Домашнее задание по курсу «Введение в теорию кодирования»

Задача № 1 (1.1). Определить:

1) $|B_k^n|$ – число всех элементов k-го слоя куба B^n;

2) $|B^n|$ – число всех вершин куба B^n.

Решение.

1) $\left|B_k^n\right| = C_k^n$;

2) Число символов алфавита, используемых для кодирования вершин куба $L=2$. Поэтому число всех возможных слов, которыми закодированы все возможные вершины куба,

$$\left|B^n\right| = L^n = 2^n .$$

Или несколько иначе: $\left|B^n\right| = \sum_{k=0}^{n} C_k^n = (1+1)^n = 2^n$.

Этот результат часто формулируется как теорема: число всех подмножеств множества, состоящего из n элементов, равно 2^n (включая пустое подмножество – подмножество, не содержащее ни одного элемента).

Задача №2 (1.2). Определить:

1) $|B_k^n(\boldsymbol{b}_i)|$ – число всех элементов сферы радиуса k с центром в $\boldsymbol{b}_i = \mathbf{0}$;

2) $|S_k^n(\boldsymbol{b}_i)|$ – число всех элементов шара радиуса k с центром в $\boldsymbol{b}_i = \mathbf{0}$.

Решение.

1) $\left|B_k^n(0)\right| = \left|B_k^n\right| = C_k^n$;

2) $\left|S_k^n(0)\right| = \sum_{i=0}^{k} C_n^i$

Заметим, что $\left|S_k^n(\boldsymbol{b}_i)\right| \equiv \left|S_k^n(0)\right|$ для $i = 1, 2, \ldots, \left|B^n\right|$.

Задача №3 (1.7). Показать, что для произвольных векторов $\boldsymbol{x}$, $\boldsymbol{y}$ и $\boldsymbol{z}$ из B^n справедливо соотношение:

$$d(\boldsymbol{x}, \boldsymbol{z}) = d(\boldsymbol{x}\oplus\boldsymbol{y}, \boldsymbol{y}\oplus\boldsymbol{z}).$$

Решение.

Предположим, что x, y и z – произвольные целые числа из $\{0, 1\}$. Покажем непосредственным вычислением, что при этом всегда справедливы соотношения

$$|x - z| = |x\oplus z| = |(x\oplus y)\oplus(x\oplus z)| \qquad (3\text{-}1)$$

(см. табл.3.1)

Таблица 3.1

x	y	z	$\lvert x - z\rvert$	$\lvert x\oplus z\rvert$	$\lvert(x\oplus y)\oplus(x\oplus z)\rvert$
0	0	0	0	0	0
0	0	1	1	1	1
0	1	0	0	0	0
1	0	0	1	1	1
1	1	0	1	1	1
1	0	1	0	0	0
0	1	1	1	1	1
1	1	1	0	0	0

Учитывая (3-1), получим

$$d(\boldsymbol{x}\oplus\boldsymbol{y}, \boldsymbol{y}\oplus\boldsymbol{z}) = \sum_{i=1}^{n}\left|\left(x_i\oplus y_i\right)-\left(y_i\oplus z_i\right)\right| = \sum_{i=1}^{n}\left|\left(x_i\oplus y_i\right)\oplus\left(y_i\oplus z_i\right)\right| = \sum_{i=1}^{n}\left|x_i - z_i\right| = d(\boldsymbol{x}, \boldsymbol{z}).$$

Задача №4 (1.11). Ниже приведены подклассы кодов из класса блоковых групповых кодов с проверкой на чётность с одинаковыми параметрами:

1) n и k,
2) n и $d_{\min}$,
3) k и $d_{\min}$.

Какой в каждом из перечисленных подклассов 1), 2) и 3) код более предпочтителен?

Решение.

