ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 3**

УДК 621.391.1 : 519.725

 Л.А. Бассалыго, В.А. Зиновьев, В.С. Лебедев

СИММЕТРИЧНЫЕ БЛОК-СХЕМЫ И ОПТИМАЛЬНЫЕ ЭКВИДИСТАНТНЫЕ КОДЫ[1]

Доказывается, что любая симметричная блок-схема (v, k, λ) порождает оптимальные троичный и четверичный равновесные эквидистантные коды, параметры которых n, N, w, d, q однозначно определяются параметрами блок-схемы. Для одного весьма частного случая построены посимвольно равномерные эквидистантные коды минимальной длины.

Ключевые слова: блок-схема, посимвольно равномерный код, эквидистантный код.

DOI: 10.31857/S055529232003002X

1. Назовем q-ичный код длины n мощности N с расстоянием d *посимвольно равномерным*, если в матрице кодовых слов размера $N \times n$ каждый ненулевой символ содержится в каждом столбце матрицы одно и то же число раз независимо от выбора символа и выбора столбца. Всюду в дальнейшем это число полагается равным t, а следовательно, нулевой символ в каждом столбце содержится $m = N - (q-1)t$ раз. Обозначим через $\bar{w}$ средний вес кодовых слов:

$$\bar{w} = \frac{\text{число ненулевых символов всех кодовых слов}}{N}.$$

Лемма. *Если*

$$q\bar{w}^2 > (q-1)(2\bar{w} - d)n,$$

то имеет место следующее неравенство:

$$N \leqslant \frac{(q-1)dn}{q\bar{w}^2 - (q-1)(2\bar{w} - d)n}. \tag{1}$$

Доказательство. Доказательство леммы для равновесных кодов приведено в работе [1], и здесь мы лишь повторим его с использованием среднего веса кодовых слов. Пусть $C = \{c_1, c_2, \ldots, c_N\}$ – код длины n с расстоянием d над q-ичным алфавитом $Q = \{\ell : \ \ell = 0, 1, \ldots, q-1\}$. Рассмотрим матрицу размера $N \times n$ кодовых слов кода C. Обозначим через $w_{\ell j}$ число использования символа ℓ в j-м столбце кодовой матрицы ($\ell = 0, 1, \ldots, q-1$, $j = 1, 2, \ldots, n$). Из определения среднего веса $\bar{w}$ вытекает, что

$$\sum_{j=1}^{n} \sum_{\ell=1}^{q-1} w_{\ell j} = N\bar{w}, \quad \sum_{j=1}^{n} w_{0j} = N(n - \bar{w}). \tag{2}$$

[1] Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 19-01-00364).

Так как

$$\sum_{\substack{k,s=1\\k\neq s}}^{N} d(c_k,c_s)=\sum_{j=1}^{n}\sum_{\ell=0}^{q-1} w_{\ell j}(N-w_{\ell j}), \tag{3}$$

то

$$\sum_{j=1}^{n}\sum_{\ell=0}^{q-1} w_{\ell j}(N-w_{\ell j}) \geqslant N(N-1)d, \tag{4}$$

причем равенство достигается тогда и только тогда, когда код является эквидистантным. С другой стороны,

$$\sum_{j=1}^{n}\sum_{\ell=0}^{q-1} w_{\ell j}(N-w_{\ell j}) = N^2 n-\sum_{j=1}^{n}\sum_{\ell=1}^{q-1} w_{\ell j}^2-\sum_{j=1}^{n} w_{0j}^2,$$

и из (2) следует, что

$$\sum_{j=1}^{n}\sum_{\ell=1}^{q-1} w_{\ell j}^2 \leqslant \frac{N^2\bar{w}^2}{n(q-1)} \quad \text{и} \quad \sum_{j=1}^{n} w_{0j}^2 \leqslant \frac{N^2(n-\bar{w})^2}{n},$$

причем равенство в этих соотношениях достигается тогда и только тогда, когда

$$w_{\ell j}=\frac{N\bar{w}}{n(q-1)}, \quad \ell=1,\ldots,q-1, \quad j=1,\ldots,n,$$

