Домашнее задание по теории кодирования

Дубровин Т.Г.

Февраль 2026

1 ДЗ 1

1.1 Условие

Дан (5,2)-линейный код с таблицей кодовых слов:

ИС	КС
00	00000
01	10110
10	01011
11	11101

1. Найти вероятность ошибки при передаче по ДСК с переходной вероятностью $p = 10^{-3}$.

2. Найти порождающую и проверочную матрицы

1.2 Решение

ДСК с вероятностью ошибки в одном символе $p = 10^{-3}$, вероятность правильной передачи символа $q = 1 - p = 0.999$.

Таблицу расстояний Хэмминга $d(c_i, c_j)$:

	00000	10110	01011	11101
00000	0	3	3	3
10110	3	0	4	2
01011	3	4	0	4
11101	3	2	4	0

Минимальное расстояние кода $d_{\min} = 2$.

При малом p ($p = 0.001$) можно использовать хорошее приближение:

$$P_{\text{err}} \approx 1 - \left(q^5 + 5\,p\,q^4\right)$$

$$P_{\text{err}} \approx 1 - (0{,}999^5 + 5 \cdot 0.001 \cdot 0{,}999^4) \approx 9.97 \times 10^{-6}$$

Составляем матрицу, строки которой — кодовые слова, соответствующие базисным информационным векторам:

ИС	кодовое слово				
00	0	0	0	0	0
01	1	0	1	1	0
10	0	1	0	1	1

Берём строки, соответствующие 01 и 10 (они линейно независимы):

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad \text{(систематический вид)}$$

Проверим, что третья строка тоже получается:

$$(1,1) \cdot G = (1,0,1,1,0) + (0,1,0,1,1) = (1,1,1,0,1) = 11101 \mod 2$$

Для систематического кода (n,k) проверочная матрица имеет вид:

$$H = \left(P^T \mid I_{n-k}\right)$$

Здесь $n-k=3$, из G берём правую часть P (столбцы 3,4,5):

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \qquad \Rightarrow \qquad P^T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Тогда

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

Проверка: $G \cdot H^T = 0$:

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

1.3 Ответы

1. Вероятность ошибки декодирования при $p = 10^{-3}$ составляет примерно $\mathbf{9.97 \times 10^{-6}}$.
2. Порождающая матрица:
$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$
Проверочная матрица:
$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

2 ДЗ 2

2.1 Условие

Показать, что расстояние Хемминга удовлетворяет аксиомам расстояния и может использоваться как метрика

2.2 Решение

Пусть $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \{0,1\}^n$.

Расстояние Хемминга определяется как число позиций, в которых векторы различаются:

$$d_H(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} 1_{\{x_i \neq y_i\}} = |\{i \mid x_i \neq y_i\}|$$

или эквивалентно:

$$d_H(\mathbf{x}, \mathbf{y}) = w_H(\mathbf{x} + \mathbf{y}) \quad \text{(где сложение по mod 2, а } w_H \text{ — вес Хемминга)}$$

Чтобы функция $d : X \times X \to \mathbb{R}_{\geq 0}$ была метрикой на множестве $X = \{0,1\}^n$, она должна удовлетворять следующим четырём аксиомам:

(M1) **Неотрицательность**: $d(\mathbf{x}, \mathbf{y}) \geq 0$ для любых $\mathbf{x}, \mathbf{y} \in X$

(M2) **Тождество нулевого расстояния**: $d(\mathbf{x}, \mathbf{y}) = 0 \iff \mathbf{x} = \mathbf{y}$

(M3) **Симметричность**: $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ для любых $\mathbf{x}, \mathbf{y}$

(M4) **Неравенство треугольника**: $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$ для любых $\mathbf{x}, \mathbf{y}, \mathbf{z}$

2.2.1 (M1)

$d_H(\mathbf{x}, \mathbf{y})$ — это количество позиций, в которых $x_i \neq y_i$. Количество всегда целое неотрицательное число:

$$d_H(\mathbf{x}, \mathbf{y}) \in \{0, 1, 2, \ldots, n\} \quad \Rightarrow \quad d_H(\mathbf{x}, \mathbf{y}) \geq 0$$

Аксиома выполнена.

2.2.2 (M2)

Если $\mathbf{x} = \mathbf{y}$, то $x_i = y_i$ для всех $i = 1, \ldots, n$. Следовательно, нет ни одной позиции, где они различаются:

$$d_H(\mathbf{x}, \mathbf{x}) = 0$$

Если $d_H(\mathbf{x}, \mathbf{y}) = 0$, то количество различающихся позиций равно нулю, то есть $x_i = y_i$ для всех i. Следовательно, $\mathbf{x} = \mathbf{y}$.

