Изучение строения линейного кода

Задача 1. Пусть $G = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$ — порождающая матрица бинарного линейного (5,3)-кода. Найти для этого кода проверочную матрицу, все кодовые слова, а также дуальный код. Найти весовые спектры этих кодов. Выписать все синдромы и лидеры смежных классов и декодировать при помощи лидеров слово 11010.

Решение. Для данного кода C длина сообщений $k = 3$, длина кодовых слов $n = 5$ и число проверочных соотношений $m = n - k = 2$. Порождающая матрица G не имеет систематического вида. Поэтому прежде чем применять известное правило нахождения проверочной матрицы приведем G эквивалентными преобразованиями над полем $\mathbb{F}_2$ к каноническому (систематическому) виду $G' = (E_3 \mid -A^{\mathrm{T}})$, где $A \in (\mathbb{F}_2)^{2\times 3}$. Тогда $H = (A \mid E_2)$ является каноническим видом проверочной матрицы кода C. Под матрицей будем записывать ее элементарные преобразования, обозначая строки матрицы римскими цифрами.

$$G = \underset{III\leftrightarrow I}{\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}} \sim \underset{III\leftrightarrow II}{\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}} \sim$$

$$\sim \underset{II+I\ III+I}{\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}} \sim G' = \Bigg(\underset{E_3}{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}} \ \Bigg|\ \underset{-A^{\mathrm{T}}}{\begin{matrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \end{matrix}}\Bigg).$$

Таким образом, $-A^{\mathrm{T}} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$, следовательно,

$$A = -(-A^{\mathrm{T}})^{\mathrm{T}} = (-A^{\mathrm{T}})^{\mathrm{T}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

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

Пусть $\mathbf{a} = (a_1, a_2, a_3)$, где $a_1, a_2, a_3 \in \mathbb{F}_2$, — сообщение, тогда соответствующее кодовое слово равно

$$\mathbf{x} = (x_1, x_2, x_3, x_4, x_5) = \mathbf{a}G' = (a_1, a_2, a_3, a_1 + a_2 + a_3, a_3).$$

Кстати, для исходной порождающей матрицы код C (в смысле "кодовой книги", т.е. набора всех кодовых слов) будет тот же, что и для G',C'. Однако соответствие между сообщениями и кодовыми словами будет, конечно, другое.

$$\mathbf{x} = (x_1, x_2, x_3, x_4, x_5) = \mathbf{a}G = (a_1 + a_2 + a_3, a_1, a_2, a_3, a_2).$$

Приведем исходную матрицу элементарными преобразованиями к систематическому виду подробно, используя MapleV. Прибавили ко второй первую строку.

```
> G1a:= matrix_modp(addrow(G1,1,2,1),2);
```

$$G1a := \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Переставили первую и третью строки.

```
> G1b :=swaprow(G1a, 1, 3);
```

$$G1b := \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Прибавили к третьей первую.

```
> G1c:= matrix_modp(addrow(G1b,1,3,1),2);
```

$$G1c := \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Прибавили к третьей вторую.

```
> G1d:= matrix_modp(addrow(G1c,2,3,1),2);
```

$$G1d := \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Прибавили ко второй третью.

```
> G1e:= matrix_modp(addrow(G1d,3,2,1),2);
```

$$G1e := \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Составим списки кодовых слов с обеими порождающими матрицами.

```
> C1:=code_list(G1e,2);
```

$C1 := [[0, 0, 0, 0, 0], [0, 0, 1, 1, 1], [0, 1, 0, 1, 0], [0, 1, 1, 0, 1], [1, 0, 0, 1, 0], [1, 0, 1, 0, 1], [1, 1, 0, 0, 0], [1, 1, 1, 1, 1]]$

```
> C1s:=sort(C1,weight_order);
```

$C1s := [[0, 0, 0, 0, 0], [0, 1, 0, 1, 0], [1, 0, 0, 1, 0], [1, 1, 0, 0, 0], [0, 0, 1, 1, 1], [0, 1, 1, 0, 1], [1, 0, 1, 0, 1], [1, 1, 1, 1, 1]]$

```
> Cs:=sort(code_list(G1,2),weight_order);
```

