ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 1**

УДК 621.391.1 : 519.725

© 2022 г. **Л.А. Бассалыго, В.А. Зиновьев, В.С. Лебедев**

СЛАБО РАЗРЕШИМЫЕ БЛОК-СХЕМЫ И НЕДВОИЧНЫЕ КОДЫ, ЛЕЖАЩИЕ НА ГРАНИЦЕ ДЖОНСОНА[1]

Указаны два новых семейства разрешимых блок-схем. Дано определение слабо разрешимой блок-схемы и доказана эквивалентность такой схемы и недвоичных кодов, лежащих на границе Джонсона. Построено новое семейство таких кодов.

Ключевые слова: разрешимая блок-схема, слабо разрешимая блок-схема, недвоичный код, граница Джонсона.

DOI: 10.31857/S0555292322010016

1. Блок-схемой $B(v,k,\lambda)$ называется такое размещение v различных элементов $a_1,\ldots,a_v$ по b блокам $B_1,\ldots,B_b$, при котором каждый блок содержит ровно k различных элементов, каждый элемент принадлежит ровно r блокам, и каждая пара различных элементов a_i,a_j, $i\neq j$, принадлежит ровно λ блокам. Параметры v,k,λ блок-схемы однозначно определяют параметры b и r (см. [1]):

$$b=\frac{\lambda v(v-1)}{k(k-1)},\quad r=\frac{\lambda(v-1)}{k-1}.$$

Блок-схема полностью описывается своей матрицей инцидентности $A=[a_{ij}]$, где

$$a_{ij}=\begin{cases}1, & \text{если } a_i\in B_j,\\ 0, & \text{если } a_i\notin B_j,\end{cases}$$

$i=1,\ldots,v$, $j=1,\ldots,b$.

Блок-схема $B(v,k,\lambda)$ называется разрешимой и обозначается через $RB(v,k,\lambda)$, если ее матрица инцидентности может быть приведена перестановкой строк (что соответствует перенумерации элементов блок-схемы) и столбцов (что соответствует перенумерации блоков) к следующему виду:

$$A=[A_1\,|\,A_2\,|\ldots|\,A_r],\tag{1}$$

где каждая подматрица A_j размера $v\times\dfrac{v}{k}$ состоит из строк веса 1. Построение новых разрешимых блок-схем зиждется на следующем результате из [2].

Т е о р е м а 1. *Существование $RB(v,k,\lambda)$-схемы эквивалентно существованию q-ичного эквидистантного кода мощности N длины n с расстоянием d, лежащего*

[1] Работа выполнена в ИППИ РАН при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364) и Национального научного фонда Болгарии (номер гранта 20-51-18002).

на границе Плоткина

$$N \leqslant \frac{qd}{qd-(q-1)n},$$

где

$$q=\frac{v}{k}, \quad N=v, \quad n=r=\frac{\lambda(v-1)}{k-1}, \quad d=r-\lambda=\frac{\lambda(v-k)}{k-1}.$$

Доказательство этой теоремы в [2] использует естественное преобразование матрицы инцидентности схемы в q-ичный код и столь же естественное обратное преобразование. Поэтому построение новых разрешимых схем эквивалентно построению новых q-ичных кодов, лежащих на границе Плоткина. Здесь мы предложим процедуру построения нового класса таких четверичных кодов из $B(v,k,\lambda)$-схем, являющуюся обобщением процедуры из работы [3].

Утверждение 1. *Любая блок-схема $B(v,k,\lambda)$ порождает четверичный равновесный эквидистантный код с параметрами*

$$N=v, \quad n=\binom{b}{3}, \quad w=\frac{r(b-2)(b-r)}{2}, \quad d=(b-2)(r-\lambda)(b-2(r-\lambda)). \tag{2}$$

Доказательство. Построение кода весьма просто: выбираются любые три столбца матрицы инцидентности блок-схемы (таковых $\binom{b}{3}$) и заменяются на один столбец q-ичного кода по следующему правилу:

$$\begin{aligned}
&(0,0,0),(1,1,1)\to 0, \quad (0,0,1),(1,1,0)\to 1,\\
&(0,1,0),(1,0,1)\to 2, \quad (1,0,0),(0,1,1)\to 3,
\end{aligned}$$

так что в результате получаем четверичный код. Очевидно, что построенный код имеет дину $n=\binom{b}{3}$ и число слов $N=v$. Нетрудно проверить, что расстояние между любыми двумя кодовыми словами равно

$$\begin{aligned}
&\binom{b-2(r-\lambda)}{2}\binom{2(r-\lambda)}{1}+\binom{b-2(r-\lambda)}{1}\binom{2(r-\lambda)}{2}=\\
&=(b-2)(r-\lambda)(b-2(r-\lambda),
\end{aligned}$$

а вес кодовых слов равен

$$\binom{b}{3}-\binom{r}{3}-\binom{b-r}{3}=\frac{r(b-2)(b-r)}{2}. \quad \blacktriangle$$

Если в качестве схемы $B(v,k,\lambda)$ выбрать симметричную (т.е. такую, в которой $b=v$ и $r=k$) схему $B(4t-1,2t,t)$ (полученную из $(0,1)$-матрицы Адамара с нулевой строкой и нулевым столбцом выкидыванием этой строки и этого столбца), то получим четверичный код с параметрами

$$N=4t-1, \quad n=\frac{(4t-1)(2t-1)(4t-3)}{3}, \quad w=d=t(2t-1)(4t-3). \tag{3}$$

Присоединив к коду нулевое слово, получим эквидистантный код, лежащий на границе Плоткина:

$$4t=\frac{4t(2t-1)(4t-3)}{4t(2t-1)(4t-3)-(4t-1)(2t-1)(4t-3)}.$$

В [3], а еще ранее в [4] с помощью выбора любых двух столбцов матрицы инцидентности из схемы $B(4t-1, 2t, t)$ был построен другой четверичный код, лежащий на границе Плоткина, с параметрами

$$N = 4t, \quad n = (4t-1)(2t-1), \quad d = 3t(2t-1).$$

Воспользовавшись теоремой 1 из [2], получаем следующее

Утверждение 2. *Любая блок-схема $B(4t-1, 2t, t)$ порождает две разрешимые блок-схемы*:

$$RB(4t, t, (t-1)(2t-1)) \quad \textit{и} \quad RB(4t, t, (t-1)(2t-1)(4t-3)/3).$$

Замечание 1. Казалось естественным продолжить такую конструкцию, выбирая любые четыре (или даже больше) столбца матрицы инцидентности симметричной схемы $B(4t-1, 2t, t)$, но уже выбор четырех столбцов не привел к кодам, лежащим на границе Плоткина, а следовательно, и к новым разрешимым схемам.