и

$$w_{0j}=\frac{N(n-\bar{w})}{n}, \quad j=1,\ldots,n.$$

Следовательно,

$$\sum_{j=1}^{n}\sum_{\ell=0}^{q-1} w_{\ell j}(N-w_{\ell j}) \leqslant N^2 n-\frac{N^2\bar{w}^2}{n(q-1)}+\frac{N^2(n-\bar{w})^2}{n},$$

причем равенство достигается тогда и только тогда, когда код является посимвольно равномерным. Отсюда и из (4) получаем

$$N(q\bar{w}^2-(q-1)(2\bar{w}-d)n) \leqslant (q-1)dn,$$

что и завершает доказательство. ▲

Из доказательства леммы вытекает следующее

Утверждение 1. *Код достигает границы* (1) *тогда и только тогда, когда он эквидистантен и посимвольно равномерен.*

Обратим внимание, что мы не потребовали равновесности кода, как в стандартной формулировке границы (1), ибо верно следующее

Утверждение 2. *Если $m \neq t$, то эквидистантный посимвольно равномерный код равновесен.*

Доказательство. Пусть x_s – слово кода, а w_s – его вес, $s=1,2,\ldots,N$. В силу эквидистантности кода

$$\sum_{i=1}^{N} d(x_i,x_s)=(N-1)d. \tag{5}$$

С другой стороны, подсчитывая эту сумму по столбцам, получим

$$\sum_{i=1}^{N} d(x_i, x_s) = (N-t)w_s + (N-m)(n-w_s). \tag{6}$$

Следовательно,

$$w_s(m-t) = (N-1)d - (N-m)n, \tag{7}$$

и если $m \neq t$, то вес w_s кодового слова не зависит от s, что доказывает равновесность кода. ▲

Если же $m = t$, то $(N-1)d = (N-m)n$ и $N = qm$. Отсюда получаем, что

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

т.е. имеет место

С л е д с т в и е 1 [2]. *Если $m = t$, то эквидистантный посимвольно равномерный (n, N, d)-код C лежит на границе Плоткина*

$$N \leqslant \frac{qd}{qd-(q-1)n}. \tag{8}$$

Много семейств кодов, лежащих на границе Плоткина (8), было указано в [2]. Так как сдвиг такого кода на любое слово сохраняет не только эквидистантность кода, но и его посимвольную равномерность, то вычтя из всех кодовых слов фиксированное кодовое слово, придем к коду, все кодовые слова которого за исключением нулевого слова имеют вес, равный расстоянию кода (при этом операция сложения в алфавите определяется по модулю q). Средний вес этого кода равен

$$\bar{w} = \frac{(N-1)d}{N} = \frac{(q-1)n}{q},$$

и согласно утверждению 1 этот код лежит на границе Джонсона (1), которая в данном случае совпадает с границей Плоткина, что нетрудно проверить. Удалив из этого кода нулевое слово, получим равновесный код, лежащий на границе Джонсона (1) (но, естественно, не лежащий на границе Плоткина). С другой стороны, если код лежит на границе Джонсона (и следовательно, эквидистантен) и при этом средний вес кода $\bar{w} = d$ (и следовательно, код равновесен), то присоединяя к этому коду нулевое слово, получим код, лежащий на границе Плоткина.

2. *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 [3]:

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

Отметим, что $b \geqslant v$ согласно неравенству Фишера [3]. Блок-схема полностью описывается своей матрицей инцидентности $A = [a_{ij}]$, где

$$a_{ij} = \begin{cases} 1, & \text{если } i \in B_j, \\ 0, & \text{если } i \notin B_j, \end{cases} \qquad i = 1, \ldots, v, \quad j = 1, \ldots, b.$$

Утверждение 3. *Любая блок-схема $B(v,k,\lambda)$ порождает троичный равновесный эквидистантный код с параметрами*

$$N = v, \quad n = \binom{b}{2}, \quad w = r(b-r), \quad d = (r-\lambda)(2b - 3(r-\lambda)) \tag{9}$$

и четверичный равновесный эквидистантный код с параметрами

$$N = v, \quad n = \binom{b}{2}, \quad w = \frac{r}{2}(2b-r-1), \quad d = (r-\lambda)(2b - 2(r-\lambda) - 1). \tag{10}$$