1) Среди кодов с одинаковыми параметрами n и k наиболее предпочтителен код, имеющий *наибольшее кодовое расстояние* $d_{\min}$;
2) Среди кодов с одинаковыми параметрами n и $d_{\min}$ более предпочтителен код, имеющий наибольшее число информационных символов k и, следовательно, обладающий наибольшим значением $N=2^k$ и $R=k/n$;
3) Среди кодов с одинаковыми параметрами k и $d_{\min}$ более предпочтителен код, имеющий наименьшую длину кодовых комбинаций, и, следовательно, обладающий наибольшим значением $R=k/n$.

Задача №5 (1.12). Ниже приведены различные двоичные пятизначные блоковые коды. Требуется:

- определить вид кода;
- охарактеризовать потенциальные обнаруживающую и исправляющую способности кода; определить параметры d_{min} и R кода;
- произвести сравнение приведенных кодов как корректирующих.

1) (5, 1)-код:

$$\boldsymbol{H}_{(5,\,1)} = \begin{bmatrix} 11000 \\ 10100 \\ 10010 \\ 11001 \end{bmatrix}$$

2) 00011 00101 00110 01001 01010 01100 10001 10010 10100 11000

3) (5, 2)-код:

$$\boldsymbol{H}_{(5,\,2)} = \begin{bmatrix} 11100 \\ 10010 \\ 01001 \end{bmatrix}$$

4) (5, 3)-код:

$$\boldsymbol{H}_{(5,\,3)} = \begin{bmatrix} 11010 \\ 01101 \end{bmatrix}$$

5) 00001 00010 00100 01000 10000

6) (5,4)-код:

$$\boldsymbol{H}_{(5,\,4)} = \begin{bmatrix} 11111 \end{bmatrix}$$

Решение. См. табл. 3.2.

Таблица 3.2

№	Заданный код	Вид заданного кода	Параметры заданного кода	$d_{\min}$, R
1	(5,1)-код $G_{(5,1)} = [I_1 R_{1\times4}]$ $H_{(5,1)} = [R^T_{1\times4} I_4]$	Двоичный линейный (групповой) пятизначный (5,1) код; код с повторением	L=2; N_0=32; n=5; k=1; r=4	N=2; $d_{\min}$=5; R=1/5=0.20
2	00011 00101 00110 01001 01010 01100 10001 10010 10100 11000	Двоичный пятизначный нелинейный равновесный код «2 из 5». Применяется при несимметричных ошибках.	L=2; N_0=32; n=5	N=10; $d_{\min}$=2; R=ld(10)/5=0.664
3	(5,2)-код $G_{(5,2)} = [I_2 R_{2\times3}]$ $H_{(5,2)} = [R^T_{2\times3} I_3]$	Двоичный пятизначный линейный (групповой) (5,2)-код	L=2; N_0=32; n=5; k=2; r=3	N=4; $d_{\min}$=3; R=2/5=0.40
4	(5,3)-код $G_{(5,3)} = [I_3 R_{3\times2}]$ $H_{(5,3)} = [R^T_{3\times2} I_2]$	Двоичный пятизначный линейный (групповой) (5,3)-код	L=2; N_0=32; n=5; k=3; r=2	N=8; $d_{\min}$=2; R=3/5=0.60
5	00001 00010 00100 01000 10000	Двоичный пятизначный нелинейный эквидистантный и равновесный код «1 из 5»	L=2; N_0=32; n=5	N=5; $d_{\min}$=2; R=ld(5)/5=0.464
6	(5,4)-код $G_{(5,4)} = [I_4 R_{4\times1}]$ $H_{(5,4)} = [R^T_{4\times1} I_1]$	Двоичный пятизначный линейный (групповой) (5,4)-код, код с общей проверкой (со стиранием и возможно с переспросом)	L=2; N_0=32; n=5; k=4; r=1	N=16; $d_{\min}$=2; R=4/5=0.80

Код №1 обладает самой высокой исправляющей способностью ($d_{\min}$=5, t=2, s=4); второе место после него занимает код №3 ($d_{\min}$=3, t=1, s=2).

Коды №№ 2, 4, 5 и 6 ($d_{\min}$=2) позволяют только обнаруживать, но не исправлять ошибки.

Код №6 обладает самой высокой скоростью (R=0.8); код №1 обладает самой низкой скоростью (R=0.2).