2. Теорема 1 указывает на взаимосвязь разрешимой схемы и недвоичных кодов, лежащих на границе Плоткина. Теперь мы хотим слегка обобщить понятие разрешимой схемы, чтобы установить аналогичную взаимосвязь между этим обобщением и недвоичными равновесными кодами, лежащими на границе Джонсона [5]

$$N \leqslant \frac{(q-1)dn}{qw^2 - (q-1)(2w-d)n}, \tag{4}$$

где N – мощность кода, n – его длина, d – кодовое расстояние, w – вес кодового слова.

Предлагаемое обобщение отличается от разрешимой схемы $RB(v, k, \lambda)$ только в одном: в разрешимой схеме каждый столбец подматриц A_j, $j = 1, 2, \ldots, r$, содержит ровно k единиц, а в слабо разрешимой $WRB_m(v, k, \lambda)$-схеме один столбец подматрицы A_j, $j = 1, 2, \ldots, r$, содержит m единиц, $m \geqslant 1$. Очевидно, что при $m = k$ слабо разрешимая схема превращается в разрешимую. В слабо разрешимой схеме каждая подматрица A_j, $j = 1, 2, \ldots, r$, имеет размер $v \times \dfrac{v-m+k}{k}$, а параметр r (число блоков, которым принадлежит каждый элемент, что для разрешимых схем совпадает с числом подматриц A_j или, что то же самое, с весом каждой строки матрицы A) определяется следующим соотношением:

$$\lambda\binom{v}{2} = r\left(\binom{m}{2} + \frac{v-m}{k}\binom{k}{2}\right). \tag{5}$$

Это соотношение доказывается стандартным образом: скалярное произведение любых двух различных строк матрицы A по определению равно λ, а число пар строк равно $\dbinom{v}{2}$. С другой стороны, сумма скалярных произведений попарных строк в любой подматрице A_j равна

$$\binom{m}{2} + \frac{v-m}{k}\binom{k}{2},$$

а число матриц A_j равно r. Следовательно,

$$r = \frac{\lambda\dbinom{v}{2}}{\dbinom{m}{2} + \dfrac{v-m}{k}\dbinom{k}{2}}. \tag{6}$$

Теперь мы уже можем сформулировать аналог теоремы 1.

Т е о р е м а 2. *Существование слабо разрешимой $WRB_m(v,k,\lambda)$-схемы эквивалентно существованию q-ичного эквидистантного кода мощности N длины n с расстоянием d, лежащего на границе Джонсона* (4), *где параметры схемы и кода связаны следующими равенствами*:

$$q = \frac{v-m+k}{k}, \quad n = r = \frac{\lambda v(v-1)}{m(m-1)+(v-m)(k-1)},$$
$$N = v, \quad d = r-\lambda, \quad w = \frac{r(v-m)}{v}. \tag{7}$$

Д о к а з а т е л ь с т в о. Доказательство теоремы очевидно. Без ограничения общности можно считать, что в каждой подматрице A_j столбец с m единицами стоит на первом месте. Установим следующее взаимно-однозначное соответствие между строками подматриц (их длина равна $(v-m+k)/k$) и символами алфавита $0,1,\ldots,q-1 = (v-m)/k$: строке $(1,0,\ldots,0)$ поставим в соответствие 0, а строке с единицей на i-м месте – символ $i-1$, где $i>1$. При таком соответствии каждый ненулевой символ встретится в столбце кода k раз, а нуль – m раз (такой код мы назвали посимвольно равномерным [3]). Очевидно, что полученный код эквидистантен и $d=r-\lambda$. Согласно [3, утверждение 1] код лежит на границе Джонсона тогда и только тогда, когда он посимвольно равномерен и эквидистантен, а при $m \neq k$ он к тому же равновесен (см. [3, утверждение 2]). Это же соответствие переводит каждый столбец q-ичного кода в подматрицу слабо разрешимой $WRB_m(v,k,\lambda)$-схемы. ▲

С л е д с т в и е. *Так как четверичный код с параметрами* (3) *лежит на границе Джонсона, то существует слабо разрешимая* $WRB_{t-1}(4t-1,t,(t-1)(2t-1)\times(4t-3)/3)$*-схема. Параметры схемы легко вычисляются по параметрам кода*:

$$v=N, \quad \lambda = n-d, \quad m = \frac{N(n-w)}{n}, \quad k = \frac{Nw}{n(q-1)}.$$

Замечание 2. Теорема 1 является частным случаем теоремы 2 при $m=k$. Надо только помнить, что при $m=k$ код не является равновесным, а величина $\frac{r(v-m)}{v}$ является средним весом $\bar{w}$ кодовых слов, при котором также верна граница Джонсона (см. [3]).

