Дмитрий Герасимов (4538)
Теория кодирования **Задание 7** 31 декабря 2013 г.

Задача 1

Индивидуальное задание: вариант 5, последовательность $s = 100011001000$.

- Так как в последовательности присутствует три нуля подряд, если бы n было равно 3, то в какой-то момент состояние генератора было бы равно 000, и последовательность бы была нулевая.
- Рассмотрим $n = 4$:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

, из чего легко получить единственное решение $c_1 = 1, c_4 = 1, c_3 = 1, c_2 = 1$. Генератор с такими значениями порождает последовательность $s' = \mathbf{100011000}\ 110001$, что не совпадает с нашей последовательностью.

- Рассмотрим $n = 5$:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

, легко видеть, что эта система приводится к нижнетреугольному виду, из которого получаем единственное решение $c_5 = 0, c_4 = 0, c_3 = 0, c_2 = 1, c_1 = 1$. Такой генератор порождает последовательность $s' = 1001010111110000\ \mathbf{1000110010}\ 10111$, что не является подходящей для нас последовательностью.

- Рассмотрим $n = 6$:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

, приведем систему заменой строк на линейные комбинации и перестановкой строк к виду

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} c_1 \\ c_3 \\ c_2 \\ c_4 \\ c_5 \\ c_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

, из чего получаем $c_6 = 0, c_5 = 1, c_4 = 1, c_2 = 0, c_3 = 0, c_1 = 1$. Такой генератор порождает последовательность

$$s' = 100100000101110110101001111\ \mathbf{100011001000}\ 001011101101010011110011$$

Таким образом, следующие 10 символов последовательности: 0010111011.

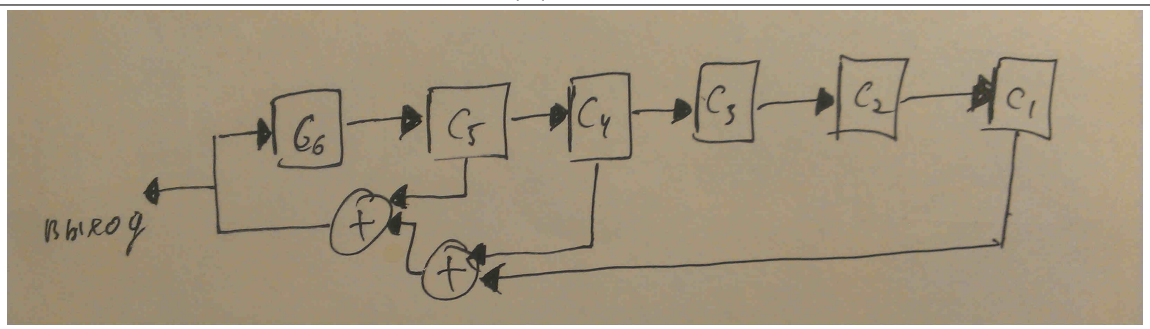

Рис. 1: Схема генератора к заданию 1.

Задача 2

Для получения РС-кода с конструктивным расстоянием d можно просто взять произвольный b и порождающий полином $g(x) = \prod_{i=b}^{b+d-2}(x - \alpha^i)$. Таким образом, будет существовать:

- 1 код с $k = n$ и конструктивным расстоянием 1 (тривиальный)
- n кодов с $k = n - 1$ и конструктивным расстоянием 2
- n кодов с $k = n - 2$ и конструктивным расстоянием 3
- ...
- n кодов с $k = 1$ и конструктивным расстоянием n
- 1 код с $k = 0$ (вырожденный)

Рассмотрим теперь пример РС-кода над $GF(7)$ с конструктивным расстоянием 5 (исправляющего две ошибки). В качестве генератора мультипликативной группы возьмем $\alpha = 3$, тогда:

$$g(x) = (x - \alpha^1)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) = (x - 3)(x - 2)(x - 6)(x - 4) = 4 + 2x + 3x^2 + 6x^3 + x^4$$

$$G = \begin{bmatrix} 4 & 2 & 3 & 6 & 1 & 0 \\ 0 & 4 & 2 & 3 & 6 & 1 \end{bmatrix}$$

Пусть при передаче информационной последовательности $m = 00$, которой соответствует кодовое слово $c = 000000$, произошла ошибка $e = 503000$, и было получено $v = c + e = 503000$.