Задача №6 (1.13). Пусть вероятность искажения одиночного символа в ДСК $p = 0.01$. Определить вероятность появления q-кратной ошибки на выходе ДСК $P(q)$, q=0, 1, …, 5 при условии, что используемый с ДСК код является двоичным пятизначным, а передаваемые по каналу сообщения являются равновероятными. Определить математическое ожидание и среднеквадратическое отклонение (с.к.о) кратности ошибки q.

Решение (Maple 9).

Начальные условия:

$$p := 0.01$$

$$q := [0, 1, 2, 3, 4, 5]$$

Формула для расчета вероятности q-кратной ошибки:

$$P := (p, q) \to \frac{5!\, p^q\, (1-p)^{(5-q)}}{q!\, (5-q)!}$$

Вероятности ошибок кратности от 0 до 5:

$$\mathrm{P}(0) = 0.9509900499$$

$$\mathrm{P}(1) = 0.0480298005$$

$$\mathrm{P}(2) = 0.0009702990$$

$$\mathrm{P}(3) = 0.98010\ 10^{-5}$$

$$\mathrm{P}(4) = 0.495\ 10^{-7}$$

$$\mathrm{P}(5) = 0.1\ 10^{-9}$$

Математическое ожидание кратности ошибки:

$$Mq = \sum_{q=0}^{5} q\, \mathrm{P}(q)$$

$$Mq := 0.05000000000$$

Дисперсия кратности ошибки:

$$Dq = \sum_{q=0}^{5} \mathrm{P}(q)\, (q - Mq)^2$$

$$Dq := 0.04950000000$$

Среднеквадратичное отклонение кратности ошибки:

$$Sq = \sqrt{Dq}$$

$$Sq := 0.2224859546$$

Задача №7 (1.14). Какие предпосылки:

1) о свойствах передаваемых сообщений или о свойствах двоичных кодовых слов, поступающих на вход канала,

2) о свойствах канала,

3) о методе декодирования на приёмном конце канала

необходимы для обоснования оптимальности метода декодирования по максимуму правдоподобия (декодирование принятой комбинации $\boldsymbol{y}$ в ближайшую кодовую комбинацию в смысле расстояния Хэмминга) и почему?

Решение.
1) Кодовые слова, поступающие на вход канала (а, следовательно, и передаваемые сообщения) должны быть ***равновероятными.***
2) Канал должен быть каналом ***без памяти*** (СБПК). При этом в выходных последовательностях символов длины n ошибки будут ***статистически независимыми***.
3) Если p_0 – вероятность искажения двоичных символов в ДСК, то должно выполняться ***соотношение:*** $p_0 < 0.5$ (на практике $p_0 << 1$); отсюда следует, что низкократные ошибки являются более вероятными.
Вывод: при выполнении условий, указанных в пп. 1), 2) и 3) справедливо соотношение:

$$p(\bar{y},\bar{a}_s) = p_0^{d(\bar{y},\bar{a}_s)} \cdot (1-p_0)^{(n-d(\bar{y},\bar{a}_s))} = p_0^{w(\bar{e}_i)} \cdot (1-p_0)^{(n-w(\bar{e}_i))} \quad (1\text{-}14\text{-}1),$$

где $\boldsymbol{a}_s$ – переданная по ДСК кодовая комбинация, $\boldsymbol{y}$ – принятая на его выходе комбинация, $\boldsymbol{e}_i$ – ошибка, обусловившая преобразование $\boldsymbol{a}_s$ в $\boldsymbol{y}$.
Таким образом, наилучшим способом декодирования полученной на выходе канала комбинации, содержащей ошибки, является ее декодирование в ближайшую в смысле расстояния Хемминга кодовую комбинацию (т.е. декодирование по максимуму правдоподобия).

Задача №8 (1.15). Показать, что если на вход ДСК поступают статистически независимые *неравновероятные кодовые слова* $\boldsymbol{x}_i$, i=1, 2, …, N, то вывод (в решении задачи **1.14**), вообще говоря, не является обоснованным.