Замечание 3. Введенная в [6] m-квазиразрешимая $NRB_m(v,k,\lambda)$-схема эквивалентна слабо разрешимой $WRB_m(v,k,\lambda')$-схеме, столбцы которой с m единицами образуют $B(v,m,\xi)$-схему, где

$$\xi = \frac{\lambda m(m-1)}{(v-m)(k-1)}.$$

Эквивалентность здесь такова: квазиразрешимая схема получается из слабо разрешимой удалением из каждой матрицы A_j (см. (1)) столбца с m единицами, а слабо разрешимая из квазиразрешимой – вставкой в каждую матрицу A_j столбца с m единицами на позициях, соответствующих нулевым строкам матрицы A_j. При этом, очевидно, $\lambda' = \lambda + \xi$.

3. Рассмотрим теперь другой частный случай слабо разрешимой схемы: $k=2$, $\lambda=1$. Так как вес кодовых слов (см. (7)) является целым числом

$$w = \frac{n(N-m)}{N} = \frac{r(v-m)}{v} = r-m+\frac{m(m-1)^2}{v+m(m-2)},$$

то целочисленной является дробь

$$\frac{m(m-1)^2}{v+m(m-2)}. \tag{8}$$

Таким образом, целочисленность дроби (8) является необходимым условием для существования слабо разрешимой $WRB_m(v,2,1)$-схемы, и следовательно, для существования кода, лежащего на границе Джонсона, параметры которого определены в теореме 2. Впрочем, иногда это необходимое условие является и достаточным, примеры чему будут приведены ниже.

Нетрудно проверить, что если мы ищем знаменатель дроби (8) в виде произведения сомножителей ее числителя, то единственным таким решением (при $m \geqslant 3$) является

$$v = m(m-1)^2 - m(m-2) = m(m^2-3m+3) = (m-1)^3+1. \tag{9}$$

Конечно, существует много других значений параметра v, при которых дробь (8) является целым числом. Мы приведем только два таких примера – по одному для нечетного и четного m:

$$v = \begin{cases} 2m(m-1) - m(m-2) = m^2, & m \text{ – нечетное,} \\ 2(m-1)^2 - m(m-2) = m^2-2m+2, & m \text{ – четное.} \end{cases} \tag{10}$$

Выпишем для всех трех случаев допустимые значения параметров кодов, лежащих на границе Джонсона:

(I) $N = m(m^2-3m+3)$, $n = (m-1)(m^2-3m+3)$, $d = n-1$, $w = n-m+1$, $q = \dfrac{N-m}{2}+1$;

(II) $N = m^2$, $n = \dfrac{m(m+1)}{2}$, $d = n-1$, $w = \dfrac{N-1}{2}$, $q = \dfrac{N-m}{2}+1$, m – нечетное;

(III) $N = m^2-2m+2$, $n = \dfrac{m^2-2m+2}{2}$, $d = n-1$, $w = \dfrac{N-m}{2}$, $q = \dfrac{N-m}{2}+1$, m – четное.

Во всех трех случаях удалось для некоторых значений m построить коды с такими параметрами.

4. Начнем со случая (II), для которого удалось построить семейства кодов с указанными параметрами.

Предложение 1. *Для любого нечетного простого m существует код со значениями параметров* (II).

Доказательство. Представим код C в виде матрицы размера $m^2 \times \dfrac{m(m+1)}{2}$:

$$C = \begin{bmatrix} B_1 & A_{1,1} & \dots & A_{1,(m-1)/2} \\ B_2 & A_{2,1} & \dots & A_{2,(m-1)/2} \\ \dots & \dots & \dots & \dots \\ B_m & A_{m,1} & \dots & A_{m,(m-1)/2} \end{bmatrix},$$

где каждая из матриц B_r, $r = 1,\dots,m$, и $A_{r,s}$, $r = 1,\dots,m$, $s = 1,\dots,(m-1)/2$, является циркулянтной (по модулю m) матрицей размера $m \times m$ (строки и столбцы любой квадратной матрицы размера $p \times p$ всюду далее будем нумеровать от 0 до $p-1$). Следовательно, каждая из этих матриц определяется своей первой строкой. Сначала зададим первые строки матриц B_r:

$$b_{0,0}(r) = 0, \quad b_{0,t}(r) = (r-1)(m-1)/2 + \min\{t, m-t\}, \quad t = 1,2,\dots,m-1. \tag{11}$$

Для пояснения приведем простой пример при $m = 7$, а именно выпишем первые строки матриц B_1, B_2 и B_7 ($q = 22$, символы алфавита обозначаем числами от 0 до 21):

$$(0\ 1\ 2\ 3\ 3\ 2\ 1), \quad (0\ 4\ 5\ 6\ 6\ 5\ 4), \quad (0\ 19\ 20\ 21\ 21\ 20\ 19).$$

Так как в каждой первой строке матриц B_r используется $\dfrac{m-1}{2}$ различных ненулевых символов, в двух разных строках используются различные ненулевые символы алфавита, а число первых строк равно m, то мощности алфавита, равной $m(m-1)/2+1$, достаточно для первых строк всех матриц. Нетрудно видеть, что расстояние между словами матрицы B_r равно $m-1$ при любом r, $r = 1, 2, \ldots, m$. Обозначим через P_B матрицу первых строк матриц B_r, $r = 1, \ldots, m$.

Далее требуется построить первые строки матриц $A_{r,s}$, $r = 1, \ldots, m$, $s = 1, \ldots, (m-1)/2$. Обозначим через P_s, $s = 1, \ldots, (m-1)/2$, матрицу, образованную первыми строками матриц $A_{r,s}$, $r = 1, \ldots, m$, и укажем способ ее построения (координаты в матрице на пересечении i-й строки и ℓ-го столбца будем обозначать через (i, ℓ)). Сначала определим расположение нулей в матрице P_s: в каждой строке и каждом столбце матрицы встретится ровно один 0 в позиции $(i, is \bmod m)$, $i = 0, 1, \ldots, m-1$, (напомним, что m – простое число и $s \leqslant (m-1)/2$). Всего в матрице P_s имеется $\binom{m}{2}$ пар нулей. Каждая такая пара нулей с координатами $(i, is \bmod m)$ и $(j, js \bmod m)$ определяет координаты $(i, js \bmod m)$ и $(j, is \bmod m)$, $i \neq j$, и на этих позициях располагается некоторый ненулевой символ, причем различным парам нулей соответствуют различные ненулевые символы (это возможно, так как число ненулевых символов алфавита и число пар нулей одно и то же: $m(m-1)/2$).

