Содержание

1 Коды Рида-Соломона

Важный частный случай q-ичных БЧХ-кодов длины $q^m - 1$ представляют кода с $m = 1$. Такие кода называются кодами Рида-Соломона, так как они впервые были описаны И.Ридом и Г.Соломоном в публикации 1960 г. После появления в том же 1960 г. работы Н. Цилера и Д.Горенстейна, содержащей обобщение конструкции БЧХ-кодов на недвоичный код, оказалось, что коды Рида–Соломона являются частным случаем БЧХ-кодов.

Легко видеть, что размерность k q-ичного кода Рида-Соломона длины $n = q - 1$ с конструктивным расстоянием d равна $n - d + 1$, т.е. длина, размерность и конструктивное расстояние кодов Рида–Соломона связаны равенством

$$d = n - k + 1 \tag{1.1}$$

В то же время известно следующая теорема, неравенство которой называется границей Синглтона.

Теорема 16.4. *Для любого (n, k)-кода с минимальным расстоянием d,справедливо неравенство $d \leq n - k + 1$.*

Доказательство. Пусть $\mathbf{H}$ — проверочная матрица линейного (n, k)-кода с минимальным расстоянием d. Ранг этой матрицы равен $n - k$, и при этом любые ее $d - 1$ столбцов линейно независимы. Следовательно, $n - k \geq d - 1$. Теорема доказана.

Из сравнения границы Синглтона и равенства (1.1) следует, что конструктивное расстояние кодов Рида-Соломона совпадает с их минимальным расстоянием, а сами коды являются максимальными.

Найдем порождающий многочлен кода Рида-Соломона длины 15, исправляющего две ошибки. В качестве поля из 16 элементов возьмем поле $\mathbb{Z}_2[\alpha]$, где α – корень примитивного многочлена $x^4 \oplus x \oplus 1$. Напомним, что степни примитивного элемента α этого поля выглядят следующим образом:

$\alpha^0 = (0001)$,	$\alpha^4 = (0011)$,	$\alpha^8 = (0101)$,	$\alpha^{12} = (1111)$,
$\alpha^1 = (0010)$,	$\alpha^5 = (0110)$,	$\alpha^9 = (1010)$,	$\alpha^{13} = (1101)$,
$\alpha^2 = (0100)$,	$\alpha^6 = (1100)$,	$\alpha^{10} = (0111)$,	$\alpha^{14} = (1001)$,
$\alpha^3 = (1000)$,	$\alpha^7 = (1011)$,	$\alpha^{11} = (1110)$.	

В этом случае многочлен

$$h(x) = (x \oplus \alpha)(x \oplus \alpha^2)(x \oplus \alpha^3)(x \oplus \alpha^4)$$

$=$

$x^4 \oplus (\alpha \oplus \alpha^2 \oplus \alpha^3 \oplus \alpha^4)x^3 \oplus (\alpha^3 \oplus \alpha^4 \oplus \alpha^6 \oplus \alpha^7)x^2 \oplus (\alpha^6 \oplus \alpha^7 \oplus \alpha^8 \oplus \alpha^9)x \oplus \alpha^{10}$

$=$

$$x^4 \oplus \alpha^{13}x^3 \oplus \alpha^6 x^2 \oplus \alpha^3 x \oplus \alpha^{10}$$

будет искомым порождающим многочленом.