = (x-\alpha^3)(x-\alpha^{15}) = x^2 - (\alpha^3+\alpha^{15})x + \alpha^{18}.$$

Найдём коэффициенты многочлена с учётом $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}
\alpha^3 &= \alpha \cdot \alpha^2 = \alpha(4\alpha+3) = 4\alpha^2 + 3\alpha = 4(4\alpha+3) + 3\alpha = 4\alpha + 2, \\
\alpha^{15} &= (\alpha^3)^5 = (4\alpha+2)^5 = 4\alpha^5 + 2 = 4\alpha^2\alpha^3 + 2 = 4(4\alpha+3)(4\alpha+2) + 2 = \\
&= 4(\alpha^2+1) + 2 = 4(4\alpha+4) + 2 = \alpha + 3, \\
\alpha^3 + \alpha^{15} &= 4\alpha + 2 + \alpha + 3 = 0, \\
\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha+2)(\alpha+3) = 4(4\alpha+3) + 4\alpha + 1 = 3.
\end{aligned}$$

Заметим, что в полном соответствии с теорией значения коэффициентов $m(x)$ получились из $\mathbb{F}_5$. В итоге

$$m(x) = x^2 + 3.$$

Задание 6.1

Циклический (m, n)-код задан свои порождающим полиномом $g(x)$. Требуется определить минимальное расстояние кода d, а также осуществить систематическое кодирование полинома $u(x)$.

Алгоритм

Переводим код длины n в код длины m. Кодовое расстояние вычисляется перебором всех значений полинома $v(x) = g(x) \cdot Q_n(x)$. Раскрываем скобки и строим табличку для всевозможных значений коэффициентов многочлена в множестве $\{0, 1\}$. В каждой ненулевой строке считаем количество единиц, затем выбираем наименьшее получившееся значение - это будет кодовое расстояние d.

Для кодирования полинома $u(x)$ нужно домножить его на x^k (k - степень $g(x)$) и поделить на $g(x)$. Получившийся остаток $r(x)$ добавить делимому. То есть кодированием полинома будет $u(x) \cdot x^k + r(x)$.

Пример

Циклический (7, 3)-код задан свои порождающим полиномом $g(x) = x^4 + x^3 + x^2 + 1$. Требуется определить минимальное расстояние кода d, а также осуществить систематическое кодирование полинома $u(x) = x^2 + 1$.

Задача 6.3.21 Код (7, 3) циклический.

Задан полиномом $g(x) = x^4 + x^3 + x^2 + 1$. Опр. кодовое расст. Полином закодировать $u(x) = x^2 + 1$.

Решение:

Код (7, 3): 7 символов в кодовых словах (Будем код. слова длины 3)
3 информационных символа.

Кодовое расстояние: ← т.к. 3 симв.

$$v(x) = g(x) \cdot (ax^2 + bx + c) = (x^4 + x^3 + x^2 + 1)(ax^2 + bx + c) =$$

$$= (ax^6 + bx^5 + cx^4) + (ax^5 + bx^4 + cx^3) + (ax^4 + bx^3 + cx^2) +$$

$$+ (ax^2 + bx + c) = ax^6 + (a+b)x^5 + (c+b+a)x^4 + (c+b)x^3 +$$

$$+ (c+a)x^2 + bx + c$$

a b c	0	1	2	3	4	5	6	N
0 0 1	1	0	1	1	1	0	0	4
0 1 0	0	1	0	1	1	1	0	4
0 1 1	1	1	1	0	1	1	0	4
1 0 0	0	0	1	0	1	1	1	4
1 0 1	1	0	0	1	0	1	1	4
1 1 0	0	1	1	1	0	0	1	4
1 1 1	1	1	0	0	1	0	1	4

$\Rightarrow \boxed{d = 4}$

Кодируем:

$u(x) \cdot x^4 = x^6 + x^4$

$v(x) = x + 1 + u(x)x^4 =$

$= x + 1 + x^6 + x^4$

$\boxed{1100101}$

$x^6 + x^4 \;|\; x^4 + x^3 + x^2 + 1$

$-(x^6 + x^5 + x^4 + x^2) \;|\; x^2 + x + 1$

$-x^5 + x^2$

$-(x^5 + x^4 + x^3 + x)$

$-x^4 + x^3 + x$

$-(x^4 + x^3 + x^2 + 1)$

$x + 1$

Задание 6.2

Линейный код задан своей проверочной матрицей $H^{n\times m}$ (n строк и m столбцов). Требуется построить порождающую матрицу кода G для систематического кодирования, при котором биты исходного сообщения переходят в последние биты кодового слова. Найти систематическое кодирование для векторов $u_1,\ u_2$.