Приведем в качестве примера такого построения матрицы P_1 и P_2 при $m = 5$:

$$P_1 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 5 & 6 & 7 \\ 2 & 5 & 0 & 8 & 9 \\ 3 & 6 & 7 & 0 & 10 \\ 4 & 8 & 9 & 10 & 0 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 0 & 3 & 1 & 4 & 2 \\ 1 & 6 & 0 & 7 & 5 \\ 2 & 8 & 5 & 9 & 0 \\ 3 & 0 & 6 & 10 & 8 \\ 4 & 10 & 7 & 0 & 9 \end{bmatrix}.$$

Так как все символы в первой строке матриц $A_{r,s}$, $r = 1, \ldots, m$, $s = 1, \ldots, (m-1)/2$, различны, а сами матрицы циркулянтны, то расстояние между строками каждой матрицы равно m, и следовательно, расстояние между кодовыми словами внутри r-го слоя кода C равно $n-1$. Осталось доказать, что расстояние между любыми двумя кодовыми словами матрицы C из разных слоев равно $n-1$. Определим следующую матрицу $P(C)$ размера $m \times m(m+1)/2$:

$$P(C) = [P_B \,|\, P_1 \,|\, \ldots \,|\, P_s| \ldots \,|\, P_{(m-1)/2}].$$

Нетрудно видеть, что расстояние между кодовыми словами матрицы C из разных слоев в силу циркулянтности матриц B_r и $A_{r,s}$ совпадает с расстоянием между некоторыми фиксированными сдвигами соответствующих строк матрицы $P(C)$. Естественно, эти сдвиги определяются выбранными кодовыми словами, а сами сдвиги (по модулю m) происходят в каждой из матриц P_B, P_s, $s = 1, \ldots, (m-1)/2$, размера $m \times m$. Опять же в силу циркулянтности матриц B_r и $A_{r,s}$ можно зафиксировать одну строку матрицы $P(C)$ и сдвигать лишь другую. Отметим прежде всего, что по построению в любых двух строках каждой матрицы P_s, $s = 1, \ldots, (m-1)/2$, имеется ровно два одинаковых символа алфавита: один нулевой, а другой ненулевой, причем никакой сдвиг одной строки матрицы P_s, $s = 1, \ldots, (m-1)/2$, относительно другой не может привести к совпадению этих двух символов на соответствующих позициях этих двух строк.

Зафиксируем теперь две строки матрицы $P(C)$ с номерами i и j и рассмотрим эти строки в матрицах P_s и $P_{s'}$, $s \neq s'$. По построению нули в этих строках находятся в позициях $(i, si \bmod m)$ и $(j, sj \bmod m)$ в матрице P_s и в позициях $(i, s'i \bmod m)$ и $(j, s'j \bmod m)$ в матрице $P_{s'}$, а позиции одинаковых ненулевых символов – $(i, sj \bmod m)$ и $(j, si \bmod m)$ в матрице P_s и $(i, s'j \bmod m)$ и $(j, s'i \bmod m)$ в матрице $P_{s'}$.

Чтобы при сдвиге j-й строки совпали позиции нулей в обеих матрицах, должно выполняться следующее условие:

$$(i-j)s \equiv (i-j)s' \pmod m,$$

т.е.

$$(i-j)(s-s') \equiv 0 \pmod m,$$

что невозможно, так как m – простое число, а $i \neq j$ и $s \neq s'$. Напомним, что

$$i < m, \quad j < m, \quad s \leqslant (m-1)/2, \quad s' \leqslant (m-1)/2.$$

Чтобы при сдвиге j-й строки совпали позиции нулей в одной матрице (например, в P_s) и позиции одинаковых ненулевых символов в другой матрице, должно выполняться следующее условие:

$$(i-j)s \equiv (j-i)s' \pmod m,$$

т.е.

$$(i-j)(s+s') \equiv 0 \pmod m,$$

что невозможно, так как m – простое число, а $i \neq j$ и $s+s' \leqslant (m-1)$. Совпадение при сдвиге j-й строки позиций одинаковых ненулевых символов в одной матрице и одинаковых ненулевых символов в другой матрице невозможно по той же причине, что и совпадение двух нулевых символов.

Так как число различных матриц P_s равно $(m-1)/2$, в каждой матрице P_s всего для двух сдвигов j-й строки относительно i-й происходит совпадение символов в i-й и j-й строках (одного нулевого и одного ненулевого), а число различных ненулевых сдвигов j-й строки относительно i-й равно $m-1$, то при каждом сдвиге происходит совпадение символов этих двух строк ровно в одной позиции. При нулевом сдвиге, т.е. при отсутствии сдвига, совпадают нулевые символы в i-й и j-й строках матрицы P_B. Следовательно, расстояние между любыми кодовыми словами матрицы C равно $n-1$. ▲.

Приведенное доказательство не применимо к случаю, когда m – не простое число. Однако в теории кодирования редко бывает, чтобы некоторое утверждение было верным только для простого поля, а не любого конечного поля (в нашем случае для m, являющегося степенью простого). И действительно, справедливо

П р е д л о ж е н и е 2. *Для любого нечетного m, являющегося степенью простого числа, существует код со значениями параметров* (II).

