ДЗ № 2

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. Расширенный код Хэмминга $(8, 4)$ (он же код первого порядка Рида–Мюллера $RM(1, 3)$) можно задать породжающей матрицей в следующем удобном виде (столбцы соответствуют точкам $\{0, 1\}^3$ в порядке $(000), (001), (010), (011), (100), (101), (110), (111)$):

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

Строки соответствуют функциям $1, x_1, x_2, x_3$ на вершинах куба. Этот код имеет параметры $[8, 4, d]$.

Минимальное расстояние. Для $RM(1, 3)$ (а значит и для расширенного кода Хэмминга $(8, 4)$) все ненулевые неконстантные аффинные функции принимают значение 1 ровно на половине точек $\{0, 1\}^3$, т.е. на 4 точках. Константные ненулевые функции дают вектор веса 8. Таким образом возможные веса кодовых слов:

$$0,\ 4,\ 8.$$

Отсюда минимальное расстояние кода

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

Полный список весов и их кратности. Размер пространства кодов $2^k = 2^4 = 16$; распределение весов:

- вес 0: ровно 1 кодовое слово (нулевое);

- вес 8: ровно 1 кодовое слово (вектор всех единиц, соответствующий строке [1 0 0 0] в базисе строк G с добавленной константой);
- вес 4: остальные $16 - 2 = 14$ кодовых слов.

Расстояния между парами кодовых слов. Код линейный, поэтому расстояние между любыми двумя кодовыми словами равно весу их разности, т.е. принадлежит множеству $\{0, 4, 8\}$. Следовательно любые два различных кодовых слова находятся на расстоянии либо 4, либо 8, а минимальное расстояние между различными словами равно 4.

Задача 2

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

Решение. Рассмотрим (нерасширенный) двоичный код Хэмминга длины 7 и размера 2^4 (параметры $[7, 4]$). Его проверочная матрица H (размер 3×7) можно выбрать так, чтобы в столбцах были все ненулевые векторы из $\mathbb{F}_2^3$ (в некотором порядке). Один из стандартных вариантов:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

где столбцы по порядку равны

$$(0,0,1)^\top,\ (0,1,0)^\top,\ (0,1,1)^\top,\ (1,0,0)^\top,\ (1,0,1)^\top,\ (1,1,0)^\top,\ (1,1,1)^\top,$$

т.е. всем ненулевым векторам $\mathbb{F}_2^3$.

Дуальный код $C^\perp$ коду Хэмминга имеет в качестве порождающей матрицы строки H (или эквивалентную матрицу) и имеет параметры $[7, 3]$ (так как $\dim C^\perp = 7 - 4 = 3$). Возьмём ненулевой вектор $v \in \mathbb{F}_2^3$ и рассмотрим кодовое слово $c = vH$ (произведение строки на матрицу даёт вектор длины 7). Компонента i этого вектора равна $v \cdot h_i$, где h_i—i-й столбец H. Линейная функция $x \mapsto v \cdot x$ на пространстве $\mathbb{F}_2^3$ имеет ядро размерности 2 (подпространство из 4 элементов), следовательно среди 7 ненулевых столбцов ровно 3 столбца дают скалярное произведение 0,

а ровно 4 — дают 1. Значит любой ненулевой $c = vH$ имеет ровно 4 единицы, т.е. вес 4.

Таким образом в $C^\perp$ все ненулевые кодовые слова имеют одинаковый вес 4, а код имеет параметры $[7, 3, 4]$. Это как раз определение (одного из) *симплексных* кодов — кодов, все ненулевые слова которых имеют одинаковый вес. Следовательно дуальный коду Хэмминга код действительно является симплексом.

Задача 3

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

Решение. Под кодом с проверкой на чётность обычно подразумевают *код чётности* длины n:

$$C_{\text{par}} = \{x \in \mathbb{F}_2^n : \ x_1 + \cdots + x_n = 0\},$$

то есть все векторы чётного веса. Этот код имеет параметры $[n, n-1, 2]$ (размерность $n-1$, минимальное расстояние 2).

Пусть C_{par} — код проверки на чётность. Его дуальный код $C_{\text{par}}^\perp$ имеет размерность

$$\dim C_{\text{par}}^\perp = n - \dim C_{\text{par}} = n - (n-1) = 1,$$

и, очевидно, порождается вектором всех единиц

$$\mathbf{1} = (1, 1, \ldots, 1).$$

Следовательно дуальный код — это *повторяющийся код* длины n (repetition code):

$$C_{\text{rep}} = \{(0, 0, \ldots, 0), \ (1, 1, \ldots, 1)\}.$$

Характеристики данного кода:

- длина: n;
- размерность: $k = 1$;

- количество кодовых слов: $2^k = 2$;
- минимальное расстояние: $d_{\min} = n$ (так как ненулевое кодовое слово имеет вес n).

Сколько ошибок он может исправить? Код с минимальным расстоянием $d = n$ исправляет до

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{n-1}{2} \right\rfloor$$

ошибок (при классическом декодировании по ближайшему коду — для повторяющегося кода это соответствует большинственному правилу: декодировать в тот из двух слов, к которому полученный вектор ближе). Заметим, что для повторяющегося кода это интуитивно: при нечисле ошибок $\leq \lfloor (n-1)/2 \rfloor$ большинство битов будут верны, и мы корректно восстановим исходный символ.