$Cs := [[0, 0, 0, 0, 0], [1, 0, 0, 1, 0], [1, 1, 0, 0, 0], [0, 1, 0, 1, 0], [1, 0, 1, 0, 1], [0, 0, 1, 1, 1], [0, 1, 1, 0, 1], [1, 1, 1, 1, 1]]$

Код (в смысле множества векторов) тот же самый. Правда отображение $L_k - - > L_n$ другое, например, образы сообшения (001) различные.

```
> multiply( [0,0,1], G1 );multiply( [0,0,1], G1e );
```

$$[1, 0, 0, 1, 0]$$

$$[0, 0, 1, 1, 1]$$

Систематический вид проверочной матрицы

```
> H:=matrix([[1,1,1,1,0],[0,0,1,0,1]]);
```

$$H := \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Умножим ее на порождающую

```
> matrix_modp(multiply(G1,transpose(H)),2);
```

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

```
> matrix_modp(multiply(G1e,transpose(H)),2);
```

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Матрица является проверочной и для исходного кода.

Приведем таблицу всевозможных сообщений и соответствующих кодовых слов.

$\mathbf{F_2^3}$	000	001	010	011	100	101	110	111
C	00000	10010	10101	00111	11000	01010	01101	11111
C'	00000	00111	01010	01101	10010	10101	11000	11111

Проверочная матрица используется для установления наличия ошибок и их исправления. Ее основное свойство $G \cdot H^T = 0$ отражает тот факт, что проверочная матрица, будучи порождающей для дуального кода, имеет строки, ортогональные всем кодовым словам. Поэтому переход от исходной матрицы G к систематической G' (к другому базису) этого условия не нарушает.

Запишем таблицу лидеров $\mathbf{e_i}$ и соответствующих смежных классов $\mathbf{e}_i + C$. С точки зрения математики это разложение группы по смежным классам. Новый класс мы начинаем с так называемого "лидера", который трактуется как вектор -ошибка. Число лидеров (смежных классов) равно $2^n/|C| = 2^n/2^k = 2^m = 4$. Заполнение таблицы происходит следующим образом: сначала выписываем все кодовые слова $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$, $\mathbf{x}_4$, $\mathbf{x}_5$, $\mathbf{x}_6$, $\mathbf{x}_7$ $\mathbf{x}_8$, (первая строка таблицы). Очевидно, синдромы нулевые, $S(\mathbf{x}_j) = (0,0)^{\mathrm{T}}$. Затем выбираем лидеры $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{e}_3$, $\mathbf{e}_4$ смежных классов, так, чтобы их вес был как можно меньше и $S(\mathbf{e}_i) \neq S(\mathbf{e}_j)$ для $i \neq j$.

Векторы из $\mathbb{F}_2^5$ наименьшего веса — суть

$$\mathbf{x}_1 = 00000,\ \mathbf{w}_1 = 00001,\ \mathbf{w}_2 = 00010,$$
$$\mathbf{w}_3 = 00100,\ \mathbf{w}_4 = 01000,\ \mathbf{w}_5 = 10000.$$

Напомним, что $S(\mathbf{y}) = S(\mathbf{e}_i)$, если $\mathbf{y} \in \mathbf{e}_i + C$ и $S(\mathbf{e}_i) \neq S(\mathbf{e}_j)$ для $i \neq j$, где $S(\mathbf{y}) = H \cdot \mathbf{y}^T$ — синдром вектора $\mathbf{y}$.Посчитаем их синдромы:

$$S(\mathbf{x}_1) = (0,0)^{\mathrm{T}},\ S(\mathbf{w}_1) = (0,1)^{\mathrm{T}},$$
$$S(\mathbf{w}_2) = S(\mathbf{w}_4) = S(\mathbf{w}_5) = (1,0)^{\mathrm{T}},\ S(\mathbf{w}_3) = (1,1)^{\mathrm{T}}.$$

Возьмем в качестве векторов $\mathbf{e}_1 = \mathbf{x}_1$, $\mathbf{e}_2 = \mathbf{w}_1$, $\mathbf{e}_3 = \mathbf{w}_2$. Оставшийся лидер $\mathbf{e}_4$ из векторов $\mathbf{w}_4$, $\mathbf{w}_5$ выбирать нельзя, т.к. они уже вошли в смежный класс $\mathbf{w}_2 + C$. В качестве $\mathbf{e}_4$ можно взять вектор 00100. Итак, имеем следующую таблицу лидеров и их синдромов

$\mathbf{e}_i$	$S(\mathbf{e}_i)$
00000	$(0,0)^{\mathrm{T}}$
00001	$(0,1)^{\mathrm{T}}$
00010	$(1,0)^{\mathrm{T}}$
00100	$(1,1)^{\mathrm{T}}$

В некоторых случаях (не в данном) приходится рассматривать вектора из $\mathbb{F}_2^n$ с весами, равными двум и выбирать среди них очередного лидера, если векторов с меньшим весом не хватает для построения таблицы.