Решение. Если сообщения не являются равновероятными, то соотношение (1-14-1) уже не имеет места и, следовательно, вывод, сделанный в решении задачи 1.14, уже не является обоснованным.
Заметим также, что равномерное распределение $p(\mathbf{x}_i)=1/N$, i=1, 2, …, N, максимизирует скорость передачи информации; при этом $R=ld(N)/n$ [бит/симв].

Задача №9 (1.23). Показать, что если код с минимальным расстоянием Хэмминга e+1 между кодовыми блоками используется для канала со стиранием, то можно декодировать таким образом, что будут исправлены все комбинации из e (или меньше) стираний, но не все комбинации из e+1 стираний.

Решение. Согласно условию задачи, $d_{\min} = e+1$. Для того, чтобы корректирующий код гарантированно обнаруживал все ошибки кратности, не превышающей s, необходимо и достаточно, чтобы выполнялось условие $d_{\min} \geq s+1$. В рассматриваемом случае исправление эквивалентно обнаружению и поэтому, если требуется исправить e+1 стирание, то необходимо, чтобы выполнялось неравенство $d_{\min} \geq e+2$. Но тогда код с $d_{\min} = e+1$ способен исправить только e стираний.

Задача №10 (1.24). Показать, что для исправления всех комбинаций из t ошибок и e стираний необходимо и достаточно, чтобы минимальное расстояние Хэмминга между двоичными кодовыми блоками равнялось, по крайней мере, $2t+e+1$.

Решение. Согласно условию задачи, $d_{\min} = 2t+e+1$. Для декодера стирание – это ошибка, позиция которой известна, а значение может быть, а может и не быть нулевым.
Сначала декодер пытается декодировать принятое слово, подставив на место стираний некоторые произвольные значения, например, нулевые. Затем декодер заменяет первоначальные предположительные значения стираний на их дополнения и вновь декодирует.
Если f, $0 \le f \le e$, первоначальных предположительных стираний оказались неверными, то $(e - f)$ значений их дополнений будут также неверными. Так как $\min(f, e\text{-}f) \le e/2$, то в одном из этих 2-х случаев общее число ошибок не будет превышать $(d_{\min} - 1)/2$ и их можно будет исправить.

Задача №11 (2.1). Показать, что число двоичных векторов из B^n , представимых линейными комбинациями вида

$$\lambda_1 \boldsymbol{x}_1 + \lambda_2 \boldsymbol{x}_2 + \ldots + \lambda_s \boldsymbol{x}_s \,, \qquad (2\text{-}1\text{-}1)$$

в которых $\sum_{i=1}^{s} \lambda_i \le t$, а $\{\boldsymbol{x}_i\}$ – совокупность линейно независимых комбинаций, не превосходит $\sum_{i=0}^{t} C_s^i$.

Рекомендуется решить эту же задачу, отказавшись от условия линейной независимости комбинаций $\{\boldsymbol{x}_i\}$, $i = 1, 2, \ldots, s$.

Решение. Из условия задачи следует, что $0 \le t \le s \le n$. Искомое число двоичных векторов из B^n равно числу всевозможных двоичных комбинаций $\{\lambda_1, \lambda_2, \ldots, \lambda_s\}$ веса t; $0 \le t \le s$. Очевидно, что число векторов из B^n не превосходит $\sum_{i=0}^{t} C_s^i \le 2^s \le 2^n$.

При отсутствии условия линейной независимости комбинаций $\{\boldsymbol{x}_i\}$, $i = 1, 2, \ldots, s$, число двоичных векторов из B^n уменьшается по сравнению со случаем наличия условия линейной независимости этих комбинаций.

Задача №12 (2.2). Показать, что кодовые слова чётного веса двоичного группового (n, k)-кода C образуют подгруппу.

