Дмитрий Герасимов (4538)
Теория кодирования **Задание 2** 29 ноября 2013 г.

Упражнение 12

Сначала докажем вспомогательное утверждение:

Лемма Пусть у нас есть матрицы $P : k \times n = \begin{bmatrix} I_k & A \end{bmatrix}$ и $Q : n \times k = \begin{bmatrix} B \\ I_{n-k} \end{bmatrix}$. Тогда $PQ = A + B$.

Доказательство. Рассмотрим элемент произведения $(PQ)[i][j] = \sum_{t=1}^{n} P[i][t]Q[t][j]$.

- Заметим, что когда $t \leq k$, все $P[i][t]$ равны 0, кроме $P[i][i]$, равного 1, так как они соответствуют матрице I_k.
- Аналогично, когда $t > k$, все $Q[t][j]$ равны 0, кроме $Q[k + j][j]$, равного 1, так как он соответствует матрице I_{n-k}.

Таким образом, можно записать $(PQ)[i][j] = P[i][i]Q[i][j] + P[i][k + j]Q[k + j][j] = A[i][j] + B[i][j]$, что и требовалось. □

Теперь покажем, что в случае q-арного кода, если матрица G равна $\begin{bmatrix} I_k & P \end{bmatrix}$, то матрицу H можно найти как $H = \begin{bmatrix} -P^\top & I_{n-k} \end{bmatrix}$. Для этого надо умножить G на матрицу $H^\top = \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix}$, и из предыдущего утверждения непосредственно получаем $GH^\top = P - P = 0$, что и требовалось доказать.

Заметим, что для бинарного кода в поле, в котором мы работаем, отрицательный элемент по сложению совпадает с исходным, поэтому $-P = P$, и можно было пользоваться формулой $H = \begin{bmatrix} P^\top & I_{n-k} \end{bmatrix}$

Задача 1

- $(6, 1)$-код с минимальным расстоянием 6, очевидно, это максимально возможное расстояние:
$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$
- Рассмотрим произвольный линейный $(6, 2)$-код. Его минимальное расстояние ограничего границей Синглтона, и не может быть больше пяти, проверим, может ли оно быть равно пяти. Пусть он задан проверочной матрицей H размера 4×6. Его минимальное расстояние равно 5 тогда и только тогда, когда любые 4 из столбцов H линейно независимы, и есть набор из пяти линейно зависимых столбцов. Рассмотрим произвольные четыре ЛНЗ столбца, не теряя общности, пусть это будут столбцы 1, 2, 3, 4. Столбец 5 тогда обязятельно будет раскладываться в линейную комбинацию этих четырех столбцов, так как они образуют базис в пространстве размерности 4 (высота проверочной матрицы), то есть $\mathbf{c_5} = \sum_{i=1}^{4} a_i \mathbf{c_i}$ (где a_i — коэффициент линейной комбинации, а $\mathbf{c_i}$ — столбец проверочной матрицы). Тогда утверждается, что все $a_i = 1$. Пусть это не так,

тогда существует $t \in \{1,2,3,4\}$, что $a_t = 0$. Тогда набор из четырех столбцов $\{\mathbf{c_1}, \mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}\} \setminus \mathbf{c_t} + \mathbf{c_5}$ не будет линейно независимым, так как $\mathbf{c_5}$ раскладывается по $\{\mathbf{c_1}, \mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}\} \setminus \mathbf{c_t}$, получили противоречие. Значит, $\mathbf{c_5} = \mathbf{c_1} + \mathbf{c_2} + \mathbf{c_3} + \mathbf{c_4}$. Но теперь то же рассуждение можно повторить для столбца $\mathbf{c_6}$, и получим, что он равен $\mathbf{c_1} + \mathbf{c_2} + \mathbf{c_3} + \mathbf{c_4} = \mathbf{c_5}$. Таким образом, не любые четыре столбца ЛНЗ, и расстояние кода не может быть равно 5.

Построим код с расстоянием 4, воспользовавшись тем, что если в H все столбцы различны и ненулевые, то минимальное расстояние кода не меньше трех, и если в одной из строк H нет нулей, то минимальное расстояние четно. Приведем $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$

Методом Гаусса приведем ее к систематической форме: $\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$, получим $-P^\top = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$, то есть $P = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$, и в итоге,

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- $(6,3)$-код. Аналогично пункту 2, можно показать, что граница Синглтона $d = 4$ недостижима. Легко можно придумать код с расстоянием 3, воспользовавшись тем, что если в H все столбцы различны и ненулевые, то расстояние кода не меньше трех: $H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$, она уже в систематической форме, и $P^\top = P = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$, то есть

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

- $(6,4)$-код, с минимальным расстоянием 2, граница Синглтона недостижима по рассуждениям, аналогичным пункту 2. Воспользуемся тем, что если в H одна из строк не содержит нулей, то минимальное расстояние кода четно. Пусть $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$, ее систематическая форма — $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$, соот-

ветствующая матрица

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

- $(6, 5)$-код, с минимальным расстоянием 2, большее расстояние нельзя получить по границе Синглтона.