Д о к а з а т е л ь с т в о. Известно [7], что для любого m, являющегося степенью простого, существует МДР-код с параметрами

$$N' = m^2, \quad n' = m+1, \quad d' = m, \quad q = m. \tag{12}$$

Так как размерность этого МДР-кода равна 2, то любые две позиции кода являются информационными, т.е. любые два столбца кода содержат каждую пару символов алфавита ровно один раз (символы алфавита обозначим через $0, 1, \ldots, m-1$). Обратимся теперь к матрицам B_r, введенным в предложении 1 (заметим, что их определение не зависит от простоты числа m). Это циркулянтные матрицы, первая строка которых определяется равенствами (11). Обозначим j-ю строку матрицы B_r через $b_j(r)$ и зададим отображение

$$f(j,r) = b_j(r),$$

переводящее каждую пару символов МДР-кода (j,r), $j = 0,1,\dots,m-1$, $r = 0,1,\dots,m-1$, в j-ю строку $b_j(r)$ длины m матрицы B_r. Разобьем теперь столбцы МДР-кода на пары и, используя отображение $f(j,r)$, поставим в соответствие каждой паре столбцов матрицу размера $m^2 \times m$. В результате получим матрицу кода с параметрами (II). Действительно, число кодовых слов равно числу кодовых слов МДР-кода, т.е. $N = m^2$, длина кода равна числу пар столбцов $(m+1)/2$, умноженному на m, т.е. $n = m(m+1)/2$, алфавит кода равен объединению алфавитов, используемых во всех матрицах B_r в предложении 1, т.е. $q = 1 + m(m-1)/2 = 1 + (N-m)/2$, а вес кодовых слов равен числу пар столбцов $(m+1)/2$, умноженному на вес строки матриц B_r, равный $m-1$, т.е. $(N-1)/2$. Осталось вычислить кодовое расстояние. Очевидно, что для $(j,r) \neq (j',r')$

$$d\big(f(j,r), f(j',r')\big) = \begin{cases} m, & \text{если } j \neq j' \text{ и } r \neq r', \\ m-1, & \text{если } j = j' \text{ или } r = r'. \end{cases} \tag{13}$$

Так как у любых двух слов МДР-кода символы совпадают лишь в одной позиции (и эти символы, естественно, принадлежат лишь одной паре столбцов разбиения МДР-кода), то согласно (13) расстояние между соответствующими словами построенного нами кода равно $m(m-1)/2 + m - 1 = n - 1$. ▲

Замечание 4. Конечно, предложение 1 представляет собой частный случай предложения 2, но авторам показалась достаточно своеобразной и заслуживающей изложения конструкция кода в предложении 1.

5. При рассмотрении случая (II) в предыдущем пункте мы ограничились нечетными m, так как при четных m слабо разрешимая схема $WRB_m(m^2,2,1)$ не существует, ибо не выполнено необходимое условие, что $w = \dfrac{N-1}{2}$ – целое число. Поэтому, если мы хотим оставить первые два параметра схемы неизменными ($v = m^2$, $k = 2$), то мы должны перейти к схеме $WRB_m(m^2,2,2)$. При этом согласно теореме 2 параметры кода должны быть следующими:

$$\begin{gathered} N = m^2, \quad n = m(m+1), \quad d = n-2, \quad w = N-1, \\ q = \frac{N-m}{2} + 1, \quad m \text{ – четное.} \end{gathered} \tag{14}$$

И при m, равном степени числа 2, такие коды удается построить.

П р е д л о ж е н и е 3. *Для любого m, являющегося степенью числа 2, существует код со значениями параметров* (14).

Д о к а з а т е л ь с т в о. Построение таких кодов, по существу, весьма близко к тому, которое использовалось в предложении 2 для m, равного степени нечетного простого числа. Отличие связано с тем, что при четных m длина МДР-кода с параметрами (12) нечетна, и следовательно, он не может быть разбит на пары столбцов. Поэтому в строки матриц, весьма схожих с матрицами B_r из предложения 1, отображается каждый столбец МДР-кода.

Сначала для любого элемента a алфавита нашего будущего кода ($a = 0,1,\dots,m(m-1)/2$) определим циркулянтную матрицу $D(a)$ размера $(m-1)\times(m-1)$, первая строка которой имеет вид

$$a, a+1, a+2, \dots, a+(m-2)/2, a+(m-2)/2, a+(m-2)/2-1, \dots, a+2, a+1.$$

Затем превратим эту матрицу в матрицу $D(a,\ell)$ размера $m \times m$, присоединив к ней сначала снизу строку $a, a, \ldots, a$ длины $m-1$, а затем вставив нулевой столбец в ℓ-й позиции, $\ell = 0, 1, \ldots, m-1$. Приведем пример такого построения при $m = 8$:

$$D(a) = \begin{bmatrix} a & a+1 & a+2 & a+3 & a+3 & a+2 & a+1 \\ a+1 & a & a+1 & a+2 & a+3 & a+3 & a+2 \\ \multicolumn{7}{c}{\dotfill} \\ a+2 & a+3 & a+3 & a+2 & a+1 & a & a+1 \\ a+1 & a+2 & a+3 & a+3 & a+2 & a+1 & a \end{bmatrix}$$

и

$$D(a,3) = \begin{bmatrix} a & a+1 & a+2 & 0 & a+3 & a+3 & a+2 & a+1 \\ a+1 & a & a+1 & 0 & a+2 & a+3 & a+3 & a+2 \\ \multicolumn{8}{c}{\dotfill} \\ a+2 & a+3 & a+3 & 0 & a+2 & a+1 & a & a+1 \\ a+1 & a+2 & a+3 & 0 & a+3 & a+2 & a+1 & a \\ a & a & a & 0 & a & a & a & a \end{bmatrix}.$$

Нетрудно видеть, что расстояние между строками матрицы $D(a,\ell)$ равно $m-2$. Положим $A = \{1 + rm/2 : \ r = 0, 1, \ldots, m-2\}$. Очевидно, что для любых $a, a' \in A$, $a \neq a'$, расстояние между строками матриц $D(a,\ell)$ и $D(a',\ell')$ равно m, если $\ell \neq \ell'$. Теперь уже мы можем определить матрицы D_r: $D_r = D(1 + rm/2, r)$, $r = 0, 1, \ldots, m-2$. Матрицу D_{m-1} определим несколько иным способом: положим ее r-й столбец равным $(r+1)$-му столбцу матрицы D_r, $r = 0, 1, \ldots, m-2$, а последний ($(m-1)$-й) столбец положим нулевым.