Таким образом:

$$d_H(\mathbf{x}, \mathbf{y}) = 0 \quad \iff \quad \mathbf{x} = \mathbf{y}$$

Аксиома выполнена.

2.2.3 (M3)

Пусть $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$. Множество позиций, где $x_i \neq y_i$, совпадает с множеством позиций, где $y_i \neq x_i$ (сравнение симметрично). Поэтому число таких позиций одинаково:

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}| = |\{i : y_i \neq x_i\}| = d_H(\mathbf{y}, \mathbf{x})$$

Аксиома выполнена.

2.2.4 (M4)

Пусть $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \{0,1\}^n$.

Для каждой координаты $i = 1, \ldots, n$ рассмотрим возможные значения троек $(x_i, y_i, z_i) \in \{0,1\}^3$.

Неравенство треугольника в терминах индикаторов различия:

$$1_{\{x_i \neq z_i\}} \leq 1_{\{x_i \neq y_i\}} + 1_{\{y_i \neq z_i\}}$$

Проверим это для всех 8 возможных комбинаций:

x_i	y_i	z_i	$x_i \neq z_i$	$x_i \neq y_i$	$y_i \neq z_i$
левая $\leq$ правая					
0	0	0	0	0	0
$0 \leq 0{+}0$					
0	0	1	1	0	1
$1 \leq 0{+}1$					
0	1	0	1	1	1
$1 \leq 1{+}1$					
0	1	1	0	1	0
$0 \leq 1{+}0$					
1	0	0	1	1	0
$1 \leq 1{+}0$					
1	0	1	0	1	1
$0 \leq 1{+}1$					
1	1	0	1	0	1
$1 \leq 0{+}1$					
1	1	1	0	0	0
$0 \leq 0{+}0$					

Во всех случаях неравенство выполняется (и даже строго — левая часть никогда не больше правой).

Суммируя по всем координатам $i = 1, \ldots, n$:

$$\sum_{i=1}^{n} 1_{\{x_i \neq z_i\}} \leq \sum_{i=1}^{n} \big(1_{\{x_i \neq y_i\}} + 1_{\{y_i \neq z_i\}}\big)$$

то есть

$$d_H(\mathbf{x}, \mathbf{z}) \leq d_H(\mathbf{x}, \mathbf{y}) + d_H(\mathbf{y}, \mathbf{z})$$

Аксиома выполнена.

2.3 Ответ

Расстояние Хемминга $d_H(\mathbf{x}, \mathbf{y})$ **является метрикой** в пространстве двоичных векторов длины n.

3 ДЗ 3

3.1 Условие

Доказать теорему

Код с минимальным расстоянием d_{min} исправляет любые комбинации ошибок кратности $t \leq \lfloor (d-1)/2 \rfloor$, где $\lfloor x \rfloor$ - наибольшее целое, не превышающее x

3.2 Решение

Пусть $C \subseteq \{0,1\}^n$ — код (не обязательно линейный) с минимальным расстоянием Хемминга

$$d_{\min} = \min_{\substack{\mathbf{c}_1, \mathbf{c}_2 \in C \\ \mathbf{c}_1 \neq \mathbf{c}_2}} d_H(\mathbf{c}_1, \mathbf{c}_2).$$

Пусть передано кодовое слово $\mathbf{c} \in C$, а принято слово

$$\mathbf{r} = \mathbf{c} + \mathbf{e},$$

где $\mathbf{e}$ — вектор ошибки, $w_H(\mathbf{e}) = t$ (вес Хемминга, число единиц).

Требуется показать, что если $t \leq \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$, то $\mathbf{c}$ — **единственное** кодовое слово, ближайшее к $\mathbf{r}$ по расстоянию Хемминга (т.е. декодер максимального правдоподобия всегда восстановит правильное $\mathbf{c}$).

Предположим противное: существует кодовое слово $\mathbf{c}' \in C$, $\mathbf{c}' \neq \mathbf{c}$, такое что

$$d_H(\mathbf{r}, \mathbf{c}') \leq d_H(\mathbf{r}, \mathbf{c}).$$

То есть принятое слово $\mathbf{r}$ находится не дальше от другого кодового слова $\mathbf{c}'$, чем от переданного $\mathbf{c}$.

