Дмитрий Герасимов (4538)
Теория кодирования

Задание 5

14 декабря 2013 г.

Задача 1

- $q = 3$; $x^3 + 1 = (x + 1)(x^2 + x + 1)$, то есть существует 3 различных (невырожденных в пустой) циклических кода:

  1. $p(x) = 1$, тривиальный $(3, 3)$-код, скорость 1, минимальное расстояние 1
  2. $p(x) = x + 1$, $(3, 2)$-код, скорость $\frac{2}{3}$, минимальное расстояние 2
  3. $p(x) = x^2 + x + 1$, тривиальный $(3, 1)$-код, скорость $\frac{1}{3}$, минимальное расстояние 3

- $q = 4$; $x^4 + 1 = (x + 1)^4$, 4 различных (невырожденных в пустой) циклических кода:

  1. $p(x) = 1$, тривиальный $(4, 4)$-код, скорость 1, минимальное расстояние 1
  2. $p(x) = x + 1$, $(4, 3)$-код, скорость $\frac{3}{4}$, минимальное расстояние 2
  3. $p(x) = (x + 1)^2 = x^2 + 1$, $(4, 2)$-код, скорость $\frac{1}{2}$, минимальное расстояние 2
  4. $p(x) = (x + 1)^3 = x^3 + x^2 + x + 1$, тривиальный $(4, 1)$-код, скорость $\frac{1}{4}$, минимальное расстояние 4

- $q = 5$; $x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$, 3 различных невырожденных циклических кода

  1. $p(x) = 1$, тривиальный $(5, 5)$-код, скорость 1, минимальное расстояние 1
  2. $p(x) = x + 1$, $(5, 4)$-код, скорость $\frac{4}{5}$, минимальное расстояние 2
  3. $p(x) = x^4 + x^3 + x^2 + x + 1$, $(5, 1)$-код, скорость $\frac{1}{5}$, минимальное расстояние 5

- $q = 6$; $x^6 + 1 = (x + 1)^2 * (x^2 + x + 1)^2$, 8 различных невырожденных циклических кодов

  1. $p(x) = 1$, тривиальный $(6, 6)$-код, скорость 1, минимальное расстояние 1
  2. $p(x) = x + 1$, $(6, 5)$-код, скорость $\frac{5}{6}$, минимальное расстояние 2
  3. $p(x) = (x + 1)^2 = x^2 + 1$, $(6, 4)$-код, скорость $\frac{2}{3}$, минимальное расстояние 2
  4. $p(x) = x^2 + x + 1$, $(6, 4)$-код, скорость $\frac{2}{3}$, минимальное расстояние 2
  5. $p(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1$, $(6, 2)$-код, скорость $\frac{1}{3}$, минимальное расстояние 3
  6. $p(x) = (x + 1)(x^2 + x + 1) = x^3 + 1$, $(6, 3)$-код, скорость $\frac{1}{2}$, минимальное расстояние 2
  7. $p(x) = (x+1)^2(x^2+x+1) = x^4+x^3+x+1$, $(6, 2)$-код, скорость $\frac{1}{3}$, минимальное расстояние 2
  8. $p(x) = (x+1)(x^2+x+1)^2 = x^5+x^4+x^3+x^2+x+1$, тривиальный $(6, 1)$-код, скорость $\frac{1}{6}$, минимальное расстояние 6

- $q = 7$; $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$, 7 различных невырожденных циклических кодов

1. $p(x) = 1$, тривиальный $(7, 7)$-код, скорость 1, минимальное расстояние 1
2. $p(x) = x + 1$, $(7, 6)$-код, скорость $\frac{6}{7}$, минимальное расстояние 2
3. $p(x) = x^3 + x + 1$, $(7, 4)$-код (код Хэмминга), скорость $\frac{4}{7}$, минимальное расстояние 3
4. $p(x) = x^3 + x : 2 + 1$, $(7, 4)$-код (код Хэмминга), скорость $\frac{4}{7}$, минимальное расстояние 3
5. $p(x) = (x + 1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$, $(7, 3)$-код (дуальный коду Хэмминга), скорость $\frac{3}{7}$, минимальное расстояние 4
6. $p(x) = (x + 1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$, $(7, 3)$-код (дуальный коду Хэмминга), скорость $\frac{3}{7}$, минимальное расстояние 4
7. $p(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, тривиальный $(7, 1)$-код, минимальное расстояние 7

- $q = 8$; $x^8 + 1 = (x + 1)^8$, 8 различных (невырожденных в пустой) циклических кодов:

1. $p(x) = 1$, тривиальный $(8, 8)$-код, скорость 1, минимальное расстояние 1
2. $p(x) = x + 1$, $(8, 7)$-код, скорость $\frac{3}{4}$, минимальное расстояние 2
3. $p(x) = (x + 1)^2 = x^2 + 1$, $(8, 6)$-код, скорость $\frac{2}{3}$, минимальное расстояние 2
4. $p(x) = (x + 1)^3 = x^3 + x^2 + x + 1$, $(8, 5)$-код, скорость $\frac{5}{8}$, минимальное расстояние 2
5. $p(x) = (x + 1)^4 = x^4 + 1$, $(8, 4)$-код, скорость $\frac{1}{2}$, минимальное расстояние 2
6. $p(x) = (x + 1)^5 = x^5 + x^4 + x + 1$, $(8, 3)$-код, скорость $\frac{3}{8}$, минимальное расстояние 4
7. $p(x) = (x + 1)^6 = x^6 + x^4 + x^2 + 1$, $(8, 2)$-код, скорость $\frac{2}{3}$, минимальное расстояние 4
8. $p(x) = (x + 1)^7 = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, тривиальный $(8, 1)$-код, скорость $\frac{1}{8}$, минимальное расстояние 8

- $q = 9$; $x^9 + 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$, 7 различных (невырожденных в пустой) циклических кодов:

1. $p(x) = 1$, тривиальный $(9, 9)$-код, скорость 1, минимальное расстояние 1
2. $p(x) = x + 1$, $(9, 8)$-код, скорость $\frac{8}{9}$, минимальное расстояние 2
3. $p(x) = x^2 + x + 1$, $(9, 7)$-код, скорость $\frac{7}{9}$, минимальное расстояние 2
4. $p(x) = x^6 + x^3 + 1$, $(9, 3)$-код, скорость $\frac{1}{3}$, минимальное расстояние 3
5. $p(x) = (x + 1)(x^2 + x + 1) = x^3 + 1$, $(9, 6)$-код, скорость $\frac{2}{3}$, минимальное расстояние 2
6. $p(x) = (x + 1)(x^6 + x^3 + 1) = x^7 + x^6 + x^4 + x^3 + x + 1$, $(9, 2)$-код, скорость $\frac{2}{9}$, минимальное расстояние 6
7. $p(x) = (x^2 + x + 1)(x^6 + x^3 + 1) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, тривиальный $(9, 1)$-код, скорость $\frac{1}{9}$, минимальное расстояние 9

Задача 2

Рассмотрим возможные многочлены третьего порядка над $\mathbb{Z}_2$ и выберем из них неприводимые:

- x^3 — делится на x
- x^3+1 — делится на $x+1$
- x^3+x — делится на x
- x^3+x+1 — неприводимый
- x^3+x^2 — делится на x
- x^3+x^2+1 — неприводимый
- x^3+x^2+x — делится на x
- x^3+x^2+x+1 — делится на $x+1$

Таким образом, имеем два поля F_8^1, порожденное полиномом x^3+x+1 и F_8^2, порожденное x^3+x^2+1.

Заметим, что мультипликативные группы этих полей цикличны и порождаются степенями элемента x. Породим первое поле степенями x (по модулю x^3+x+1), а второе — степенями x^3 (по модулю x^3+x^2+1):

$x^1=x$	$x^2=x^2$	$x^3=x+1$	$x^4=x^2+x$	$x^5=x^2+x+1$	$x^6=x^2+1$	$x^7=1$
$x^3=x^2+1$	$x^6=x^2+x$	$x^9=x^2$	$x^{12}=x+1$	$x^{15}=x$	$x^{18}=x^2+x+1$	$x^{21}=1$

Обозначим за $o(e)$ минимальную степень, в которую надо возвести генератор g мультипликативной группы, чтобы получить e. Тогда можно записать операцию умножения элементов поля F_8 как: $a\cdot b = g^{o(a)}\cdot g^{o(b)} = g^{o(a)+o(b) \bmod 7}$. Для каждого из полей F_8^1 и F_8^2 будет своя функция o_1 и o_2 соответственно, в качестве функции изоморфизма f возьмем функцию, сопоставляющая элементу $e_1 \in F_8^1$ такой элемент $e_2 \in F_8^2$, что $o_1(e_1) = o_2(e_2)$, то есть будет выполняться $o_1(e_1) = o_2(f(e_1))$.