Решение. Пусть $C_ч$ – множество кодовых комбинаций двоичного группового (n, k)-кода четного веса, в котором определена основная операция – поэлементное сложение по mod 2 кодовых комбинаций.
Сумма двух комбинаций четного веса есть комбинация четного веса. Каждая комбинация $C_ч$ относительно операции сложения кодовых комбинаций является обратным элементом самой себе. Следовательно, в $C_ч$ имеет место свойство замкнутости и имеется единичный элемент, а этого как раз достаточно, чтобы утверждать, что кодовые комбинации четного веса двоичного группового (n, k)-кода образуют подгруппу группы C.

Задача №13 (2.3). Показать, что в каждом двоичном линейном коде либо каждый кодовый вектор имеет чётный вес, либо половина кодовых векторов имеет чётные веса и половина – нечётные.

Решение. Решение данной задачи начнём с констатации следующих фактов.
Кодовая комбинация нулевого веса имеет чётный вес; любая кодовая комбинация нечётного веса имеет не нулевой
вес,
Если поэлементно суммируются по mod 2 две комбинации из B^n веса w_1 и w_2, то вес получившейся комбинации (комбинации-«суммы») выражается соотношением

$$w = w_1 + w_2 - 2p, \qquad (2\text{-}3\text{-}1)$$

где p - суммарное число одних и тех же позиций суммируемых комбинаций, в которых эти комбинации имеют единицы; эти единицы при суммировании по mod 2 дают нули и, следовательно, выбывают из числа единиц, учитываемых при определении веса комбинации-«суммы».
Из (4-28) вытекают следующие факты:

1. вес комбинации-«суммы» двух комбинаций чётного веса является чётным;
2. вес комбинации-«суммы» двух комбинаций нечётного веса является чётным;
3. вес комбинации-«суммы» двух комбинаций, одна из которых имеет чётный вес, а другая – нечётный, является нечётным.
4. Если все кодовые комбинации - строки порождающей матрицы $G_{(n,k)}$ группового (n, k)-кода имеют чётный вес, то все кодовые комбинации этою кода имеют чётный вес. Действительно, так как каждая комбинация кода может быть представлена как линейная комбинация k строк порождающей матрицы и, учитывая п.1, можно утверждать, что п.4 верен.
5. Если все кодовые комбинации группового (n, k)-кода имеют чётный нес, то все строки порождающей матрицы $G_{(n,k)}$ этого кода имеют чётный вес.
   Очевидно, так как строки порождающей матрицы являются кодовыми комбинациями, образующими базис линейного подпространства.
6. Если среди кодовых комбинаций группового (n, k)-кода имеются комбинации нечётного веса, то его порождающая матрица $G_{(n,k)}$ имеет, по крайней мере, одну кодовую комбинацию – строку нечётного веса.
   Действительно, если предположить противное, т.е. допустить, что все строки порождающей матрицы имеют чётный вес, то получим противоречие, ибо согласно п.4 все кодовые комбинации группового (n, k)-кода в этом случае должны иметь чётный вес.
7. Если среди кодовых комбинаций – строк порождающей матрицы $G_{(n,k)}$ группового (n, k)-кода имеется хотя бы одна комбинации нечётного веса, то половина комбинаций группового (n, k)-кода имеют чётный вес, и половина комбинаций имеют нечётный вес.

Пусть $\boldsymbol{y}_1$, $\boldsymbol{y}_2$, …, $\boldsymbol{y}_k$ - кодовые комбинации - строки порождающей матрицы $G_{(n,k)}$. Произвольная кодовая комбинация группового (n, k)-кода

$$\boldsymbol{y} = \alpha_1 \boldsymbol{y}_1 + \alpha_2 \boldsymbol{y}_2 + \ldots + \boldsymbol{y}_k \qquad (2\text{-}3\text{-}2)$$

где $\{\alpha_1, \ldots, \alpha_k\}$ - некоторое множество двоичных чисел. Предположим, что $\boldsymbol{y}_1$ имеет нечётный вес. Так как, согласно (4-29), $\boldsymbol{y}_1$ входит (при $\alpha_1 = 1$) ровно в половину кодовых комбинаций группового кода и не входит (при $\alpha_1 = 0$) ровно в половину кодовых комбинаций группового кода, то, согласно п.3, ровно половина кодовых комбинаций группового (n, k)-кода имеют чётный вес и ровно половина имеют нечётный вес.
Таким образом, предложенная задача решена.