- Декодируем по алгоритму ПГЦ:
  1. Кодовое слово $c(x) = 0$
  2. Выход канала $v(x) = 5 + 3x^2$
  3. Синдромный многочлен $S(x) = 4x + 3x^2 + x^3 + 4x^4$
  4. Система уравнений для коэффициентов многочлена локаторов ошибок:
     $\begin{pmatrix} 4 & 3 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} \Lambda_2 \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} 6 \\ 3 \end{pmatrix}$
     , из которой получим полином локаторов ошибок $\Lambda(x) = 1 + 4x + 2x^2$

5. Корнями полинома локаторов ошибок являются $x = 4$ и $x = 1$, локаторы ошибок — 2 и 1 как обратные к корням элементы. Эти элементы имеют степени 2 и 0 соответственно, что действительно является позициями ошибок.

6. система уравнений для значений ошибок:
$$\begin{pmatrix} 2 & 1 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$$
, из которой получим $Y_1 = 3, Y_2 = 5$, что действительно является значениями ошибок на позициях 2 и 0 соответственно. Таким образом, вектор ошибок действительно равен $e(x) = 3x^2 + 5$, после вычитания его из $v(x)$, получим кодовое слово, которое отправляли.

- Рассчитаем полином локаторов ошибок по алгоритму БМ:

r	Δ	$B(x)$	$\Lambda(x)$	L
1	4	2	$3x + 1$	1
2	1	$2x$	$x + 1$	1
3	4	$2x + 2$	$6x^2 + x + 1$	2
4	2	$2x^2 + 2x$	$2x^2 + 4x + 1$	2

Многочлен локаторов ошибок $\Lambda(x) = 1 + 4x + 2x^2$, что совпадает с многочленом, рассчитанным по алгоритму ПГЦ.

Найдем значения ошибок по алгоритму Форни:

$\Omega(x) = S(x)\Lambda(x) \mod x^2 = 5x+4$; $\Lambda'(x) = 4x+4$, из чего по формуле $Y_i = \frac{-\Omega(X_i^{-1})}{\Lambda'(X_i^{-1})}$ получаем $Y_1 = 3, Y_2 = 5$, что совпадает с значениями ошибок, рассчитанными по алгоритму ПГЦ.

Задача 3

Код Рида-Соломона длины 7 должен быть построен над полем $GF(2^3)$, для его построения построим его как поле полиномов по модулю $p(x) = x^3 + x + 1$:

Степень	Элемент
0	1
1	a
2	a^2
3	$a + 1$
4	$a^2 + a$
5	$a^2 + a + 1$
6	$a^2 + 1$

Чтобы код исправлял двойные ошибки, необходимо хотя бы $d = 5$, возьмем в качестве порождающего многочлена $g(x) = (x - a^1)(x - a^2)(x - a^3)(x - a^4) = a^3 + ax + x^2 + a^3x^3 + x^4$. Получили код с конструктивным расстоянием 5 и $k = 3$.

Пусть при передаче информационной последовательности $m = 000$, которой соответствует кодовое слово $c = 0000000$, произошла ошибка $e = 00a^3a^2000$, и было получено $v = c+e = 00a^3a^2000$.

- Декодируем по алгоритму ПГЦ:

1. Кодовое слово $c(x) = 0$
2. Выход канала $v(x) = a^3x^2 + a^2x^3$
3. Синдромный многочлен $S(x) = a^3x^2 + ax^3 + a^5x^4$

4. Система уравнений для коэффициентов многочлена локаторов ошибок:
$$\begin{pmatrix} 0 & a^3 \\ a^3 & a \end{pmatrix} \begin{pmatrix} \Lambda_2 \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} a \\ a^5 \end{pmatrix}$$
, из которой получим полином локаторов ошибок $\Lambda(x) = 1 + a^5 x + a^5 x^2$

5. Корнями полинома локаторов ошибок являются $x = a^4$ и $x = a^5$, локаторы ошибок — a^3 и a^2 как обратные к корням элементы. Эти элементы имеют степени 3 и 2 соответственно, что действительно является позициями ошибок.