Доказательство. Построение как троичного, так и четверичного кодов происходит по одной и той же весьма простой схеме: выбираются любые два столбца матрицы инцидентности блок-схемы (таковых $\binom{b}{2}$) и заменяются на один столбец q-ичного кода по следующему правилу: для $q = 3$

$$(0,0) \to 0, \quad (1,1) \to 0, \quad (0,1) \to 1, \quad (1,0) \to 2,$$

а для $q = 4$

$$(0,0) \to 0, \quad (0,1) \to 1, \quad (1,0) \to 2, \quad (1,1) \to 3,$$

так что в результате получаем троичный и четверичный коды. Очевидно, что длина построенных кодов $n = \binom{b}{2}$, а число слов в каждом из них $N = v$. Нетрудно проверить, что число совпадений между любыми двумя кодовыми словами троичного кода равно

$$\binom{b-2(r-\lambda)}{2} + 2\binom{r-\lambda}{2},$$

а четверичного –

$$\binom{b-2(r-\lambda)}{2},$$

так как число позиций, в которых два кодовых слова совпадают, не зависит от выбора кодовых слов. Вес кодовых слов при $q = 3$ равен $r(b-r)$, а при $q = 4$ равен

$$\binom{b}{2} - \binom{b-r}{2} = \frac{r}{2}(2b-r-1). \quad \blacktriangle$$

Так как предложенный в утверждении 3 способ построения троичного и четверичного кодов приводит к равновесным эквидистантным кодам, то естественно задаться вопросом, когда эти коды лежат на обобщенной границе Джонсона (1). Из утверждения 1 вытекает, что для выполнения этого условия коды должны быть посимвольно равномерны. Нетрудно видеть, что для посимвольной равномерности кодов из утверждения 3 необходимо, чтобы в (v,k,λ)-схеме скалярное произведение любых двух столбцов матрицы инцидентности не зависело от выбора столбцов. Если $b > v$, то такие схемы не существуют [3]. Если $b = v$, то такая (v,k,λ)-схема называется *симметричной*, и скалярное произведение любых двух столбцов матрицы инцидентности симметричной схемы равно λ [3].

Поэтому верна

Теорема 1. *Троичный код из утверждения 3 лежит на границе Джонсона тогда и только тогда, когда (v,k,λ)-схема симметрична. Четверичный код из* *утверждения 3 лежит на границе Джонсона тогда и только тогда, когда (v,k,λ)-схема симметрична и выполняется равенство $\lambda = k - \lambda$.*

Итак, все симметричные (v,k,λ)-схемы порождают оптимальные троичные равновесные эквидистантные коды с параметрами (9), которые лежат на границе Джонсона (1). Если же симметричная схема является к тому же $(4\lambda-1, 2\lambda, \lambda)$-схемой, то она порождает оптимальный четверичный равновесный эквидистантный код с параметрами (10), также лежащий на границе Джонсона (1). Присоединяя к этому коду нулевое слово, получим четверичный код, лежащий на границе Плоткина. Такие четверичные коды из симметричных схем уже были построены ранее [4].

3. Построенные в предыдущем разделе троичные и четверичные коды, лежащие на границе Джонсона (см. теорему 1), согласно утверждению 1 являются посимвольно равномерными. Параметры (m,t) этих кодов легко вычисляются через параметры симметричных (v,k,λ)-схем. Например, у таких троичных кодов $m = v - 2(k-\lambda)$, $t = k - \lambda$. В [5,6] были приведены семейства q-ичных эквидистантных равновестных кодов, лежащих на границе Джонсона, – эти коды в силу утверждения 1 являются посимвольно равномерными, и их параметры также легко вычисляются. Возникает естественный вопрос: при любых ли значениях параметров q,m,t существует посимвольно равномерный код, лежащий на границе Джонсона при $m \neq t$ и Плоткина при $m = t$? Согласно утверждению 1 и следствию 1 этот вопрос эквивалентен следующему: при любых ли значениях этих параметров существует посимвольно равномерный эквидистантный код? Ответ почти очевиден: при любых значениях параметров q,m,t такой код существует. Действительно, любая матрица размера

$$N \times \frac{N!}{N_0!\,N_1!\ldots N_{q-1}!},$$

состоящая из всех столбцов заданной композиции $N_0 + N_1 + \ldots + N_{q-1} = N$ над q-ичным алфавитом, представляет собой эквидистантный код длины n с расстоянием d, где

$$n = \frac{N!}{N_0!\,N_1!\ldots N_{q-1}!}, \quad d = n - \sum_{i=0}^{q-1} \frac{(N-2)!}{N_0!N_1!\ldots(N_i-2)!\ldots N_{q-1}!},$$