Запишем:

$$\mathbf{r} = \mathbf{c} + \mathbf{e}, \qquad w_H(\mathbf{e}) = t.$$

Тогда по неравенству треугольника:

$$\begin{aligned} d_H(\mathbf{c}, \mathbf{c}') &\leq d_H(\mathbf{c}, \mathbf{r}) + d_H(\mathbf{r}, \mathbf{c}') \\ &\leq d_H(\mathbf{c}, \mathbf{r}) + d_H(\mathbf{c}, \mathbf{r}) && \text{(по предположению)} \\ &= 2 \cdot d_H(\mathbf{c}, \mathbf{r}) \\ &= 2 \cdot w_H(\mathbf{e}) \\ &= 2t. \end{aligned}$$

Но $d_H(\mathbf{c}, \mathbf{c}') \geq d_{\min}$, поскольку $\mathbf{c} \neq \mathbf{c}'$ и $d_{\min}$ — минимальное расстояние в коде.

Получаем:

$$d_{\min} \leq d_H(\mathbf{c}, \mathbf{c}') \leq 2t \quad \Rightarrow \quad d_{\min} \leq 2t.$$

Отсюда следует:

$$t \geq \frac{d_{\min}}{2}.$$

Но по условию теоремы

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

(заметим, что $\left\lfloor \frac{d_{\min}-1}{2} \right\rfloor \leq \frac{d_{\min}-1}{2} < \frac{d_{\min}}{2}$)
Получили противоречие:

$$t < \frac{d_{\min}}{2} \quad \text{и} \quad t \geq \frac{d_{\min}}{2}.$$

Следовательно, наше предположение неверно.
То есть **не существует** кодового слова $\mathbf{c}' \neq \mathbf{c}$, для которого

$$d_H(\mathbf{r}, \mathbf{c}') \leq d_H(\mathbf{r}, \mathbf{c}).$$

Иными словами, $\mathbf{c}$ — строго ближайшее кодовое слово к $\mathbf{r}$.
Теорема доказана.

3.3 Ответ

Код с минимальным расстоянием $d_{\min}$ исправляет все ошибки кратности

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

4 ДЗ 4

4.1 Условие

Найти порождающую и проверочную матрицы для кода

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

4.2 Решение

Берём кодовые слова, соответствующие единичным информационным векторам (базисным):

ИС	КС					
100	1	1	0	1	0	0
010	0	1	1	0	1	0
001	1	0	1	0	0	1

Таким образом, можно сразу записать матрицу-генератор в **несистематическом** виде:

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

Рассмотрим все кодовые слова и найдём три линейно независимых столбца, которые можно привести к I_3.

После анализа таблицы видно, что удобнее всего взять столбцы 1, 2, 6 как независимые:

Соответствующие кодовые слова:

ИС	1	2	3	4	5	6
100	1	1	0	1	0	**0**
010	0	1	1	0	1	**0**
001	1	0	1	0	0	**1**

Матрица по столбцам 1,2,6:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{определитель по mod 2} \neq 0 \quad \Rightarrow \text{ обратима}$$

Выполняем приведение к виду $I_3|P$:

Исходная матрица (переставляем столбцы мысленно: 1,2,6,3,4,5):

$$G'' = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \qquad \text{(столбцы в порядке 1,2,6,3,4,5)}$$

Теперь приводим левую часть к I_3:

1. Строка 3 ← Строка 3 + Строка 1 → (1 0 1 | 1 0 0) + (1 1 0 | 0 1 0) = (0 1 1 | 1 1 0)

2. Строка 3 ← Строка 3 + Строка 2 → (0 1 1 | 1 1 0) + (0 1 0 | 1 0 1) = (0 0 1 | 0 1 1)

Теперь:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right)$$

3. Строка 1 ← Строка 1 + Строка 3 → (1 1 0 | 0 1 0) + (0 0 1 | 0 1 1) = (1 1 1 | 0 0 1)

4. Строка 1 ← Строка 1 + Строка 2 → (1 1 1 | 0 0 1) + (0 1 0 | 1 0 1) = (1 0 1 | 1 0 0)

5. Строка 1 ← Строка 1 + Строка 3 → (1 0 1 | 1 0 0) + (0 0 1 | 0 1 1) = (1 0 0 | 1 1 1)

Получаем систематическую порождающую матрицу (в порядке информационных позиций 1,2,6):

$$\boxed{G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad \text{(информационные позиции: 1,2,6)}}$$

Для систематического кода $G = (I_k \mid P)$ проверочная матрица

$$H = (P^T \mid I_{n-k})$$

Здесь $k = 3$, $n - k = 3$,

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \qquad P^T = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Тогда

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

4.3 Ответ

Порождающая матрица (систематический вид, информационные позиции 1, 2, 6):

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

Проверочная матрица:

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