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- $(6, 6)$-код, с минимальным расстоянием 1, большее расстояние нельзя получить по границе Синглтона. Фактически, равносильно отсутствию кодирования.

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Задача 2

Пусть ДСК характеризуется переходной вероятностью p_0

- Без использования кодирования вероятность правильной передачи k информационных бит равна $P_c = (1-p_0)^k$, то есть вероятность ошибки $P_e = 1-(1-p_0)^k$
- С использованием кодирования верная передача n бит кода происходит, когда ошибки произошли в не более, чем $t = \lfloor \frac{d-1}{2} \rfloor$ битах, то есть $P_c = \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} p_0^i (1-p_0)^{n-i}$, тогда $P_e = 1 - P_c = 1 - \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} p_0^i (1-p_0)^{n-i}$

Зависимости вероятности ошибки от p_0 для лучших кодов:

n	2	4	6	8	10	12	14	16	18
k	1	2	3	4	5	6	7	8	9
d	2	2	3	4	4	4	4	5	6
$p_0 = 0.1000$	0.01	0.052	0.11	0.038	0.07	0.11	0.16	0.21	0.098
$p_0 = 0.0100$	0.0001	0.00059	0.0015	5.4e-05	0.00011	0.00021	0.00034	0.00051	2.7e-05
$p_0 = 0.0010$	1e-06	6e-06	1.5e-05	5.6e-08	1.2e-07	2.2e-07	3.6e-07	5.5e-07	3e-09

n	20	22	24	26	28	30	32	34	36
k	10	11	12	13	14	15	16	17	18
d	6	7	8	7	8	8	8	8	8
$p_0 = 0.1000$	0.13	0.17	0.085	0.26	0.14	0.18	0.21	0.25	0.29
$p_0 = 0.0100$	4.3e-05	6.3e-05	3.6e-06	0.00013	8.1e-06	1.2e-05	1.6e-05	2.2e-05	2.9e-05
$p_0 = 0.0010$	4.8e-09	7.2e-09	4.2e-11	1.5e-08	9.6e-11	1.4e-10	2e-10	2.7e-10	3.7e-10

Энергетический выигрыш для $p = 10^{-5}$ рассчитывается как разность энергетических уровней ДСК, необходимых для достижений вероятности ошибки p без декодирования и при декодировании.

Зависимость переходной вероятности ДСК от отношения сигнал-шум на бит: $p_0(\frac{E_0}{N_0}) = \Phi(-\sqrt{2}\sqrt{\frac{E_0}{N_0}})$. Далее подставим эту зависимость в зависимость вероятности ошибки от переходной вероятности в канале, и будем решать уравнение: $P_e(\frac{E_0}{N_0}) = p$ при использовании кодирования и без. Получим:

n	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36
k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
d	2	2	3	4	4	4	4	5	6	6	7	8	7	8	8	8	8	8
Gain	3.9	3.3	3.1	5.1	4.9	4.8	4.6	4.5	5.8	5.7	5.6	6.6	5.5	6.4	6.3	6.2	6.2	6.1

Задача 3, 7

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

1. Возьмем в качестве пяти линейно независимых колонки с номерами 9, 7, 6, 8, 4:

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

   и приведем проверочную матрицу к систематическому виду:

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

   тогда легко получить:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

2. Скорость кода равна $\frac{k}{n} = \frac{4}{9}$
3. Минимальное расстояние кода равно четырем
4. Таблица синдромного декодирования:

00000	000000000
00001	000000001
00010	000000010
00011	000000011
00100	000000100
00101	000000101
00110	000000110
00111	001000000
01000	000001000
01001	000001001
01010	000001010
01011	000001011
01100	000001100
01101	010000000
01110	000100000
01111	000100001
10000	000010000
10001	000010001
10010	000010010
10011	100000000
10100	000010100
10101	000010101
10110	000010110
10111	001010000
11000	000011000
11001	000011001
11010	000011010
11011	100001000
11100	000011100
11101	010010000
11110	000110000
11111	000110001

Задача 8

На самом деле, большинство результатов второго раздела как раз таки сформулированы в терминах линейных пространств, и поэтому не нуждаются в переформулировке.

Некоторые определения и утверждения, которые могут быть обобщены:

- Проверочная матрица вычисляется как $H = \begin{bmatrix} -P^\top & I_r \end{bmatrix}$ (упражнение 12)

- Упражнение 16, пункт А. Остается верным: пусть в H нет нулевых столбцов, тогда любой столбец является линейно независимой совокупностью векторов, воспользовавшись теоремой 2.4 получим, что минимальное расстояние равно двум, или больше.