Запишем лидеры в первый столбец таблицы лидеров и их смежных классов. Элемент, стоящий в i-й строке и j-м столбце таблицы, равен $\mathbf{y}_{ij} = \mathbf{e}_i + \mathbf{x_j}$. Таким образом, i-я строка таблицы представляет собой смежный класс $\mathbf{e_i} + \mathbf{C}$.

$\mathbf{F_2^3}$	000	001	010	011	100	101	110	111
C	00000	10010	10101	00111	11000	01010	01101	11111
$\mathbf{e}_2 + C$	00001	10011	10100	00110	11001	01011	01100	11110
$\mathbf{e}_3 + C$	00010	10000	10111	00101	11010	01000	01111	11101
$\mathbf{e}_4 + C$	00100	10110	10001	00011	11100	01110	01001	11011

Синдром слова $\mathbf{y} = 11010$, которое нужно декодировать, равен $S(\mathbf{y}) = (1,0)^{\mathrm{T}} = S(\mathbf{e}_3)$, т.е. $\mathbf{y} \in \mathbf{e}_3 + C$, а именно, слово $\mathbf{y}$ находится в 3-й строке и 7-м столбце. Следовательно, с наибольшей вероятностью передано слово $\mathbf{x}_3 = \mathbf{y} - \mathbf{e}_3 = 11000$(иначе - ближайшее к полученному кодовое слово). Соответствующее сообщение представляет собой слово $\mathbf{a} = 100$.

Найдем дуальный (5,2)-код C^*. Порождающей матрицей G^* для этого кода является матрица H, а проверочной — матрица G. Можно привести матрицу G^* элементарными преобразованиями над $\mathbb{F}_2$ к систематическому виду $G^{*\prime} = (E_2| - A^{*T})$. Если $\mathbf{a}^* = (a_1^*, a_2^*)$ — сообщение, тогда соответствующее кодовое слово из дуального кода равно

$$\mathbf{x}^* = (x_1^*, x_2^*, x_3^*, x_4^*, x_5^*) = \mathbf{a}^* H.$$

Приведем таблицу всевозможных сообщений и соответствующих кодовых слов для кода C^*.

$\mathbf{a}^*$	00	01	10	11
$\mathbf{x}^*$	00000	00101	11110	11011

Таким образом, $C^* = \{00000, 00101, 11011, 11110\}$.

Найдем весовые спектры кодов. Отсортируем в порядке возрастания веса.

```
> C1s:=sort(C1,weight_order);
```

$C1s :=$ {(0, 0, 0, 0, 0), (1, 0, 0, 1, 0)], (1, 1, 0, 0, 0), ∗(0, 1, 0, 1, 0), (1, 0, 1, 0, 1),
(0, 0, 1, 1, 1), (0, 1, 1, 0, 1), (1, 1, 1, 1, 1)}

$C^* = \{\mathbf{x}_1^*, \mathbf{x}_2^*, \mathbf{x}_3^*, \mathbf{x}_4^*\}$. Находим веса слов этих кодов:

```
> weight_enumerator_vector(G1,2);

                          [1, 0, 3, 3, 0, 1]
weight_enumerator_vector(H,2);
                          [1, 0, 1, 0, 2, 0]
```

Отсюда имеем следующие весовые спектры для кодов C и C^*:

$$A_0 = 1,\ A_2 = 3,\ A_3 = 3,\ A_5 = 1\ A_1 = A_4 = 0;$$
$$A_0^* = A_2^* = 1, A_4^* = 2,\ A_1^* = A_3^* = A_5^* = 0.$$

Задача 2. Найти *проверочные* и *порождающие* матрицы и *информационные скорости* для (7,4)-кода Хемминга и удлиненного (8,4)-кода Хемминга. Сколько ошибок обнаруживают и исправляют эти коды? Декодировать слова 1101011 и 01011011 в коде Хемминга и его удлиненном коде соответственно.