6. система уравнений для значений ошибок:
$$\begin{pmatrix} a^3 & a^2 \\ a^6 & a^4 \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} 0 \\ a^3 \end{pmatrix}$$
, из которой получим $Y_1 = a^2, Y_2 = a^3$, что действительно является значениями ошибок на позициях 3 и 2 соответственно. Таким образом, вектор ошибок действительно равен $e(x) = a^3x^2 + a^2x^3$, после вычитания его из $v(x)$, получим кодовое слово, которое отправляли.

- Рассчитаем полином локаторов ошибок по алгоритму БМ:

r	Δ	$B(x)$	$\Lambda(x)$	L
r	Δ	$\Lambda(x)$	L	
1	0	x	1	0
2	$a+1$	a^2+a	$(a+1)\,x^2+1$	2
3	a	$(a^2+a)\,x$	$(a+1)\,x^2+(a^2+a+1)\,x+1$	2
4	a^2+a+1	$(a^2+a)\,x^2$	$(a^2+a+1)\,x^2+(a^2+a+1)\,x+1$	2

Многочлен локаторов ошибок $\Lambda(x) = 1 + a^5x + a^5x^2$, что совпадает с многочленом, рассчитанным по алгоритму ПГЦ.

Найдем значения ошибок по алгоритму Форни:

$\Omega(x) = S(x)\Lambda(x) \mod x^4 = (a+1)\,x$; $\Lambda'(x) = a^2 + a + 1$, из чего по формуле $Y_i = \frac{-\Omega(X_i^{-1})}{\Lambda'(X_i^{-1})}$ получаем $Y_1 = a^2, Y_2 = a + 1 = a^3$, что совпадает с значениями ошибок, рассчитанными по алгоритму ПГЦ.

Задача 6

Индивидуальное задание: вариант 5

Примитивный полином 73: $p(x) = 1 + t + t^2 + 0 + t^4 + t^5$

Выход канала 4602671437: $v(x) = x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{22} + x^{21} + x^{18} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x^5 + x^4 + x$

Циклическое представление мультипликативной группы поля:

Степень	Элемент
0	1
1	a
2	a^2
3	a^3
4	a^4
5	$a^4 + a^2 + a + 1$
6	$a^4 + a^3 + 1$
7	$a^2 + 1$
8	$a^3 + a$
9	$a^4 + a^2$
10	$a^4 + a^3 + a^2 + a + 1$
11	$a^3 + 1$
12	$a^4 + a$
13	$a^4 + a + 1$
14	$a^4 + 1$
15	$a^4 + a^2 + 1$
16	$a^4 + a^3 + a^2 + 1$
17	$a^3 + a^2 + 1$
18	$a^4 + a^3 + a$
19	$a + 1$
20	$a^2 + a$
21	$a^3 + a^2$
22	$a^4 + a^3$
23	$a^2 + a + 1$
24	$a^3 + a^2 + a$
25	$a^4 + a^3 + a^2$
26	$a^3 + a^2 + a + 1$
27	$a^4 + a^3 + a^2 + a$
28	$a^3 + a + 1$
29	$a^4 + a^2 + a$
30	$a^4 + a^3 + a + 1$

- Декодируем по алгоритму ПГЦ:

  1. Синдромный многочлен $S(x) = (a^4 + a^3 + a + 1)\,x^4 + (a^2 + a + 1)\,x^3 + (a^4 + a^2 + 1)\,x^2 + (a^2 + a + 1)\,x$
  2. Система уравнений для коэффициентов многочлена локаторов ошибок:
     $$\begin{pmatrix} a^2 + a + 1 & a^4 + a^2 + 1 \\ a^4 + a^2 + 1 & a^2 + a + 1 \end{pmatrix} \begin{pmatrix} \Lambda_2 \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} a^2 + a + 1 \\ a^4 + a^3 + a + 1 \end{pmatrix}$$
     , из которой получим полином локаторов ошибок $\Lambda(x) = (a^4 + a^2)x^2 + (a^2 + a + 1)x + 1$
  3. Корнями полинома локаторов ошибок являются $x = a^3 + a^2 + a + 1$ и $x = a^4 + a^3 + a^2 + a$, локаторы ошибок — $a^4 + a^2 + a + 1$ и a^4 как обратные к корням элементы. Эти элементы имеют степени 5 и 4 соответственно, что является позициями ошибок.
  4. система уравнений для значений ошибок:
     $$\begin{pmatrix} a^4 + a^2 + a + 1 & a^4 \\ a^4 + a^3 + a^2 + a + 1 & a^3 + a \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} a^2 + a + 1 \\ a^4 + a^2 + 1 \end{pmatrix}$$
     , из которой получим $Y_1 = 1, Y_2 = 1$, что является значениями ошибок на позициях 5 и 4 соответственно. Таким образом, вектор ошибок равен $e(x) = x^5 + x^4$, после

вычитания его из $v(x)$, получим кодовое слово $c(x) = x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{22} + x^{21} + x^{18} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x$

5. разделив кодовое слово на порождающий многочлен $g(x) = x^4 + (a^4 + a^3 + a^2 + a)\,x^3 + a^2x^2 + ax + a^4 + a^3 + a^2 + a + 1$, получим информационный многочлен $m(x) = x^{26} + (a^4 + a^3 + a^2 + a + 1)\,x^{25} + (a^4 + a^3 + a^2)\,x^{24} + (a^4 + a^3 + a^2 + 1)\,x^{23} + (a^4 + a^3 + a + 1)\,x^{22} + (a^4 + a^3 + a^2)\,x^{21} + (a^4 + a + 1)\,x^{20} + a^2x^{19} + (a^4 + a^3 + 1)\,x^{18} + (a^4 + a^2)\,x^{17} + (a^4 + a)\,x^{16} + (a^4 + a^2)\,x^{15} + (a^2 + 1)\,x^{14} + a^4x^{13} + (a^4 + a + 1)\,x^{12} + a^2x^{11} + (a^4 + a^3)\,x^{10} + (a^3 + a + 1)\,x^9 + (a^3 + a^2 + a + 1)\,x^8 + (a^4 + a^2 + a + 1)\,x^7 + (a^4 + a^3 + a^2 + 1)\,x^6 + (a^3 + a^2)\,x^5 + (a^4 + a^3 + 1)\,x^4 + (a^4 + a^3 + a + 1)\,x^3 + (a^4 + a)\,x^2 + (a^3 + a^2)\,x$, причем остаток от деления равен 0, как и должно быть.

- Рассчитаем полином локаторов ошибок по алгоритму БМ:

r	Δ	$B(x)$	$\Lambda(x)$	L
1	$a^2 + a + 1$	$a^3 + a$	$(a^2 + a + 1)\,x + 1$	1
2	0	$(a^3 + a)\,x$	$(a^2 + a + 1)\,x + 1$	1
3	a	$(a^4 + a^3)\,x + a^4 + a^3 + a + 1$	$(a^4 + a^2)\,x^2 + (a^2 + a + 1)\,x + 1$	2
4	0	$(a^4 + a^3)\,x^2 + (a^4 + a^3 + a + 1)\,x$	$(a^4 + a^2)\,x^2 + (a^2 + a + 1)\,x + 1$	2

Многочлен локаторов ошибок $\Lambda(x) = (a^4 + a^2)\,x^2 + (a^2 + a + 1)\,x + 1$, что совпадает с многочленом, рассчитанным по алгоритму ПГЦ.

Найдем значения ошибок по алгоритму Форни:

$\Omega(x) = S(x)\Lambda(x) \mod x^4 = a^2 + a + 1$; $\Lambda'(x) = a^2 + a + 1$, из чего по формуле $Y_i = \frac{-\Omega(X_i^{-1})}{\Lambda'(X_i^{-1})}$ получаем $Y_1 = 1, Y_2 = 1$, что совпадает с значениями ошибок, рассчитанными по алгоритму ПГЦ.