Домашнее задание 2

Задача 1

Рассмотрим код Хэмминга длины 7 и размерности 4 над полем $\mathbb{F}_2$. В систематическом виде его порождающая матрица имеет вид

$$G_7 = (I_4 \mid P),$$

где I_4 — единичная 4×4 матрица, а P — некоторая 4×3 матрица над $\mathbb{F}_2$. В качестве конкретного представителя можно взять, например,

$$G_7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Расширенный код длины 8 и той же размерности 4 получаем добавлением восьмой координаты, обеспечивающей чётность веса каждого кодового слова. Порождающая матрица одного из таких расширенных кодов может быть выбрана в виде

$$G_8 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Каждый вектор $u \in \mathbb{F}_2^4$ порождает кодовое слово

$$c(u) = uG_8 \in \mathbb{F}_2^8.$$

Всего получается $2^4 = 16$ кодовых слов.

Минимальное расстояние расширенного кода обозначим через $d_{\min}$. Его удобно находить с помощью перебора всех кодовых слов с использованием программы на Python (см. ниже). Для выбранной матрицы G_8 вычисления показывают, что

$$d_{\min} = 4,$$

а веса ненулевых кодовых слов принимают только значения 4 и 8. Следовательно, расстояния между любыми парами кодовых слов лежат в множестве

$$\{0, 4, 8\}.$$

Задача 2

Рассмотрим код Хэмминга длины $n = 2^r - 1$ и размерности $k = 2^r - 1 - r$. Его проверочная матрица H имеет размер $r \times n$ и строится так, что её столбцами служат все ненулевые двоичные векторы длины r:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{(для случая } r = 3,\ n = 7\text{)}.$$

Дуальный код $C^\perp$ по определению состоит из всех векторов, ортогональных всем словам исходного кода C. Для линейного кода с проверочной матрицей H строки H порождают именно $C^\perp$, поэтому порождающая матрица дуального кода может быть выбрана в виде

$$G^\perp = H.$$

Код $C^\perp$ называется *симплекс-кодом*, если все его ненулевые кодовые слова имеют одинаковый вес. Из конструкции H (все ненулевые r-битные столбцы) следует, что:

- длина дуального кода: $n = 2^r - 1$;
- размерность: $\dim C^\perp = r$;
- каждый ненулевой вектор $u \in \mathbb{F}_2^r$ задаёт кодовое слово $c(u) = uH$;
- множество решений уравнения $u \cdot h_j = 0$ (для фиксированного столбца h_j) имеет размер 2^{r-1}, то есть в половине столбцов координата $c(u)_j$ равна нулю, а в другой половине — единице.

Отсюда следует, что для любого $u \neq 0$

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

то есть все ненулевые кодовые слова имеют один и тот же вес. Так как код линейный, расстояние между любыми двумя различными кодовыми словами равно весу их разности, которая снова является ненулевым кодовым словом дуального кода. Следовательно,

$$d(x, y) = 2^{r-1}$$

для любых $x \neq y$ в $C^\perp$, и дуальный код действительно является симплекс-кодом.

Задача 3

Рассмотрим *код с проверкой на чётность* длины n:

$$C = \left\{ x \in \mathbb{F}_2^n : \sum_{i=1}^{n} x_i = 0 \right\}.$$

Это линейный подкод в $\mathbb{F}_2^n$, задаваемый одним линейным ограничением. Поэтому:

$$\dim C = n - 1, \qquad |C| = 2^{n-1}, \qquad d_{\min}(C) = 2.$$

Проверочная матрица для такого кода имеет вид одной строки

$$H = (1\ 1\ \dots\ 1) \in \mathbb{F}_2^{1\times n}.$$

Дуальный код $C^\perp$ порождается этой строкой, то есть

$$G^\perp = H.$$

Таким образом, $C^\perp$ содержит только два кодовых слова:

$$00\dots0, \quad 11\dots1.$$

Это *код повторения* длины n.

Его параметры:

$$\dim C^\perp = 1, \quad |C^\perp| = 2, \quad d_{\min}(C^\perp) = n.$$

Число исправляемых ошибок выражается через минимальное расстояние:

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{n - 1}{2} \right\rfloor.$$