8 Код БЧХ

Одним з класів циклічних кодів, здатних виправляти багаторазові помилки, є коди БЧХ. Примітивним кодом БЧХ, виконуючим t_u помилок, називається код довжиною $n = q^m - 1$ над GF (q), для якого елементи $\alpha^1, \alpha^2, \ldots, \alpha^{2t_u}$ є корінням породжує многочлена.
Тут а - примітивний елемент GF (q^{m}).
Породжує многочлен визначається з виразу
$g(x) = HOK\left[f_1(x), f_2(x), \ldots, f_{2t_u}(x)\right],$ де f_1 (x), f_2 (x)...- мінімальні многочлени коренів g (x).

Число перевірочних елементів коду БЧХ задовольняє співвідношенню $r = n - k \le mt_u$.
Приклад. Визначити значення породжує многочлена для побудови примітивного коду БЧХ над GF (2) довжини 31, виправляє двох кратні помилки ($t_u = 2$).

Виходячи з визначення коду БЧХ корінням многочлена g (x) є: $\alpha^1, \alpha^2, \alpha^3, \alpha^{4(2t_u)}$, Де а - примітивний елемент GF (q^{m}) = GF (2^{5}).

Породжує многочлен визначається з виразу $g(x) = HOK\left[f_1(x), f_2(x), f_3(x), f_4(x)\right],$ де

f_1 (x), f_2 (x), f_3 (x), f_4 (x) - мінімальні многочлени коренів відповідно $\alpha^1, \alpha^2, \alpha^3, \alpha^4$.
Примітка.
Мінімальний многочлен елемента b поля GF (q^{m}) визначається з

виразу $f(x) = \left(x - \beta^{q^0}\right)\cdot\left(x - \beta^{q^1}\right)\cdot\left(x - \beta^{q^2}\right)\ldots\left(x - \beta^{q^{l-1}}\right)$, Де l - Найменше ціле число,

при якому $\beta^{q^l} = \beta$.
Значення мінімальних многочленів будуть наступними:

$$f_1(x) = (x-\alpha^1)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16}) =$$
$$= x^5 + x^2 + 1;$$
$$f_2(x) = (x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16})(x-\alpha^1) =$$
$$= x^5 + x^2 + 1;$$
$$f_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^{24})(x-\alpha^{17}) =$$
$$= x^5 + x^4 + x^3 + x^2 + 1;$$
$$f_4(x) = (x-\alpha^4)(x-\alpha^8)(x-\alpha^{16})(x-\alpha^1)(x-\alpha^2) =$$
$$= x^5 + x^2 + 1.$$

Так як f1 (x) = f2 (x) = f4 (x), то

$$g(x) = f_1(x)\cdot f_3(x) = \left(x^5 + x^2 + 1\right)\cdot\left(x^5 + x^4 + x^3 + x^2 + 1\right) =$$
$$= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

На практиці при визначенні значень породжує многочлена користуються спеціальною таблицею мінімальних многочленів (див. таблицю 8 додатка), і виразом для породжує многочлена $g(x) = f_1(x) f_3(x) \ldots f_j(x).$ При цьому робота здійснюється в такій послідовності.
По заданій довжині коду n і кратності виправляє помилок t_u визначають:
- З виразу $n = 2^m - 1$ значення параметра m, який є максимальним ступенем співмножників g (x); - з виразу $j = 2t_u - 1$ максимальний порядок мінімального многочлена, що входить до

числа співмножників g (x).
- Користуючись таблицею мінімальних многочленів, визначається вираз для g (x) в залежності від m та j. Для цього з колонки, відповідної параметру m, вибираються многочлени з порядками від 1 до j, які в результаті перемножування дають значення g (x).
У виразі для g (x) утримуватися мінімальні многочлени тільки для непарних ступенів a, так як зазвичай відповідні їм мінімальні многочлени парних ступенів a мають аналогічні вирази.

Наприклад, мінімальні многочлени елементів $\alpha^2, \alpha^4, \alpha^8, \ldots$ відповідають мінімальному многочлену елемента a^{1}, мінімальні многочлени елементів $\alpha^6, \alpha^{12}, \alpha^{24}, \ldots$ відповідають мінімальному многочлену a^3 та т.п.