- Упражнение 16, пункт Б. Необходимо модифицировать, так как он верен только для $q = 2$, приведем контрпример для $q = 3$:

$$H = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

тогда

$$G = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}$$

то есть минимальное расстояние равно двум, хотя все столбцы проверочной матрицы различны.

Необходимо другое условие:

Утверждение Пусть в H все столбцы ненулевые и нет двух различных столбцов, линейная комбинация которых нулевая.Тогда минимальное расстояние кода не меньше трех.

Доказательство. Действительно, никакая совокупность одного столбца и двух столбцов не является линейно зависимой, значит, минимальное расстояние равно трем или более. □

Формулировка утверждения эквивалентна исходной формулировке для случая бинарного кода, так как единственный ненулевой коэффициент при $q = 2$ равен 1, и сумма векторов нулевая тогда и только тогда, когда векторы совпадают.

- Упражнение 16, пункт В. Необходимо модифицировать, контрпример для $q = 3$:

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 0 & 1 \end{bmatrix}$$

тогда

$$G = \begin{bmatrix} 1 & 2 & 2 \end{bmatrix}$$

К сожалению, какого-нибудь разумного обобщения не придумал.

- Определение эквивалентности кодов можно модифицировать и разрешить умножать столбец порождающей матрицы на ненулевой скаляр.

Утверждение Умножение столбца порождающей матрицы G для q-ичного линейного кода на ненулевой скаляр $a \in F_q$ не изменит минимального расстояния кода.

Доказательство. Воспользуемся тем, что для линейного кода минимальное расстояние определяется как минимальный вес ненулевого кодового слова: $d = \min\limits_{\mathbf{c}\in C, \mathbf{c}\neq 0} w(\mathbf{c})$. Пусть умножили столбец j на скаляр a, рассмотрим произвольное кодовое слово $\mathbf{c} = \sum\limits_{i=1}^{n} a_i \mathbf{e_i}$, и его j-й символ, он изменится с $\mathbf{c_j} = \sum\limits_{i=1}^{n} a_i$ на $\mathbf{c'_j} = a\sum\limits_{i=1}^{n} a_i = a\mathbf{c_j}$. Таким образом:

- если $\mathbf{c_j}$ было нулем, то $a\mathbf{c_j}$ также будет нулем.
- если $\mathbf{c_j}$ не было нулем, то $a\mathbf{c_j}$ не может стать нулем, так как это означало бы, что $a\mathbf{c_j}$ делит нацело основание кода q, а так как оно простое по определению поля, над которым мы работаем, это значит, что либо a делит нацело q (чего быть не может, так как $a < q$), либо $\mathbf{c_j}$ делит нацело q (чего быть не может, так как мы предположили, что оно ненулевое).

Значит, вес кодового слова не изменится, и минимальное расстояние также не изменится. □

Задача 9

1. Порождающая матрица $G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

   Этот код действительно является линейным циклическим $(7, 4)$-кодом, так как строки матрицы G линейно независимы, что легко видно из того, что подматрица, соответствующая первым четырем столбцам, верхнетреугольная, то есть G можно привести в систематическую форму, то есть кодовые слова в G являются базисом подпространства размерности 4.

   Покажем теперь, что код, порожденный этой матрицей, будет циклическим, то есть, если он порождает кодовое слово $\mathbf{c}$, то он также порождает его правый сдвиг $\mathbf{c}'$. Пусть кодовое слово $\mathbf{c} = (a_1, a_2, a_3, a_4) \times G = a_1\mathbf{c_1} + a_2\mathbf{c_2} + a_3\mathbf{c_3} + a_4\mathbf{c_4}$. Приведем координатный вектор (b_1, b_2, b_3, b_4), такой, что $(b_1, b_2, b_3, b_4) \times G = \mathbf{c}'$

   Из структуры базисных векторов видно, что

   $$c = (a_1, a_1 + a_2, a_2 + a_3, a_1 + a_3 + a_4, a_2 + a_4, a_3, a_4)$$

   а после сдвига должны получить

   $$c' = (a_4, a_1, a_1 + a_2, a_2 + a_3, a_1 + a_3 + a_4, a_2 + a_4, a_3)$$

   Легко видеть замену координатат: $b_1 = a_1 + a_2$; $b_2 = a_1 + a_4$; $b_3 = a_4$; $b_4 = a_1$, которая приводит к порождению $\mathbf{c}'$, что и требовалось.

2. Минимальное расстояние кода равно трем.

Задача 11

$$G = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Код нетривиален, так как состоит из двух кодовых слов и не эквивалентен коду, порождающая матрица которого единична. Очевидно, код циклический.