ДСК, код (5,2)

Дан блочный код длины $(n = 5)$ и мощности (2^2) с кодовыми словами:

$$c_{00} = 00000, \quad c_{01} = 10110, \quad c_{10} = 01011, \quad c_{11} = 11101.$$

Требуется:

1. найти вероятность ошибки при передаче по ДСК с переходной вероятностью $(p = 10^{-3})$;
2. выбрать минимальное расстояние кода $(d_{\min} = \min_{x \neq y} d(x, y))$.

---

1. Минимальное расстояние кода $(d_{\min})$

Вычислим попарные расстояния:

- $(d(c_{00}, c_{01}) = w(00000 \oplus 10110) = w(10110) = 3)$.
- $(d(c_{00}, c_{10}) = w(00000 \oplus 01011) = w(01011) = 3)$.
- $(d(c_{00}, c_{11}) = w(00000 \oplus 11101) = w(11101) = 4)$.
- $(d(c_{01}, c_{10}) = w(10110 \oplus 01011) = w(11101) = 4)$.
- $(d(c_{01}, c_{11}) = w(10110 \oplus 11101) = w(01011) = 3)$.
- $(d(c_{10}, c_{11}) = w(01011 \oplus 11101) = w(10110) = 3)$.

Следовательно,

$$d_{\min} = \min\{3, 3, 4, 4, 3, 3\} = 3.$$

Ответ:

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

---

2. Исправляющая способность

Для блочного кода с минимальным расстоянием $(d_{\min})$ гарантированно исправляется

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

ошибок в блоке.

При $(d_{\min} = 3)$:

$$t = \left\lfloor \frac{3-1}{2} \right\rfloor = \lfloor 1 \rfloor = 1.$$

То есть код гарантированно исправляет **1 ошибку** в 5-битном блоке.

---

3. Вероятность ошибки при передаче по ДСК

Пусть $(W \sim \mathrm{Bin}(n = 5, p))$ - число ошибок в блоке при передаче по ДСКс вероятностью ошибки бита (p).

При декодировании по минимальному расстоянию и $(d_{\min} = 3)$ гарантированно корректно декодируются все случаи $(W \le t = 1)$. Поэтому вероятность ошибки оценивается как

$$P_e = \mathbb{P}(W \ge t+1) = \mathbb{P}(W \ge 2) = \sum_{i=2}^{5} \binom{5}{i} p^i (1-p)^{5-i}.$$

Эквивалентно:

$$P_e = 1 - \Big[(1-p)^5 + 5p(1-p)^4\Big].$$

Подставим $(p = 10^{-3})$:

$$(1-p)^5 = 0.999^5 \approx 0.995009990004999,$$

$$5p(1-p)^4 = 5 \cdot 10^{-3} \cdot 0.999^4 \approx 0.004970024990005.$$

Тогда

$$P_e \approx 1 - (0.995009990004999 + 0.004970024990005) \approx 9.980014996 \times 10^{-6}.$$

Ответ:

$$\boxed{P_e \approx 9.98 \cdot 10^{-6}.}$$

Порождающая и проверочная матрицы

Дан код $(5, 2)$ с множеством кодовых слов:

$$C = \{00000,\ 10110,\ 01011,\ 11101\} \subset \mathbb{F}_2^5.$$

---

1. Проверка линейности

Для линейного кода требуется:

1. $(0 \in C)$;
2. замкнутость относительно сложения по модулю 2 (XOR).

Имеем $(00000 \in C)$. Также:

$$10110 \oplus 01011 = 11101 \in C.$$

Следовательно, (C) - подпространство $(\mathbb{F}_2^5)$. Так как $(|C| = 4 = 2^2)$, то $(\dim C = 2)$, т.е. это линейный код $((n, k) = (5, 2))$.

---

2. Порождающая матрица (G)

Выберем два линейно независимых ненулевых кодовых слова в качестве базиса:

$$g_1 = 10110, \qquad g_2 = 01011,$$

причём $(g_1 \oplus g_2 = 11101 \neq 00000)$, значит они независимы.