Докажем, что этот изоморфизм сохраняет операцию умножения:

$$f(a\cdot b) = f(x^{o_1(a)}\cdot x^{o_1(b)}) = f(x^{o_1(a)+o_1(b) \bmod 7})$$

При этом:

$$f(a)\cdot f(b) = (x^3)^{o_2(f(a))}\cdot (x^3)^{o_2(f(b))} = (x^3)^{o_2(f(a))+o_2(f(b)) \bmod 7} = (x^3)^{o_1(a)+o_1(b) \bmod 7}$$

Заметим, что

$$o_2(f(x^{o_1(a)+o_1(b) \bmod 7})) = o_1(x^{o_1(a)+o_1(b) \bmod 7})$$

, что по нашему определению f означает, что

$$f(x^{o_1(a)+o_1(b) \bmod 7}) = (x^3)^{o_1(a)+o_1(b) \bmod 7}$$

, что и требовалось доказать.

Изоморфизм аддитивной группы:

- сопоставим нулевому элементу нулевой
- $f(a+b) = f(x^{o_1(a)} + x^{o_1(b)})$, не теряя общности, пусть $o_1(a) \leq o_1(b)$, тогда

  $$f(x^{o_1(a)} + x^{o_1(b)}) = f(x^{o_1(a)} \cdot (1 + x^{o_1(b)-o_1(a)})) = f(x^{o_1(a)}) \cdot f(1 + x^{o_1(b)-o_1(a)})$$

  Проверим непосредственно, что изоморфизм сохраняется относительно прибавления единицы, и получим:

  $$f(x^{o_1(a)}) \cdot f(1+x^{o_1(b)-o_1(a)}) = f(x^{o_1(a)}) \cdot (1+f(x^{o_1(b)-o_1(a)})) = f(x^{o_1(a)}) + f(x^{o_1(a)}) \cdot f(x^{o_1(b)-o_1(a)})$$

  $$= f(x^{o_1(a)}) + f(x^{o_1(b)}) = f(a) + f(b)$$

  , что и требовалось доказать.

Задача 1 1-5

Задача 3

G_* — мультипликативная группа, в скобках указывается порядок элемента.

- $q = 2$: $G_* = \{1(1)\}$
- $q = 3$: $G_* = \{1(1), 2(2)\}$
- $q = 4 = 2^2$: полином $p(x) = x^2 + x + 1$, $G_* = \{1(1), x(3), x+1(3)\}$
- $q = 5$: $G_* = \{1(1), 2(4), 3(4), 4(2)\}$
- $q = 7$: $G_* = \{1(1), 2(3), 3(6), 4(3), 5(6), 6(2)\}$
- $q = 8 = 2^3$: полином $p(x) = x^3 + x + 1$, $G_* = \{1(1), x(7), x+1(7), x^2(7), x^2+1(7), x^2+x(7), x^2+x+1(7)\}$
- $q = 9 = 3^2$: полином $p(x) = x^2 + x + 2$, $G_* = \{1(1), 2, x(8), x+1(8), x+2(4), 2x(8), 2x+1(4), 2x+2(8)\}$

Задача 4

После того, как построили таблицу умножения (в приложении), обратный элемент для некого a можно найти как такое b, что на пересечении строки a и столбца b стоит единица.

x	x^{-1}
a	a^3+1
a^2	a^3+a^2+1
a^3	a^3+a^2+a+1
$a+1$	a^3+a^2+a
a^2+a	a^2+a+1
a^3+a^2	a^3+a
a^3+a+1	a^2+1
a^2+1	a^3+a+1
a^3+a	a^3+a^2
a^2+a+1	a^2+a
a^3+a^2+a	$a+1$
a^3+a^2+a+1	a^3
a^3+a^2+1	a^2
a^3+1	a
1	1

Задача 5

После того, как построили таблицу умножения (в приложении), обратный элемент для некого a можно найти как такое b, что на пересечении строки a и столбца b стоит единица.

x	x^{-1}
$a+1$	a^3+a
a^2+1	a^2+a
a^3+a^2+a+1	a
a^3+a^2+a	a^3+a+1
a^3+a^2+1	a^3+a^2
a^3	a^2
a^2+a+1	a^3+1
a^3+1	a^2+a+1
a^2	a^3
a^3+a^2	a^3+a^2+1
a^3+a+1	a^3+a^2+a
a	a^3+a^2+a+1
a^2+a	a^2+1
a^3+a	$a+1$
1	1

Задача 6

Породим код Хэмминга $(7, 4)$ полиномом $p(x) = x^3 + x + 1$, который является неразложимым делителем $x^7 + 1$.

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

, в систематической форме:

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

, проверочная матрица:

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