Алгоритм

Разделяем матрицу H чертой на квадратную матрицу $n \times n$ и остаток. Изменяем матрицу линейными преобразованиями так, чтобы левая часть стала единичной матрицей. Выписываем отдельно правую часть размера $n \times (m-n)$. Теперь составляем матрицу G, разделенную горизонтально, где сверху правая часть H, а снизу единичная матрица размера $(m-n) \times (m-n)$.

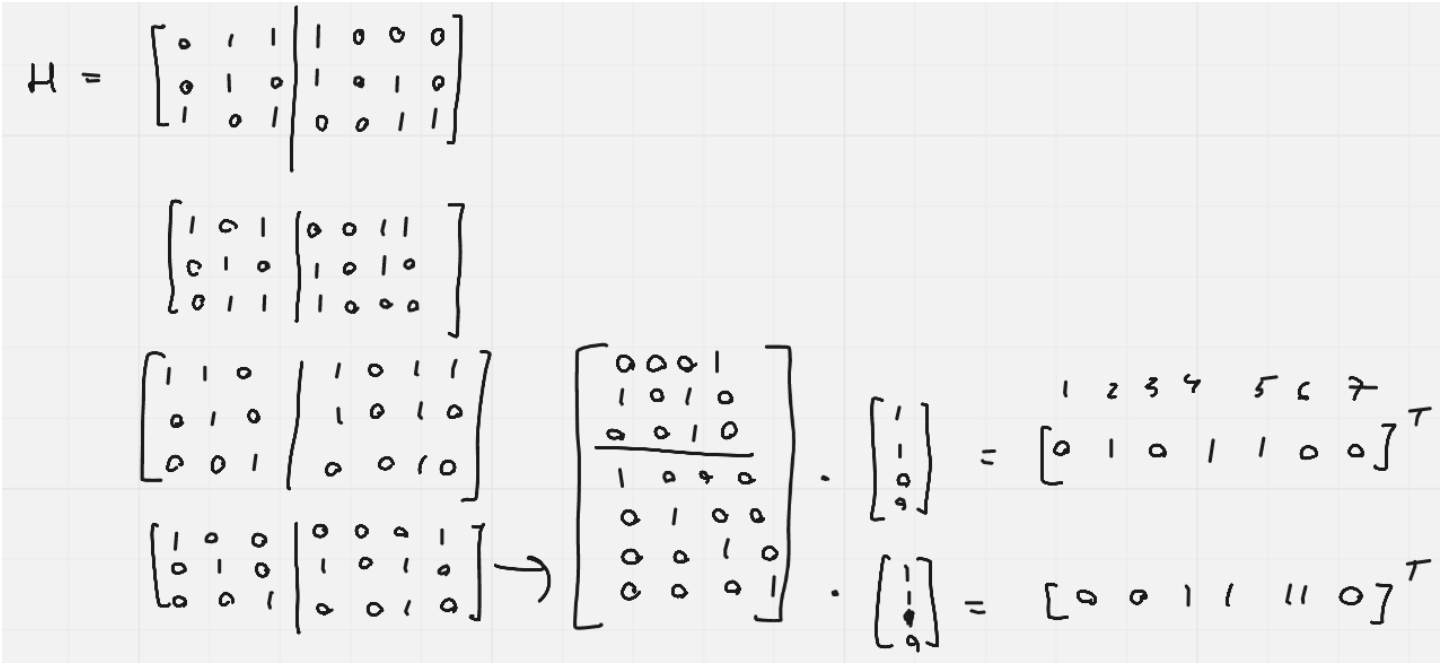
Теперь для нахождения кодирования u_1 и u_2 просто домножим каждый из них на полученную матрицу G слева.