Тогда порождающую матрицу можно взять в виде матрицы, строки которой (g_1, g_2):

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

Проверка: для $(u = (u_1, u_2) \in \mathbb{F}_2^2)$ кодовое слово равно $(c = uG)$, и получаем:

- $(00 \cdot G = 00000)$,
- $(10 \cdot G = 10110)$,
- $(01 \cdot G = 01011)$,
- $(11 \cdot G = 10110 \oplus 01011 = 11101)$.

---

3. Проверочная матрица (H)

Проверочная матрица (H) определяется условием

$$G\,H^{\mathsf{T}} = 0 \quad \text{в } \mathbb{F}_2.$$

То есть каждая строка $(h = (h_1, \ldots, h_5))$ матрицы (H) должна быть ортогональна к строкам (G):

$$(1,0,1,1,0)\cdot(h_1,\dots,h_5) = h_1 + h_3 + h_4 = 0,$$
$$(0,1,0,1,1)\cdot(h_1,\dots,h_5) = h_2 + h_4 + h_5 = 0.$$

Отсюда выражаем:

$$h_1 = h_3 + h_4, \qquad h_2 = h_4 + h_5,$$

а (h_3, h_4, h_5) — свободные параметры (что согласуется с $(\dim C^\perp = 5 - 2 = 3)$).

Выберем три независимых решения, задавая (h_3, h_4, h_5):

1. $(1,0,0) \Rightarrow h = (1,0,1,0,0)$
2. $(0,0,1) \Rightarrow h = (0,1,0,0,1)$
3. $(1,1,1) \Rightarrow h = (0,0,1,1,1)$

Тогда

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

и действительно $(GH^\mathsf{T} = 0)$ над $(\mathbb{F}_2)$.

Расстояние Хэмминга как метрика

1. Неотрицательность

Так как $(d_H(x,y))$ — мощность множества индексов, то

$$d_H(x,y) \geq 0.$$

---

2. Тождественность неразличимых

Докажем эквивалентность:

$$d_H(x,y) = 0 \iff x = y.$$

- Если $(x = y)$, то для всех i выполняется $(x_i = y_i)$, значит множество $\{i : x_i \neq y_i\}$ пусто, следовательно $d_H(x,y) = 0$.
- Если $(d_H(x,y) = 0)$, то $(\{i : x_i \neq y_i\} = \varnothing)$. Значит для всех i $(x_i = y_i)$, то есть $(x = y)$.

---

3. Симметрия

Для каждого i верно:

$$x_i \neq y_i \iff y_i \neq x_i.$$

Следовательно множества несовпадений совпадают, и

$$d_H(x,y) = d_H(y,x).$$

---

4. Неравенство треугольника

Пусть $(x, y, z \in \Sigma^n)$. Рассмотрим индекс i.
Если $(x_i \neq z_i)$, то не может одновременно быть $(x_i = y_i)$ и $(y_i = z_i)$, иначе получилось бы $(x_i = z_i)$.
Значит

$$x_i \neq z_i \Rightarrow (x_i \neq y_i) \vee (y_i \neq z_i).$$

Отсюда следует включение множеств:

$$\{i : x_i \neq z_i\} \subseteq \{i : x_i \neq y_i\} \cup \{i : y_i \neq z_i\}.$$

Берём мощности и используем $(|A \cup B| \leq |A| + |B|)$:

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

Итог

Расстояние Хэмминга удовлетворяет:

1. $(d_H(x,y) \geq 0)$,
2. $(d_H(x,y) = 0 \iff x = y)$,
3. $(d_H(x,y) = d_H(y,x))$,
4. $(d_H(x,z) \leq d_H(x,y) + d_H(y,z))$.

Следовательно, (d_H) является метрикой на (Σ^n).

Теорема об исправляющей способности кода

Теорема.

