

Циклический код Хэмминга

Примитивный полином

- Пусть $p(x)$ - примитивный полином над $GF(2)$ степени m .
- Наименьшее значение n такое, что
 - $p(x) \mid (x^n - 1)$
- равно $n = 2^m - 1$.
- Циклический код, формируемый $p(x)$ имеет длину кодового слова равной
 - $n = 2^m - 1$.

Проверочная матрица

- Проверочная матрица H с элементами вида
 - $x^i \bmod p(x)$
 - Имеет различные ненулевые столбцы, следовательно код может исправлять все одиночные ошибки.
 - Столбцы H определяются через элементы поля, как степени порождающего элемента поля $\alpha = x$ в $GF(2^m)$:
 - $H = [1 \ \alpha \ \alpha^2 \ \dots \ \alpha^{n-2} \ \alpha^{n-1}]$

Синдром

- Предположим, что одиночная ошибка расположена на позиции i , т. е., $e(x) = x^i$. Синдром вычисляется как :
- $S_1 = y(\alpha) = y_0 + y_1\alpha + \dots + y_{n-1}\alpha^{n-1}$
- $= c(\alpha) + e(\alpha) = e(\alpha) = \alpha^i$.
- Декодер определяет местоположение ошибки i по синдрому $S_1 = \alpha^i$ после вычисления дискретного логарифма по основанию α .

Циклический небинарный код Хэмминга

- Циклический небинарный код Хэмминга определяется через элемент $GF(q^m)$ порядка

- $$n = (q^m - 1)/(q - 1).$$

Проверочная матрица и порождающий полином

- Проверочная матрица

- $$H = [1 \ \beta \ \beta^2 \ \dots \ \beta^{n-1}],$$

- Порождающий полином $g(x)$ является минимальным полиномом над $GF(q)$

- $$\deg g(x) = m$$

Условие существования

- Столбцы H являются ЛН над $GF(q)$ если и только если $\beta^j / \beta^i = \beta^l$ не принадлежит $GF(q)$.
- Циклический код Хэмминга длины n существует только в том случае, если n и $q - 1$ взаимно простые, что справедливо, если t и $q - 1$ взаимно простые.

Пример

- Если $q = 3$ тогда $q - 1 = 2$, следовательно m должно быть нечетным.
- Пусть $GF(3^3)$ определяется через примитивный полином
- $x^3 + 2x + 1$, и $\beta = \alpha^2$.

$$H = [1 \ \alpha^2 \ \alpha^4 \ \dots \ \alpha^{22} \ \alpha^{24}] = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 0 & 2 & 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 0 & 1 & 0 & 2 & 2 & 2 & 1 & 2 & 2 \\ 0 & 1 & 1 & 1 & 2 & 1 & 1 & 0 & 0 & 1 & 2 & 0 & 2 \end{bmatrix}$$

- $g(x) = x^3 + x^2 + x + 2$

$$GF(3^3)/x^3 + 2x + 1$$

```

clear
clc
GF_reg3=[1 0 0]
g3=[0 0 0];
%x^3 + 2x + 1,
n=25;
for i=1:n
%g2(i)=GF_reg(4); %последовательность G2
% сложение по модулю 3 первого*2 %и 3
разрядов регистра
moduloG3=mod(GF_reg3(1)+GF_reg3(3),3);
moduloG30=GF_reg3(3);
% сдвиг разрядов 1:3
GF_reg3(2:3)=mod(2*GF_reg3(1:2),3);
% присвоение modulo первому и второму
разрядам регистра
GF_reg3(2)=mod(moduloG3,3);
GF_reg3(1)=moduloG30;
GF_reg3
end

```



```

• GF_reg3 =
•   1   0   0
•   0   1   0
•   0   0   1
•   2   1   0
•   0   2   1
•   2   1   2
•   1   1   1
•   2   2   1
•   2   0   2
•   1   1   0
•   0   1   1
•   2   1   1
•   2   0   1
•   2   0   0
•   0   2   0
•   0   0   2
•   1   2   0
•   0   1   2
•   1   2   1
•   2   2   2
•   1   1   2
•   1   0   1
•   2   2   0
•   0   2   2
•   1   2   2
•   1   0   2
•   1   0   0

```