Задача №14 (2.4). Убедиться, что множество всех кодовых слов чётного веса $C_ч$ группового (n, k)-кода C есть подпространство и найти смежные классы кода C по этому подпространству.

Решение. Из решения задачи 2.2 следует, что $C_ч$ является подгруппой группы C, а следовательно, и подпространством пространства C.
Рассмотрим два случая.

1) Все 2^k кодовые комбинации группового (n, k)-кода имеют чётный вес. В этом случае имеется один смежный класс разложения C по $C_ч$, содержащий 2^k элементов - кодовые комбинации чётного веса; лидером этого смежного класса является кодовое слово нулевого веса.

2) Одна половина кодовых комбинаций группового (n, k)-кода имеют чётный вес и другая половина - нечётный вес. В этом случае имеется два смежных класса разложения C по $C_ч$, каждый из которых содержит 2^{k-1} элемента: первый класс содержит все кодовые комбинации чётного веса, и второй класс - все кодовые комбинации нечётного веса. Лидером первого смежного класса является кодовое слово нулевого веса.

Задача №15 (2.5). Проверить утверждение: множество всех кодовых слов группового (n, k)-кода, содержащих 0 в некоторой фиксированной позиции, есть подпространство. Найти разложение (n, k)-кода на смежные классы по этому подпространству. Проверку провести на примере (5, 3)-кода.

Решение.

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

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

$$C=\begin{pmatrix}0&0&0&0&0\\0&0&1&0&1\\0&1&0&1&1\\0&1&1&1&0\\1&0&0&1&0\\1&0&1&1&1\\1&1&0&0&1\\1&1&1&0&0\end{pmatrix};$$

$\mathbf{v}_0$ = (00000); $\mathbf{v}_1$ = (00101); $\mathbf{v}_2$ = (01011); $\mathbf{v}_3$ = (01110);
$\mathbf{v}_4$ = (10010); $\mathbf{v}_5$ = (10111); $\mathbf{v}_6$ = (11001); $\mathbf{v}_7$ = (11100);

Разложение кода по подпространству:

$\mathbf{v}_0$	$\mathbf{v}_1$	$\mathbf{v}_2$	$\mathbf{v}_3$
$\mathbf{v}_4$	$\mathbf{v}_5$	$\mathbf{v}_6$	$\mathbf{v}_7$

$\mathbf{v}_0+\mathbf{v}_4$ = (10010)

Задача №16 (2.6). Может ли порождающая матрица группового (n, k)-кода иметь:

a) нулевую вектор-строку,

b) нулевой вектор-столбец?

Решение.

a) По определению порождающей матрицы её строки являются базисными кодовыми комбинациями k-мерного подпространства (n-мерного пространства) - линейного (n, k)-кода и, следовательно, являются ненулевыми комбинациями.

b) Если бы некоторый i-й столбец порождающей матрицы линейного (n, k)-кода был нулевым, то тот же самый i-й столбец кодовой матрицы C также был бы нулевым. Но в этом случае, вычеркнув нулевой столбец матрицы C, мы получили бы код с тем же кодовым расстоянием, но меньшей длины.

Задача №18 (2.11). Показать, что если систематический (n, k)-код с проверкой на чётность имеет нечётный минимальный кодовый вес $d_{\text{мин}}$, то добавление ко всем его словам одного проверочного символа и модификация порождающей G и проверочной H матриц с сохранением их канонических форм создаёт новый систематический (n + 1, k)-код с проверкой на чётность с кодовым весом $d^*_{\text{мин}} = d_{\text{мин}} + 1$.