Пусть $C \subseteq \Sigma^n$ - блочный код, а $d(\cdot,\cdot)$ — расстояние Хэмминга.
Минимальное расстояние кода определяется как

$$d_{\min} = \min_{\substack{c,c' \in C \\ c \neq c'}} d(c,c').$$

Тогда код исправляет любые ошибки кратности

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

То есть, если передано кодовое слово $c \in C$, а принято слово r таково, что $d(r,c) \leq t$, то декодирование по минимальному расстоянию единственным образом восстанавливает c.

Доказательство

Зафиксируем произвольное переданное кодовое слово $c \in C$.
Пусть в канале произошло не более t ошибок, и потому для принятого слова r выполнено

$$d(r,c) \leq t.$$

Рассмотрим любое другое кодовое слово $c' \in C$, $c' \neq c$.
По неравенству треугольника для расстояния Хэмминга имеем

$$d(r,c') \geq d(c,c') - d(r,c).$$

По определению минимального расстояния $d(c,c') \geq d_{\min}$, а также $d(r,c) \leq t$.
Следовательно,

$$d(r,c') \geq d_{\min} - t.$$

Итак, для любого $c' \neq c$ выполнено

$$d(r,c) \leq t, \qquad d(r,c') \geq d_{\min} - t.$$

Чтобы c было строго ближе к r, чем любое другое $c' \neq c$, достаточно потребовать

$$t < d_{\min} - t \quad \Longleftrightarrow \quad 2t < d_{\min}.$$

Так как t - целое неотрицательное число, условие $2t < d_{\min}$ эквивалентно

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

При этом условии c является единственным ближайшим кодовым словом к r, поэтому декодирование по минимальному расстоянию возвращает c.
Следовательно, любые ошибки кратности не более t исправляются.

Порождающая и проверочная матрицы для заданного кода

По таблице задано отображение информационных символов длины 3 в кодовые слова длины 6:

- $(000 \mapsto 000000)$
- $(100 \mapsto 110100)$
- $(010 \mapsto 011010)$
- $(001 \mapsto 101001)$
- $(110 \mapsto 101110)$
- $(101 \mapsto 011101)$
- $(011 \mapsto 110011)$
- $(111 \mapsto 000111)$

---

1) Линейность кода

Поскольку $(000 \mapsto 000000)$, нулевое слово принадлежит коду.

Проверим линейность по базисным векторам $(100, 010, 001)$. Если код линейный, то должно выполняться:

$$c(u \oplus v) = c(u) \oplus c(v).$$

Например:

$$c(110) = c(100) \oplus c(010) = 110100 \oplus 011010 = 101110,$$

что совпадает с таблицей.

Аналогично:

$$c(101) = c(100) \oplus c(001) = 110100 \oplus 101001 = 011101,$$

$$c(011) = c(010) \oplus c(001) = 011010 \oplus 101001 = 110011,$$

$$c(111) = c(100) \oplus c(010) \oplus c(001) = 000111.$$

Следовательно, заданный код является линейным двоичным кодом $((n, k) = (6, 3))$.

---

2) Порождающая матрица G

Для линейного кода естественно взять в качестве строк G кодовые слова, соответствующие базисным ИС:

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

Тогда порождающая матрица:

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

и для любого $(u = (u_1, u_2, u_3) \in \mathbb{F}_2^3)$ кодовое слово равно $(c = uG)$.

---

3) Проверочная матрица H

Проверочная матрица H должна удовлетворять условию ортогональности:

$$G\,H^{\mathsf{T}} = 0 \quad \text{в } \mathbb{F}_2.$$

То есть каждая строка $(h = (h_1, \ldots, h_6))$ матрицы H должна решать систему:

$$\begin{cases} (1,1,0,1,0,0) \cdot h = h_1 + h_2 + h_4 = 0, \\ (0,1,1,0,1,0) \cdot h = h_2 + h_3 + h_5 = 0, \\ (1,0,1,0,0,1) \cdot h = h_1 + h_3 + h_6 = 0. \end{cases}$$

Один из корректных выборов трёх линейно независимых решений:

$$h^{(1)} = 001011, \quad h^{(2)} = 010110, \quad h^{(3)} = 100101.$$

Тогда

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

и действительно $(G\,H^{\mathsf{T}} = 0)$ (по модулю 2).