Пример

Линейный код задан своей проверочной матрицей

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Требуется построить порождающую матрицу кода G для систематического кодирования, при котором биты исходного сообщения переходят в последние биты кодового слова. Найти систематическое кодирование для векторов $u_1 = [1\ 1\ 0\ 0]^T,\ u_2 = [1\ 1\ 1\ 0]^T$.



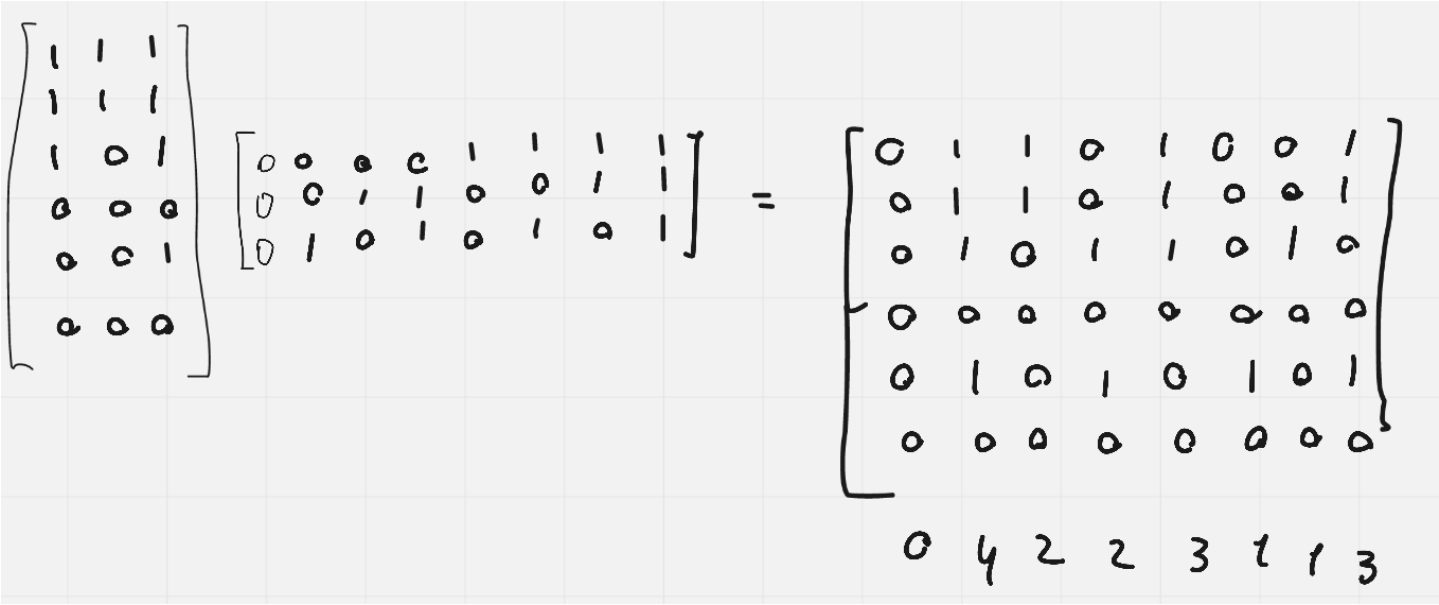
Задание 6.3

Линейный код задан своей порождающей матрицей G. Требуется определить минимальное расстояние кода d.

Пример
Линейный код задан своей порождающей матрицей

$$G = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Требуется определить минимальное расстояние кода d.
Ответ: $d = 1$



Задание 7.1

Рассмотрим код БЧХ с нулями $\alpha^i,\ i = 1, \ldots, 2r$, где α - примитивный элемент поля $\mathbb{F}_n[x]/Q_m(x)$. Требуется найти полином локаторов ошибок $\sigma(x)$ для принятого полинома $\omega(x)$

Алгоритм

1. Расписать все степени α от 1 до $p = n^m - 1$ через α^m, где α^m находится из $0 = Q_m(\alpha)$.
2. Расписать $2r$ синдромов $s_1, \ldots, s_{2r}$, где $s_i = \omega(\alpha^i)$. При этом $s_{2i} = s_i^2$ и $\alpha^z \equiv \alpha^{z \bmod p}$.
3. Записать синдромный полином $s(x) = 1 + \sum\limits_{i=1}^{2r} s_i x^i$
4. Решить соотношение Безу $x^{2r+1}a(x) + s(x)\sigma(x) = \lambda(x)$, $\deg\lambda(x) \leq r$ или другими словами — найти "обратный элемент"для $s(x)$ по x^{2r+1}, где последний шаг будет определятся тем, что порядок (deg) очередного остатка $\leq r$, а $y_z(x)$ не надо домножать на обратный элемент к остатку.