Решение. Обозначим через H и G соответственно проверочную и порождающую матрицы кода Хемминга C, а через H^* и G^* — проверочную

и порождающую матрицы удлиненного кода Хемминга C^*. Проверочной матрицей $(7,4)$-кода Хемминга является бинарная (над полем $\mathbb{F}_2$) матрица размера 3×7, i-й столбец которой есть двоичная запись числа i(младший разряд может соответствовать как первой, так и последней строкам). Значит,

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

Т.н. *удлиненный* $(8,4)$-код получают добавлением одного проверочного символа x_8 к кодовым словам кода Хемминга и добавлением одного проверочного уравнения $x_1 + x_2 + \ldots + x_8 = 0$ (проверкой на четность). Следовательно, матрица H^* может быть получена из H приписыванием сверху строки $(1,1,1,\ldots,1)$ и справа столбца $(1,0,0,\ldots,0)^{\mathrm{T}}$. Следовательно,

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

Элементарными преобразованиями приводим матрицы H и H^* к каноническому виду $H' = (A \mid E_3)$, $H^{*\prime} = (\overline{A} \mid E_4)$. В результате получаем:

$$H' = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right);$$

$$H^{*\prime} = \left(\begin{array}{cccc|cccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

Следовательно,

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

$$G^* = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right).$$

Строки любой порождающей матрицы, записанной в канонической форме, являются базисом пространства кодовых слов. Далее, кодовые слова удлиненного кода получаются из кодовых слов исходного кода добавлением символа проверки на четность. Следовательно, матрицу G^* можно было получить из G добавлением справа столбца, i-й элемент которого является сумммой всех элементов i-й строки матрицы G (проверкой на четность).

Информационная скорость кода равна отношению числа информационных символов, длины сообщения, к длине кодового слова. Для кода Хемминга C

$$k/n = (2^m - 1 - m)/(2^m - 1) = 3/7,$$

а информационная скорость удлиненного кода Хемминга C^* равна

$$k^*/n = (2^m - m)/2^m = 4/8 = 1/2.$$

Известно, что $d_{\min}(C) = 3$, $d_{\min}(C^*)$=4 , следовательно, код C обнаруживает $d_{\min}(C) - 1 = 2$ ошибки и исправляет $[(d_{\min}(C) - 1)/2] = 1$ ошибку, а код C^* обнаруживает $d_{\min}(C^*) - 1 = 3$ ошибки и исправляет $[(d_{\min}(C^*) - 1)/2] = 1$ ошибку.

Слово $\mathbf{y}_1 = 1101011$ имеет синдром $S_1(\mathbf{y}_1) = H\mathbf{y}_2^{\mathrm{T}} = (1, 1, 0)^{\mathrm{T}}$, который является двоичной записью числа 6, и декодер кода Хемминга решает, что ошибка произошла в 6-й позиции. Следовательно, слову $\mathbf{y}_1$ соответствует кодовое слово $\mathbf{x}_1 = \mathbf{y}_1 - 0000010 = 1101111$, а соответствующее сообщение будет 1101.

Синдром слова $\mathbf{y}_2 = 01011011$ равен

$$S_2(\mathbf{y}_2) = H^*\mathbf{y}_2^{\mathrm{T}} = \begin{pmatrix} \sum\limits_{i=1}^{8} y_i \\ S_1(\mathbf{y}) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

где $\mathbf{y}_2 = y_1y_2 \ldots y_7y_8 = 01011011$, $\mathbf{y} = y_1y_2 \ldots y_7 = 0101101$.

Следовательно, $S_1(\mathbf{y}) = (\mathbf{1}, \mathbf{0}, \mathbf{0})^{\mathrm{T}}$ и ошибка в слове $\mathbf{y}$ произошла в 4-й позиции кодового слова $\mathbf{x} = x_1x_2 \ldots x_7$ кода Хемминга C. Следовательно, $\mathbf{x} = \mathbf{y} - 0001000 = 0100101$. Соответствующее кодовое слово $\mathbf{x}^*$ удлиненного (8,4)-кода Хемминга $\overline{C}$ равно слову $x_1x_2 \ldots x_7x_8 = 01001011$, где $x_8 = \sum\limits_{i=1}^{7} x_i = 1$ — есть символ проверки на четность. Кодовому слову 01001011 соответствует сообщение 0100.