Нетрудно видеть, что расстояние между строками матрицы D_r, $r = 0, 1, \ldots, m-1$, равно $m-2$, а между строками матриц D_r и $D_{r'}$, $r \neq r'$, равно m.

Проиллюстрируем построение матриц D_r на примере $m = 4$. Первые три матрицы имеют вид

$$D_0 = \begin{bmatrix} 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 2 \\ 0 & 2 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \quad D_1 = \begin{bmatrix} 3 & 0 & 4 & 4 \\ 4 & 0 & 3 & 4 \\ 4 & 0 & 4 & 3 \\ 3 & 0 & 3 & 3 \end{bmatrix}, \quad D_2 = \begin{bmatrix} 5 & 6 & 0 & 6 \\ 6 & 5 & 0 & 6 \\ 6 & 6 & 0 & 5 \\ 5 & 5 & 0 & 5 \end{bmatrix},$$

а последняя –

$$D_3 = \begin{bmatrix} 1 & 4 & 6 & 0 \\ 2 & 3 & 6 & 0 \\ 2 & 4 & 5 & 0 \\ 1 & 3 & 5 & 0 \end{bmatrix}.$$

Отображение МДР-кода (12) в код с параметрами (14) совсем просто: каждый символ r этого кода, $r = 0, 1, \ldots, m-1$, заменяется на строку матрицы D_r с выполнением единственного требования – два одинаковых символа в одном столбце МДР-кода должны заменяться на разные строки соответствующей матрицы (напомним, что каждый символ МДР-кода (12) в каждом столбце встречается m раз, а каждая матрица D_r состоит из m строк). Формально такое отображение можно задать, например, следующим образом. Обозначим j-ю строку матрицы D_r через $d_j(r)$ и зададим отображение

$$\varphi(j, r) = d_j(r),$$

переводящее каждую пару (j, r), $j = 0, 1, \ldots, m-1$, $r = 0, 1, \ldots, m-1$, в j-ю строку $d_j(r)$ длины m матрицы D_r. Перенумеруем строки матрицы МДР-кода числами от 1 до m^2. В каждом столбце матрицы МДР-кода каждый из его m символов

$\{0, 1, \ldots, m-1\}$ встречается m раз. Пусть $i_0(r) < i_1(r) < \ldots < i_{m-1}(r)$ – номера строк МДР-кода, в которых встречается фиксированный символ r этого кода. Если этот символ стоит в строке с номером $i_j(r)$, то применим к этому символу отображение $\varphi(j, r)$, т.е. поставим в соответствие этому символу j-ю строку матрицы D_r. Тем самым, каждый столбец матрицы МДР-кода отобразится в некоторую матрицу размера $m^2 \times m$, состоящую из строк матриц $D_0, \ldots, D_{m-1}$. Матрица размера $m^2 \times m(m+1)$, полученная в результате такого отображения всех $m+1$ столбцов МДР-кода, представляет собой код с параметрами (14). Вычисление параметров полученного кода аналогично соответствующему вычислению в предложении 2. ▲

Продолжим иллюстрацию примера при $m = 4$:

$$\begin{bmatrix}
0&0&0&0&0\\
0&1&1&1&1\\
0&2&2&2&2\\
0&3&3&3&3\\
1&0&1&2&3\\
1&1&0&3&2\\
1&2&3&0&1\\
1&3&2&1&0\\
2&0&2&3&1\\
2&1&3&2&0\\
2&2&0&1&3\\
2&3&1&0&2\\
3&0&3&1&2\\
3&1&2&0&3\\
3&2&1&3&0\\
3&3&0&2&1
\end{bmatrix}, \quad
\begin{bmatrix}
0&1&2&2&0&1&2&2&0&1&2&2&0&1&2&2&0&1&2&2\\
0&2&1&2&3&0&4&4&3&0&4&4&3&0&4&4&3&0&4&4\\
0&2&2&1&5&6&0&6&5&6&0&6&5&6&0&6&5&6&0&6\\
0&1&1&1&1&4&6&0&1&4&6&0&1&4&6&0&1&4&6&0\\
3&0&4&4&0&2&1&2&4&0&3&4&6&5&0&6&2&3&6&0\\
4&0&3&4&4&0&3&4&0&2&1&2&2&3&6&0&6&5&0&6\\
4&0&4&3&6&5&0&6&2&3&6&0&0&2&1&2&4&0&3&4\\
3&0&3&3&2&3&6&0&6&5&0&6&4&0&3&4&0&2&1&2\\
5&6&0&6&0&2&2&1&6&6&0&5&2&4&5&0&4&0&4&3\\
6&5&0&6&4&0&4&3&2&4&5&0&6&6&0&5&0&2&2&1\\
6&6&0&5&6&6&0&5&0&2&2&1&4&0&4&3&2&4&5&0\\
5&5&0&5&2&4&5&0&4&0&4&3&0&2&2&1&6&6&0&5\\
1&4&6&0&0&1&1&1&1&3&5&0&3&0&3&3&5&5&0&5\\
2&3&6&0&3&0&3&3&5&5&0&5&0&1&1&1&1&3&5&0\\
2&4&5&0&5&5&0&5&3&0&3&3&1&3&5&0&0&1&1&1\\
1&3&5&0&1&3&5&0&0&1&1&1&5&5&0&5&3&0&3&3
\end{bmatrix}.$$

Левая матрица представляет собой исходный $[5, 2, 4]_4$-МДР-код, а правая – семеричный код мощности 16 с длиной 20, расстоянием 18 и весом 15, полученный при описанном выше отображении МДР-кода с помощью матриц D_0, D_1, D_2, D_3.

