ДЗ № 1

ДЗ 1

Дан (5,2)-код с набором кодовых слов:

ИС	КС
00	00000
01	10110
10	01011
11	11101

1. Минимальное расстояние и исправляемость

Вычислим попарные расстояния Хэмминга между кодовыми словами:

$$\begin{aligned} d(00000, 10110) &= 3, \\ d(00000, 01011) &= 3, \\ d(00000, 11101) &= 4, \\ d(10110, 01011) &= 4, \\ d(10110, 11101) &= 3, \\ d(01011, 11101) &= 3. \end{aligned}$$

Следовательно минимальное расстояние

$$d_{\min} = 3.$$

По формуле код исправляет любые комбинации ошибок кратности

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{3 - 1}{2} \right\rfloor = 1,$$

то есть все одиночные ошибки гарантированно исправляются.

2. Вероятность ошибки при передаче по ДСК с $p = 10^{-3}$

Если возникает ровно два или более ближайших кодовых слова (ничья), считаем, что декодер выбирает равновероятно одно из ближайших кодовых слов. Для фиксированного переданного кодового слова c и полученного слова r вероятность получить r равна

$$\Pr(r \mid c) = p^w (1-p)^{5-w},$$

где w — вес вектора ошибок $e = r \oplus c$. Вероятность ошибки при передаче данного c равна сумма по всем r вероятностей $\Pr(r \mid c)$, умноженных на вероятность неправильного декодирования данного r (с учётом доли в случае ничьей). Тогда средняя по всем четырём кодовым словам вероятность ошибки равна

$$P_{\text{err}} = \frac{1}{4} \sum_{c \in C} \sum_{r \in \{0,1\}^5} \Pr(r \mid c) \cdot \mathbf{1}\{\text{декодер неверно восстановил } c\}.$$

Численный расчёт даёт

$$P_{\text{err}} \approx 7.986008998 \times 10^{-6} \approx 7.99 \cdot 10^{-6}.$$

3. Порождающая и проверочная матрицы

Код линейный: 00000 принадлежит коду, и побитовые суммы соответствуют суммам информационных слов. Возьмём базис информационных векторов

$$(1,0) \mapsto c(10) = 01011, \qquad (0,1) \mapsto c(01) = 10110.$$

Тогда порождающая матрица G (размер 2×5) в выбранном порядке информационных битов (m_1, m_2):

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

Проверочная матрица H (размер 3×5) должна удовлетворять $HG^T = 0$ над $\mathbb{F}_2$. Одна из возможных таких матриц:

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

Действительно, $Hc^T = 0$ (по модулю 2) для всех кодовых слов c.

ДЗ 2

Показать, что расстояние Хэмминга является метрикой.

Пусть $x, y \in \{0,1\}^n$. Определение:

$$d(x,y) = \#\{i\colon x_i \neq y_i\} = \mathrm{wt}(x \oplus y).$$

Докажем аксиомы метрики:

1. Невозрастаемость: $d(x,y) \geq 0$ очевидно, так как это число позиций.
2. Тождественность: $d(x,y) = 0 \iff x = y$ по определению (нет позиций с различием).
3. Симметричность: $d(x,y) = \mathrm{wt}(x \oplus y) = \mathrm{wt}(y \oplus x) = d(y,x)$.
4. Неравенство треугольника: для любых x, y, z имеем

$$x \oplus z = (x \oplus y) \oplus (y \oplus z),$$

поэтому в каждой позиции, где $(x \oplus z)_i = 1$, хотя бы одно из $(x \oplus y)_i$ или $(y \oplus z)_i$ равно 1. Отсюда

$$\mathrm{wt}(x \oplus z) \leq \mathrm{wt}(x \oplus y) + \mathrm{wt}(y \oplus z),$$

то есть

$$d(x,z) \leq d(x,y) + d(y,z).$$

Таким образом все аксиломы метрики выполняются, и расстояние Хэмминга — метрика.

ДЗ 3

Теорема. Пусть код имеет минимальное расстояние $d_{\min}$. Тогда он исправляет любые комбинации ошибок кратности

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

Доказательство. Пусть передано кодовое слово c, пришло $r = c + e$, где вес ошибки $\mathrm{wt}(e) \le t$. Для любого другого кодового слова $c' \ne c$ имеем неравенство треугольника:

$$d(c', r) = d(c', c + e) \ge d(c', c) - d(c, c + e) = d(c', c) - \mathrm{wt}(e).$$

Поскольку $d(c', c) \ge d_{\min}$, следует

$$d(c', r) \ge d_{\min} - \mathrm{wt}(e).$$

Так как $\mathrm{wt}(e) \le t \le \lfloor (d_{\min} - 1)/2 \rfloor$, получаем

$$d(c, r) = \mathrm{wt}(e) \le t < \frac{d_{\min} + 1}{2} \le d(c', r).$$

Следовательно r ближе по Хэммингу строго к правильному слову c, чем к любому другому кодовому слову, и ближайший сосед даёт правильное восстановление c. Это завершает доказательство.

ДЗ 4

Дан код с $k = 3, n = 6$ (8 кодовых слов):

ИС	КС
000	000000
100	110100
010	011010
110	101110
001	101001
101	011101
011	110011
111	000111

Код линейный, поскольку нулевое слово присутствует и суммы кодовых слов соответствуют суммам информационных слов. Возьмём за образы базисных информационных слов:

$$g_1 = c(100) = 110100, \quad g_2 = c(010) = 011010, \quad g_3 = c(001) = 101001.$$

Тогда порождающая матрица G (размер 3×6) в выбранном порядке (m_1, m_2, m_3):

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

Проверочная матрица H (размер 3×6) должна удовлетворять $HG^T = 0$ над $\mathbb{F}_2$. Одна из возможных матриц:

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

Проверка: $Hc^T = 0$ (по модулю 2) для всех кодовых слов c из таблицы.