Ответ. H, G, H^*, G^*; инфомационные скорости кодов C и C^* равны соответственно 3/7 и 1/2; код C обнаруживает две ошибки и исправляет

одну ошибку, а код C^* обнаруживает три ошибки и исправляет одну ошибку; 1101111(110), 01001011(010).

==========

Задача 3. Найти порождающую матрицу, все кодовые слова и весовой спектр для линейного тернарного (т.е. над $\mathbb{F}_3$) (4,2)-кода с проверочной матрицей $H = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 \end{pmatrix}$. Выписать все синдромы и лидеры смежных классов и декодировать при помощи лидеров слово 2001. Оценить вероятность правильного декодирования.

Решение. Находим порождающую матрицу, используя известное соотношение между G и H. Элементарными преобразованиями над $\mathbb{F}_3$ приведем порождающую матрицу H кода C к каноническому (систематическому) виду $H' = (A \mid E_2)$, где $A \in (\mathbb{F}_3)^{2\times 2}$. Напомним, что в поле $\mathbb{F}_3$ справедливо следующее: $-1 = 2$, $-2 = 1$, $2 + 2 = 1$, $2 + 1 = 0$, $2 \cdot 2 = 1$, $2^{-1} = 2$.

$$H = \left(\begin{array}{cc|cc} 0 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 \end{array}\right) \underset{\text{прибавим ко } II \text{строке } I,}{\sim} \left(\begin{array}{cc|cc} 0 & 1 & 1 & 1 \\ 1 & 2 & 0 & 2 \end{array}\right) \underset{\text{умножим } II \text{ на } 2^{-1}=2}{\sim}$$

$$\sim \left(\begin{array}{cc|cc} 0 & 1 & 1 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) \underset{I-II}{\sim} \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array}\right) \underset{\text{финиш}}{\sim}$$

$$H' = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array}\right) \quad \begin{matrix} & & A & & E_2 \end{matrix}$$

Значит, $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, $G = (E_2 \mid -A^{\mathrm{T}}) = \left(\begin{array}{cc|cc} 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 2 \end{array}\right)$.

Пусть $\mathbf{a} = (a_1, a_2)$, где $a_1, a_2 \in \mathbb{F}_3$ — некоторое сообщение, тогда соответствующее кодовое слово равно

$$\mathbf{x} = (x_1, x_2, x_3, x_4) = \mathbf{a}G = (a_1, a_2, 2a_1, a_1 + 2a_2).$$

И мы имеем следующее соответствие сообщений и кодовых слов.

a	00	01	02	10	11	12	20	21	22
x	0000	0102	0201	1021	1120	1222	2012	2111	2210

Выберем, учитывая минимальный вес кодовых слов, лидеры $\mathbf{e}_1, \mathbf{e}_2 \ldots,$ $\mathbf{e}_9$ смежных классов. Теперь напишем таблицу лидеров и соответствующих смежных классов. Первая строка — это множество всех кодовых

слов, первый столбец — множество всех лидеров, i-я строка представляет собой смежный класс $\mathbf{e}_i + C$, а элемент, стоящий на пересечении i-й строки и j-го столбца, равен $\mathbf{y}_{ij} = \mathbf{e}_i + \mathbf{x}_j$. Заметим, что при выборе лидеров приходится брать элементы с весом 2, т.к. некоторые элементы с весом 1 уже вошли в перечисленные выше смежные классы.

C	0000	0102	0201	1021	1120	1222	2012	2111	2210
$\mathbf{e}_2 + C$	0001	0100	0202	1022	1121	1220	2010	2112	2211
$\mathbf{e}_3 + C$	0010	0112	0211	1001	1100	1202	2022	2121	2220
$\mathbf{e}_4 + C$	1000	1102	1201	2021	2120	2222	0012	0111	0210
$\mathbf{e}_5 + C$	0002	0101	0200	1020	1122	1221	2011	2110	2212
$\mathbf{e}_6 + C$	0020	0122	0221	1011	1110	1212	2002	2101	2200
$\mathbf{e}_7 + C$	2000	2102	2201	0021	0120	0222	1012	1111	1210
$\mathbf{e}_8 + C$	0011	0110	0212	1002	1101	1200	2020	2122	2221
$\mathbf{e}_9 + C$	1010	1112	1211	2001	2100	2202	0022	0121	0220