Ответ: $\sigma(x)$ есть найденный $y_z(x)$.

Пример

Рассмотрим код БЧХ с нулями $\alpha^i,\ i = 1, \ldots, 4$, где α – примитивный элемент поля $\mathbb{F}_2[x]/(x^4 + x + 1)$. Требуется найти полином локаторов ошибок $\sigma(x)$ для принятого полинома $w(x) = x^{14} + x^{10} + x^5 + x^4$.

Для удобства вычислений в поле $\mathbb{F}_2^4$ построим таблицу соответствий между степенным и полиномиальным представлением элементов поля:

α	α
α^2	α^2
α^3	α^3
α^4	$\alpha + 1$
α^5	$\alpha^2 + \alpha$
α^6	$\alpha^3 + \alpha^2$
α^7	$\alpha^3 + \alpha + 1$
α^8	$\alpha^2 + 1$
α^9	$\alpha^3 + \alpha$
α^{10}	$\alpha^2 + \alpha + 1$
α^{11}	$\alpha^3 + \alpha^2 + \alpha$
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$
α^{13}	$\alpha^3 + \alpha^2 + 1$
α^{14}	$\alpha^3 + 1$
α^{15}	1

С помощью этой таблицы вычислим синдромы:

$$\begin{aligned} s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \alpha^7, \\ s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\ s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\ s_4 &= w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{13}. \end{aligned}$$

В результате синдромный полином $s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1$. Синдромов всего четыре, следовательно, $t = 2$. Полином локаторов ошибок $\sigma(x)$ является решением уравнения

$$x^{2t+1}a(x) + s(x)\sigma(x) = \lambda(x),\ \deg\lambda(x) \leq t.$$

Решим данное уравнение с помощью расширенного алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^5$, // Инициализация
$r_{-1}(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1$,
$y_{-2}(x) = 0$,
$y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$, // Делим с остатком $r_{-2}(x)$ на $r_{-1}(x)$
$q_0(x) = \alpha^2 x$,
$r_0(x) = \alpha x^3 + \alpha^9 x^2 + \alpha^2 x$,
$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = \alpha^2 x$.

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$, // Делим с остатком $r_{-1}(x)$ на $r_0(x)$
$q_1(x) = \alpha^{12}x + \alpha^5$,
$r_1(x) = \alpha^{14}x^2 + 1$,
$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) = 1 + \alpha^2 x(\alpha^{12}x + \alpha^5) = \alpha^{14}x^2 + \alpha^7 x + 1$.

Таким образом, искомый полином локаторов ошибок $\sigma(x) = \alpha^{14}x^2 + \alpha^7 x + 1$.

Задание 7.2

Рассмотрим код БЧХ, нули которого определяются степенями α, где α - примитивный элемент поля $\mathbb{F}_n[x]/Q_m(x)$. Пусть для некоторого слова $\omega(x)$ полином локаторов ошибок $\sigma(x)$. Требуется определить позиции ошибок в $\omega(x)$.

Алгоритм

1. Расписать степени α от 1 до $p = n^m - 1$ через α^m, где α^m найдено из $0 = Q_m(\alpha)$.
2. Расписать таблицу соответствий локатора ошибок $\sigma(\alpha)$ для всех степеней α. Важно - $\sigma(x)$ является полиномом на полем, потому свойство $\sigma(\alpha^2) = (\sigma(\alpha))^2$ **не** выполняется.
3. Из этой таблицы найти корни полинома локатора ошибок — такие $\alpha^{k_i} \ : \ \sigma(\alpha^{k_i}) = 0$.
4. Полином ошибок будет следующего вида $e(x) = \sum\limits_i x^{p-k_i}$. Ошибки в разрядах $w(x)$ будут совпадать со степенями x из полинома ошибок $e(x)$.