6. Перейдем теперь к случаю (I), где удалось построить соответствующий код лишь при $m = 4$ и $m = 5$; при $m = 3$ соответствующий код совпадает с кодом, построенным в случае (II), и давно известен (см., например, [8]) – это четверичный код мощности 9 с длиной 6, расстоянием 5 и весом кодовых слов 4. Построение обоих кодов основано, как и в предыдущем пункте, на использовании циркулянтных матриц, но само построение циркулянтных матриц произведено “вручную”, так что нам не удалось распространить его на бóльшие значения m.

При $m = 4$ это код C_1 над алфавитом из 13 символов мощности 28 с длиной 21, расстоянием 20 и весом кодовых слов 18. Матрица размера 28×21 кодовых слов кода C_1 строится по тому же правилу, что и матрицы в случае (II):

$$C_1 = \begin{bmatrix}
B_1 & A_{1,1} & A_{1,2}\\
B_2 & A_{2,1} & A_{2,2}\\
B_3 & A_{3,1} & A_{3,2}\\
B_4 & A_{4,1} & A_{4,2}
\end{bmatrix},$$

где каждая из квадратных матриц размера 7×7 циркулянтна и поэтому, как и в случае (II), можно определить матрицу $P(C_1)$ размера 4×7, состоящую из первых строк всех матриц B_r, A_{rs}, $r = 1, 2, 3, 4$, $s = 1, 2$:

$$P(C_1) = [P_B \,|\, P_1 \,|\, P_2].$$

Здесь матрица P_B строится так же, как и в случае (II):

$$P_B = \begin{bmatrix} 0 & 1 & 2 & 3 & 3 & 2 & 1 \\ 0 & 4 & 5 & 6 & 6 & 5 & 4 \\ 0 & 7 & 8 & 9 & 9 & 8 & 7 \\ 0 & 10 & 11 & 12 & 12 & 11 & 10 \end{bmatrix}.$$

Матрица P_1 задается в следующем виде:

$$P_1 = \begin{bmatrix} 0 & 1 & 2 & 5 & 6 & 3 & 4 \\ 1 & 9 & 0 & 7 & 8 & 10 & 2 \\ 4 & 8 & 7 & 3 & 0 & 11 & 12 \\ 10 & 6 & 9 & 12 & 11 & 5 & 0 \end{bmatrix},$$

а строками матрицы P_2 являются строки матрицы P_1, записанные в обратном порядке. Нетрудно проверить непосредственно, что расстояние кода C_1 равно 20.

При $m = 5$ это код C_2 над алфавитом из 31 символа мощности 65 с длиной 52, расстоянием 51 и весом кодовых слов 48. Матрица кодовых слов C_2 размера 65×52 выглядит так:

$$C_2 = \begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,3} & A_{1,4} \\ A_{2,1} & A_{2,2} & A_{2,3} & A_{2,4} \\ A_{3,1} & A_{3,2} & A_{3,3} & A_{3,4} \\ A_{4,1} & A_{4,2} & A_{4,3} & A_{4,4} \\ A_{5,1} & A_{5,2} & A_{5,3} & A_{5,4} \end{bmatrix},$$

где каждая из квадратных матриц размера 13×13 циркулянтна. Поэтому можно определить матрицу $P(C_2)$ размера 5×13, состоящую из первых строк всех матриц A_{rs}, $r = 1, 2, 3, 4, 5$, $s = 1, 2, 3, 4$:

$$P(C_2) = [P_1 \mid P_2 \mid P_3 \mid P_4].$$

Матрицы P_s задаются в следующем виде:

$$P_1 = \begin{bmatrix} 1 & 6 & 11 & 16 & 0 & 21 & 22 & 23 & 24 & 16 & 11 & 6 & 1 \\ 2 & 7 & 12 & 17 & 21 & 0 & 25 & 26 & 27 & 17 & 12 & 7 & 2 \\ 3 & 8 & 13 & 18 & 22 & 25 & 0 & 28 & 29 & 18 & 13 & 8 & 3 \\ 4 & 9 & 14 & 19 & 23 & 26 & 28 & 0 & 30 & 19 & 14 & 9 & 4 \\ 5 & 10 & 15 & 20 & 24 & 27 & 29 & 30 & 0 & 20 & 15 & 10 & 5 \end{bmatrix},$$

$$P_2 = \begin{bmatrix} 1 & 21 & 6 & 22 & 11 & 16 & 23 & 16 & 11 & 0 & 9 & 24 & 4 \\ 2 & 0 & 7 & 25 & 12 & 17 & 26 & 17 & 12 & 21 & 10 & 27 & 5 \\ 3 & 26 & 8 & 28 & 13 & 18 & 0 & 18 & 13 & 23 & 6 & 29 & 1 \\ 4 & 27 & 9 & 29 & 14 & 19 & 30 & 19 & 14 & 24 & 7 & 0 & 2 \\ 5 & 25 & 10 & 0 & 15 & 20 & 28 & 20 & 15 & 22 & 8 & 30 & 3 \end{bmatrix},$$

$$P_3 = \begin{bmatrix} 0 & 1 & 6 & 21 & 5 & 16 & 22 & 20 & 11 & 23 & 8 & 12 & 24 \\ 21 & 2 & 7 & 0 & 12 & 16 & 25 & 18 & 1 & 26 & 9 & 13 & 27 \\ 22 & 3 & 8 & 25 & 13 & 17 & 0 & 18 & 2 & 28 & 10 & 14 & 29 \\ 23 & 4 & 9 & 26 & 14 & 17 & 28 & 19 & 3 & 0 & 6 & 15 & 30 \\ 24 & 5 & 10 & 27 & 15 & 20 & 29 & 19 & 4 & 30 & 7 & 11 & 0 \end{bmatrix},$$