Решение. Структура нового кода вытекает из описания его порождающей матрицы.
Порождающая матрица нового кода G* размерности $k\times(n+1)$ отличается от старой матрицы G размерности $k\times n$ одним (например, последним) *дополнительным столбцом,* содержащим дополнительные проверочные элементы векторов-строк новой порождающей матрицы.
Если проверочная матрица исходного кода H имеет размерность $(n\text{-}k)\times n$, то проверочная матрица нового кода H^* размерности $(n\text{-}k+1)\times(n+1)$ в этом случае имеет структуру, представленную на рисунке:

$$\begin{array}{|c|c|}\hline & 0 \\ & 0 \\ & 0 \\ H & \cdot \\ & \cdot \\ & \cdot \\ & 0 \\ \hline 1\ 1\ 1\ 0 \ldots 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 & 1 \\ \hline \end{array}$$

В *нижней строке* матрицы H, считая слева направо, идут сначала k символов, совпадающих с символами, считая сверху вниз, последнего столбца порождающей матрицы G*, затем идут $n\text{-}k$ нулей и затем (в последнем столбце матрицы) идёт одна единица. Ниже приведен пример для исходного (5, 2)-кода с $d_{\min} = 3$ и для модифицированного (6, 2)-кода с $d_{\min} = 4$.

```
%Функция, вычисляющая проверочную матрицу
%по порождающей матрице
function H = Make_H_matrix(G)
    [k,n]=size(G);
    R=G(:,(k+1):n);
    H=[R' eye(n-k)];
end

%Функция, вычисляющая кодовые комбинации
%и минимальное Хеммингово расстояние
%по порождающей матрице
function [C, d_min] = Make_C_matrix(G)
    [k,n]=size(G)
    R=G(:,(k+1):n)
    for i=1:k
        C_col=null(1,1);
        for j=1:(2^(i-1))
            len=2^(k-i);
            C_col=[C_col zeros(1,len) ones(1,len)];
        end;
        C(i,:) = C_col;
    end
    C=C';
    N=2^k;
    for i=1:N
        message=C(i,:);
        res_str=zeros(1,n-k);
        for j=1:k
            if message(j)==1
                res_str=mod(res_str+R(j,:),2);
            end
        end
        C_R(i,:)=res_str;
    end
    C=[C C_R];
    d_min=n;
    for i=1:N
        for j=(i+1):N
            d=sum(mod(C(i,:)+C(j,:),2));
            if d<d_min
                d_min=d;
            end
        end
    end
end
```

```
%Вычисления:
>> G=[1 0 1 0 1; 0 1 0 1 1]

G =
     1     0     1     0     1
     0     1     0     1     1

>> H=Make_H_matrix(G)

H =
     1     0     1     0     0
     0     1     0     1     0
     1     1     0     0     1

>> [C d_min]=Make_C_matrix(G)

C =
     0     0     0     0     0
     0     1     0     1     1
     1     0     1     0     1
     1     1     1     1     0

d_min =
     3

>> [k,n]=size(G); G1=[G ones(k,1)]

G1 =
     1     0     1     0     1     1
     0     1     0     1     1     1

>> H1=Make_H_matrix(G1)

H1 =
     1     0     1     0     0     0
     0     1     0     1     0     0
     1     1     0     0     1     0
     1     1     0     0     0     1

>> [C1 d1_min]=Make_C_matrix(G1)

C1 =
     0     0     0     0     0     0
     0     1     0     1     1     1
     1     0     1     0     1     1
     1     1     1     1     0     0

d1_min =
     4
```

Задача №22 (2.12). Доказать, что код с повторением и код с общей проверкой на чётность – дуальные друг к другу коды.

Решение. Код с повторением – это (n, 1)-код, а код с общей проверкой на четность - (n, n-1)-код. Отсюда следует, что между порождающими и проверочными матрицами этих кодов имеют место соотношения:

$$G_{(n,1)} = \left[I_1 R_{1\times(n-1)}\right] = \left[R^T_{(n-1)\times 1} I_1\right] = H_{(n,n-1)}$$

$$G_{(n,n-1)} = \left[I_{n-1} R_{(n-1)\times 1}\right] = \left[R^T_{1\times(n-1)} I_{(n-1)}\right] = H_{(n,1)}$$