Пример

12. *Рассмотрим код БЧХ, нули которого определяются степенями α, где α – примитивный элемент поля $\mathbb{F}_2[x]/(x^4 + x + 1)$. Пусть для некоторого принятого слова $w(x)$ полином локаторов ошибок $\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1$. Требуется определить позиции ошибок в $w(x)$.*

Найдём корни полинома локаторов ошибок полным перебором. Для вычислений будем пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов поля, вычисленной выше:

$$
\begin{aligned}
\sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 = \alpha^3 + 1,\\
\sigma(\alpha^2) &= \alpha^6 + \alpha^8 + 1 = \alpha^3,\\
\sigma(\alpha^3) &= \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha,\\
\sigma(\alpha^4) &= \alpha^{10} + \alpha^{10} + 1 = 1,\\
\sigma(\alpha^5) &= \alpha^{12} + \alpha^{11} + 1 = 0,\\
\sigma(\alpha^6) &= \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1,\\
\sigma(\alpha^7) &= \alpha + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1,\\
\sigma(\alpha^8) &= \alpha^3 + \alpha^{14} + 1 = 0,\\
\sigma(\alpha^9) &= \alpha^5 + 1 + 1 = \alpha^2 + \alpha,\\
\sigma(\alpha^{10}) &= \alpha^7 + \alpha + 1 = \alpha^3,\\
\sigma(\alpha^{11}) &= \alpha^9 + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,\\
\sigma(\alpha^{12}) &= \alpha^{11} + \alpha^3 + 1 = \alpha^2 + \alpha + 1,\\
\sigma(\alpha^{13}) &= \alpha^{13} + \alpha^4 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,\\
\sigma(\alpha^{14}) &= 1 + \alpha^5 + 1 = \alpha^2 + \alpha,\\
\sigma(\alpha^{15}) &= \alpha^2 + \alpha^6 + 1 = \alpha^3 + 1.
\end{aligned}
$$

Заметим, что полином локаторов ошибок $\sigma(x)$ является полиномом над полем $\mathbb{F}_2^4$. Поэтому здесь не выполняется свойство $\sigma(\alpha^2) = (\sigma(\alpha))^2$. Обратные элементы для обнаруженных корней α^5 и α^8 равны, соответственно, α^{10} и α^7. Отсюда получаем, что полином ошибок $e(x) = x^{10} + x^7$.

Задание 7.3

Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_n[x]/Q_m(x)$. Требуется декодировать полученный полином $\omega(x)$.

Алгоритм

1. Из $0 = Q_m(\alpha)$ выделить α^m.
2. Расписать все степени α от 1 до $p = n^m - 1$ через α^m.
3. Расписать $\omega(\alpha)$ через полученные степени α из таблицы, обозначим его за $s(\alpha)$.
4. Расписанный полином $s(\alpha)$ преобразовать обратно в одну из степеней α из таблички (если не получается, значит один из пунктов выше сделан неверно).
5. Найти такой полином ошибок $e(x) = x^k$, что $e(\alpha) = s(\alpha)$.

Ответ: $\omega(x) + e(x)$.

Пример
Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_2[x]/(x^3 + x^2 + 1)$. Требуется декодировать полученный полином $\omega(x) = x^3 + x$.

11. *Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом* $\alpha \in \mathbb{F}_2[x]/(x^3 + x + 1)$. *Требуется декодировать полученный полином* $w(x) = x^7 + x^6 + x^2 + 1$.

Вычислим синдром с учётом $\alpha^3 = \alpha + 1$:

$$s = w(\alpha) = \alpha^7 + \alpha^6 + \alpha^2 + 1 = \alpha(\alpha^3)^2 + (\alpha^3)^2 + \alpha^2 + 1 =$$
$$= \alpha(\alpha+1)^2 + (\alpha+1)^2 + \alpha^2 + 1 = \alpha(\alpha^2+1) + \alpha^2 + 1 + \alpha^2 + 1 = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1.$$

Далее необходимо найти полином ошибок вида $e(x) = x^k$ такой, что $e(\alpha) = s$, т.е. найти k: $\alpha^k = 1$. Очевидно, что $k = 0$. Следовательно, $\hat{v}(x) = w(x) + e(x) = x^7 + x^6 + x^2$.