Построим синдромную таблицу декодирования. Первый столбец — лидеры. Рядом запишем соответствующие синдромы.

$$S(\mathbf{e}_i) = \mathbf{e}_i \cdot H.$$

$\mathbf{e}_i$	$S(\mathbf{e}_i)$
0000	$(0,0)^{\mathrm{T}}$
0001	$(0,1)^{\mathrm{T}}$
0010	$(1,0)^{\mathrm{T}}$
1000	$(1,2)^{\mathrm{T}}$
0002	$(0,2)^{\mathrm{T}}$
0020	$(2,0)^{\mathrm{T}}$
2000	$(2,1)^{\mathrm{T}}$
0011	$(1,1)^{\mathrm{T}}$
1010	$(2,2)^{\mathrm{T}}$

Слово $\mathbf{y} = 2001$ лежит в 9-й строке и 4-м столбце, следовательно две ошибки не можем исправить.

Минимальное расстояние кода $d_{\min}(C) = 3$. Значит, код C обнаруживает $s = d_{\min}(C) - 1 = 2$ ошибки и исправляет $t = [(d_{\min}(C) - 1)/2] = 1$ ошибку.

Задача 4. Найти проверочные и порождающие матрицы для симплексного (7,3)-кода и (8,4)-кода Рида-Малера первого порядка. Содержат ли слова 0101101 и 11001100 в симплексном коде и в коде Рида-Малера обнаруживаемые ошибки? Оценить вероятность обнаружения ошибки для этих кодов.

Решение. Обозначим через H^* и G^* соответственно проверочную и порождающую матрицы симплексного кода C^*, а через $\overline{H}^*$ и $\overline{G}^*$ — проверочную и порождающую матрицы кода Рида-Малера $\overline{C}^*$ (матрицы G, H, $\overline{G}$, $\overline{H}$, означают то же, что и в задаче 2). Тогда $H^* = G$, $G^* = H$, $\overline{H}^* = \overline{G}$, $\overline{G}^* = \overline{H}$.

Выясним, содержат ли слова $\mathbf{y}_1 = 0101101$, $\mathbf{y}_2 = 11001100$ обнаруживаемые ошибки в кодах C^* и $\overline{C}^*$:

$$S_1(\mathbf{y}_1) = H^*{\mathbf{y}_1}^{\mathrm{T}} = (1,1,1,1)^{\mathrm{T}} \neq (0,0,0,0)^{\mathrm{T}};$$
$$S_2(\mathbf{y}_2) = \overline{H}^*{\mathbf{y}_2}^{\mathrm{T}} = (0,0,0,0)^{\mathrm{T}}.$$

Значит, декодер кода C^* будет выдавать сообщение об ошибке в слове $\mathbf{y}_1$, а декодер кода $\overline{C}^*$ будет считать слово $\mathbf{y}_2$ кодовым словом.

Известно, что $d_{\min}(C^*) = d_{\min}(\overline{C}^*) = 2^{m-1} = 4$ (утверждние **??**), следовательно, коды C^* и $\overline{C}^*$ обнаруживают $s = d_{\min}(C^*) - 1 = 3$ ошибки. Это означает, что для вероятностей P_1, P_2 пропуска ошибки этими кодами (т.е. для вероятностей того, что произошло не более трех ошибок) справедливы неравенства

$$P_1 \geq \sum_{i=0}^{3} \binom{7}{i} p^{n-i}q^i = p^7 + 7p^6q + 21p^5q^2 + 35p^4q^3;$$
$$P_2 \geq \sum_{i=0}^{3} \binom{8}{i} p^{n-i}q^i = p^8 + 8p^7q + 28p^6q^2 + 56p^5q^3.$$

Ответ. $H^* = G$, $G^* = H$, $\overline{H^*} = \overline{G}$, $\overline{G}^* = \overline{H}$ (матрицы G, H, $\overline{G}$, $\overline{H}$ найдены в задаче 2); в слове 0101101 произошла ошибка с вероятностью $P_1 \geq p^7 + 7p^6q + 21p^5q^2 + 35p^4q^3$; в слове 11001100 не произошла ошибка с вероятностью $P_2 \geq p^8 + 8p^7q + 28p^6q^2 + 56p^5q^3$.