$$P_4 = \begin{bmatrix} 1 & 6 & 0 & 11 & 21 & 10 & 22 & 12 & 23 & 17 & 24 & 20 & 3 \\ 2 & 7 & 21 & 12 & 0 & 6 & 25 & 15 & 26 & 18 & 27 & 16 & 4 \\ 3 & 8 & 22 & 11 & 25 & 9 & 0 & 16 & 28 & 19 & 29 & 15 & 5 \\ 4 & 9 & 23 & 13 & 26 & 8 & 28 & 14 & 0 & 18 & 30 & 20 & 1 \\ 5 & 7 & 24 & 14 & 27 & 10 & 29 & 13 & 30 & 19 & 0 & 17 & 2 \end{bmatrix}.$$

Непосредственная, но достаточно утомительная проверка показывает, что расстояние кода C_2 равно 51.

Хотя нам и не удалось для случая (I) построить бесконечное семейство кодов с заданными параметрами, но три указанных кода оставляют надежду на то, что такое семейство существует.

7. Осталось рассмотреть случай (III). Вначале отметим, что если в транспонированной матрице кодовых слов заменить все ненулевые символы на 0, а нулевой символ на 1, то эта матрица будет представлять собой двоичный код, лежащий на границе Джонсона, с параметрами

$$N = \frac{m^2 - 2m + 2}{2}, \quad n = m^2 - 2m + 2, \quad d = 2(m-1), \quad w = m,$$

или, что то же самое, блок-схему $B(v = 2k^2 - 2k + 1, k, 1)$, где $k = m/2$. Следовательно, существование таких блок-схем является необходимым условием существования кода с параметрами (III), но далеко не достаточным. Ведь наличие блок-схемы позволяет лишь правильно расположить нулевые символы в кодовой матрице, а правильное расположение пар ненулевых символов в каждом столбце – это отдельная нелегкая задача. Мы знаем, например, что указанные блок-схемы построены при $k = 2, 3, 4, 5$ (т.е. при $m = 4, 6, 8, 10$), но лишь при $m = 4$ соответствующий равновесный четверичный код длины 5 мощности 10 с расстоянием 4 давно известен (см., например, [8]).

8. В [3] была поставлена задача построения посимвольно равномерных эквидистантных кодов минимальной длины при заданных параметрах q, k, m (напомним, что каждый ненулевой символ встретится в столбце кодовой матрицы k раз, а нулевой символ – m раз; очевидно, что число кодовых слов $N = (q-1)k + m$). Согласно теореме 2 длина такого кода равна

$$n = \frac{\lambda N(N-1)}{m(m-1) + (N-m)(k-1)}, \tag{15}$$

где через $\lambda = n - d$ обозначена разность между длиной кода и его расстоянием. Так как n – целое число, то очевидно, что минимальная длина достигается при наименьшем λ, таком что правая дробь в (15) становится целым числом. Обозначим через (a, b) наибольший общий делитель чисел a и b. Ясно, что минимальное λ, при котором дробь $\dfrac{\lambda a}{b}$ становится целым числом, равно $\dfrac{b}{(a,b)}$. Следовательно, имеет место

П р е д л о ж е н и е 4. *Минимальная длина n посимвольно равномерного эквидистантного кода с параметрами q, k, m удовлетворяет неравенству*

$$n \geqslant \frac{N(N-1)}{(N(N-1), m(m-k) + N(k-1))}, \tag{16}$$

где $N = (q-1)k + m$.

Нетрудно непосредственно проверить, что все коды, приведенные в пп. 3, 4, 6, 7, имеют минимальную длину.

СПИСОК ЛИТЕРАТУРЫ

1. *Beth T., Jungnickel D., Lenz B.* Design Theory. Cambridge: Cambridge Univ. Press, 1999.
2. *Семаков Н.В., Зиновьев В.А.* Эквидистантные q-ичные коды с максимальным расстоянием и разрешимые уравновешенные неполные блок-схемы // Пробл. передачи информ. 1968. Т. 4. № 2. С. 3–10. http://mi.mathnet.ru/ppi1845

3. *Бассалыго Л.А., Зиновьев В.А., Лебедев В.С.* Симметричные блок-схемы и оптимальные эквидистантные коды // Пробл. передачи информ. 2020. Т. 56. № 3. С. 50–58. `https://doi.org/10.31857/S055529232003002X`

4. *Sinha K., Sinha N.* A Class of Optimal Quaternary Codes // Ars Combin. 2010. V. 94. P. 61–64.

5. *Бассалыго Л.А.* Новые верхние границы для кодов, исправляющих ошибки // Пробл. передачи информ. 1965. Т. 1. № 4. С. 41–44. `http://mi.mathnet.ru/ppi762`

6. *Бассалыго Л.А., Зиновьев В.А., Лебедев В.С.* Об m-квазиразрешимых блок-схемах и q-ичных равновесных кодах // Пробл. передачи информ. 2018. Т. 54. № 3. С. 54–61. `http://mi.mathnet.ru/ppi2272`

7. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.

8. *Todorov T., Bogdanova G., Yorgova T.* Lexicographic Constant-Weight Equidistant Codes over the Alphabet of Three, Four and Five Elements // Intell. Inf. Manag. 2010. V. 2. № 3. P. 183–187. `https://doi.org/10.4236/iim.2012.23021`

Бассалыго Леонид Александрович
Зиновьев Виктор Александрович
Лебедев Владимир Сергеевич
Институт проблем передачи информации
им. А.А. Харкевича РАН
`bass@iitp.ru`
`vazinov@iitp.ru`
`lebedev37@mail.ru`

Поступила в редакцию
16.04.2021
После доработки
11.09.2021
Принята к публикации
01.10.2021