Задача 1

- Найти порождающую матрицу расширенного кода Хэмминга (8,4).
- Найти минимальное расстояние кода, а также веса всех кодовых слов и расстояния между любыми парами кодовых слов.

Решение

Обычный код Хэмминга при r = 3 имеет параметры:

$$(2^r - 1, 2^r - 1 - r) = (7,4)$$

Расширенный код получают добавлением одного бита общей чётности к каждому кодовому слову длины 7.
Тогда длина становится 8, а число информационных битов остаётся 4: (8,4).

$H_{7,4}$— матрица 3×7, чьи столбцы — все ненулевые 3-битные двоичные векторы:

$$H_{7,4} = \begin{pmatrix} 1010101 \\ 1100110 \\ 0111111 \end{pmatrix}$$

Идея расширения: добавляем бит p так, чтобы сумма всех 8 бит была чётной:

$c_1 + .. c_7 + p = 0$ (mod 2).

Это означает, что к проверкам Хэмминга (3 строки) добавляется ещё одна проверка «общая чётность» (строка из единиц на первых 7 позициях и 1 на новой позиции).

Строим $H_{8,4}$ (размер 4×8) так:

- к $H_{7,4}$ добавляем справа столбец нулей,
- добавляем снизу строку из единиц длины 8 (проверка общей чётности).

Получаем:

$$H_{8,4} = \begin{pmatrix} 10101010 \\ 11001100 \\ 01111110 \\ 11111111 \end{pmatrix}$$

Нам нужна матрица G размера k×n = 4×8, такая что: $GH^T = 0$

и кодовые слова получаются как $c = mG$

Самый удобный вид — систематический: $\mathrm{G_{sys}} = [\mathrm{I_4}|\mathrm{P}]$

то есть первые 4 позиции — это прямо информационные биты, а остальные 4 — проверочные.

Приведем $\mathrm{H_{8,4}}$ к систематическому виду: $\mathrm{H_{sys}} = [P^T|I_4]$ с помощью элементарных преобразований:

$$H_{sys} = \begin{pmatrix} 01111000 \\ 10110100 \\ 11010010 \\ 11100001 \end{pmatrix}$$

Тогда:

$$\mathrm{G_{sys}} = \begin{pmatrix} 10000111 \\ 01011011 \\ 00101101 \\ 00111110 \end{pmatrix}$$

Обратив все элементарные преобразования над матрицей H найдем порождающую матрицу:

$$G = \begin{pmatrix} 11100001 \\ 10011001 \\ 01010101 \\ 11010010 \end{pmatrix}$$

Построим все кодовые слова как: $\mathrm{c} = \mathrm{mG}, \mathrm{m} \in \{0,1\}^4$

Все 16 кодовых слов:

ИС m	КС c=mG	вес	расстояния
0000	00000000	0	4,4,4,4,4,4,4,4,4,4,4,4,4,4,8
1000	11100001	4	4,4,4,4,4,4,4,4,4,4,4,4,4,8
0100	10011001	4	4,4,4,4,4,4,4,4,4,4,4,4,8
1100	01111000	4	4,4,4,4,4,4,4,4,4,4,4,8
0010	01010101	4	4,4,4,4,4,4,4,4,4,4,8
1010	10110100	4	4,4,4,4,4,4,4,4,4,8
0110	11001100	4	4,4,4,4,4,4,4,4,8
1110	00101101	4	8,4,4,4,4,4,4,4,4

0001	11010010	4	4,4,4,4,4,4,4
1001	00110011	4	4,4,4,4,4,4
0101	01001011	4	4,4,4,4,4
1101	10101010	4	4,4,4,4
0011	10000111	4	8,4,4
1011	01100110	4	4,8
0111	00011110	4	4
1111	11111111	8	-

Из таблицы: минимальный ненулевой вес равен 4 ⇒ $d_{min} = 4$

Задача 2

- Проверьте, что код дуальный коду Хэмминга действительно является симплексом.

Решение

Код Хэмминга: $\mathrm{n} = 2^{\mathrm{r}} - 1,\ \mathrm{k} = 2^{\mathrm{r}} - 1 - \mathrm{r}$

Дуальный код $\mathrm{C}^{\perp}$ имеет параметры: $(\mathrm{n}, \mathrm{n} - \mathrm{k}) = (2^{\mathrm{r}} - 1, \mathrm{r})$

То есть в дуальном коде размерность r, и всего кодовых слов:

$$|\mathrm{C}^{\perp}| = 2^{\mathrm{r}}$$

Для линейного кода:

- исходный код задаётся проверочной матрицей H: $\mathrm{cH}^{\mathrm{T}} = 0,$
- дуальный код $\mathrm{C}^{\perp}$— это все линейные комбинации строк H.

То есть порождающая матрица дуального кода — это H.

У кода Хэмминга H — матрица $\mathrm{r} \times (2^{\mathrm{r}} - 1)$, чьи столбцы — все ненулевые r-битные векторы.

Возьмём любое ненулевое $\mathrm{m} \in \mathrm{F}_2^{\mathrm{r}}$. Кодовое слово дуального кода: c=mH

j-я координата: $\mathrm{c_j} = \mathrm{m} \cdot \mathrm{h_j}$, где $\mathrm{h_j} - \mathrm{j} -$ й столбец H, а $\cdot$
$-$скалярное произведение по mod2

Функция f(v)=m·v - — ненулевая линейная функция (потому что m≠0).

У любой ненулевой линейной функции на F_2^r:

- ровно половина входов даёт 0,

- ровно половина входов даёт 1.

То есть среди всех 2^rвекторов v ровно 2^{r-1} дают f(v)=1

В H записаны все ненулевые v, но это все равно дает:

$$w(c) = 2^{r-1}$$

Значит, каждое ненулевое кодовое слово дуального кода имеет вес 2^{r-1}

Код линейный, значит: $d(c_1, c_2) = w(c_1 + c_2)$

Если $c_1 \neq c_2, c_1 + c_2 \neq 0,$ следлвательно его вес равен 2^{r-1}

$$d(c_1, c_2) = 2^{r-1} \text{ для любых } c_1 \neq c_2$$

Задача 3

- Постройте код, дуальный коду с проверкой на четность
    - Какие характеристики n, k у данного кода?
    - Сколько кодовых слов в этом коде?
    - Какое количество ошибок он может исправить?

Решение

Это код: $C = \{x \in F_2^n : x_1 + .. x_n = 0 (\text{mod } 2)\}$

У него:

- длина n,
- одна линейная проверка, значит размерность: k=n−1.

То есть это (n, n−1)-код.

Его проверочная матрица: H = (1 1 … 1)(1×n).

Дуальный код состоит из всех векторов y, таких что

y·x=0 ∀x∈C

Строки H порождают дуальный код.

А H — это одна строка из единиц.

Значит $C^{\perp}$— все кратные (по mod 2) этой строке:

$C^{\perp}$ =\{000…0, 111…1\}

Это повторный код (n,1).

Число кодовых слов: 2

Минимальное расстояние: $d_{min} = d(000..0,111..1) = n$

Исправляет количество ошибок: $t = \left[\frac{d_{min}-1}{2}\right] = \frac{n-1}{2}$