и числом кодовых слов, равным N. Следовательно, это верно и для композиции посимвольно равномерного кода, где $N = m + (q-1)t$ и $N_0 = m$, $N_1 = \ldots = N_{q-1} = t$. Поэтому интерес представляет задача построения эквидистантных кодов минимальной длины при заданных параметрах q,m,t. Но даже при $m = t$, т.е. для кодов, лежащих на границе Плоткина, эта задача далека от завершения, хотя в работах [2,7] такие коды были построены для многих пар параметров (q,t) (в частности, когда q и t являются произвольными степенями любого простого числа p). Тем более интересна такая задача для случая $m \neq t$. Мы рассмотрим первый самый простой случай $m = 3$, $t = 2$, когда число кодовых слов $N = 3 + (q-1)2 = 2q+1$. Начнем с нижней оценки минимальной длины. Так как посимвольно равномерный эквидистантный код при $m \neq t$ равновесен, то нетрудно видеть, что $wN = n(N-m)$. Отсюда и из равенства (7) получаем, что

$$d = \frac{(N-m)(N+m-t)n}{N(N-1)}. \tag{11}$$

Подставляя в это равенство значения $m = 3$, $t = 2$ и учитывая, что $N = 2(q-1)+3 = 2q+1$, получаем

$$d = \frac{(N+1)(N-3)n}{N(N-1)} = \frac{2(q-1)(q+1)n}{q(2q+1)}.$$

Из целочисленности d вытекает следующее легко проверяемое

Утверждение 4. *Пусть n – длина q-ичного эквидистантного посимвольно равномерного кода ($m = 3$, $t = 2$). Тогда*

1. *Если q нечетно и $q \not\equiv 1 \pmod 6$, то $n \geqslant q(2q+1)$;*
2. *Если q нечетно и $q \equiv 1 \pmod 6$, то $n \geqslant q(2q+1)/3$;*
3. *Если q четно и $q \not\equiv 4 \pmod 6$, то $n \geqslant q(2q+1)/2$;*
4. *Если q четно и $q \equiv 4 \pmod 6$, то $n \geqslant q(2q+1)/6$.*

Хотя мы полагаем, что указанные нижние границы минимальной длины достигаются во всех четырех случаях, здесь мы докажем это лишь для первого и третьего. В обоих этих случаях указывается способ построения эквидистантных кодов, минимальная длина которых не превосходит $q(2q+1)$ при любом q и не превосходит $q(2q+1)/2$ при четных q.

Утверждение 5. *Минимальная длина q-ичного эквидистантного посимвольно равномерного кода ($m = 3$, $t = 2$) не превосходит $q(2q+1)$.*

Доказательство. Рассмотрим матрицу размера $(2q+1)\times n$ кодовых слов посимвольно равномерного кода. В любом столбце (длины $2q+1$) этой матрицы каждый ненулевой символ встречается два раза, а нулевой символ – три раза. Перенумеруем строки кодовой матрицы целыми числами удобным для дальнейших описаний образом: первая строка получит номер q, вторая $q-1$ и т.д., последняя строка получит номер $-q$ (т.е. номера строк заполняют целочисленный отрезок $[-q, q]$). Каждый столбец кодовой матрицы индуцирует набор из q непересекающихся подмножеств номеров строк – одно подмножество мощности три, состоящее из номеров строк, содержащих нулевой символ в данном столбце (далее называемое тройкой), остальные $q-1$ подмножеств мощности два, состоящие из номеров строк, содержащих одинаковый ненулевой символ в данном столбце (далее называемые парой). Такой набор, индуцированный j-м столбцом, будем обозначать через V_j, $j = 1, 2, \ldots, n$. Дистанционные свойства кода полностью определяются этими наборами, так как расстояние Хэмминга между двумя кодовыми словами с номерами u и u', $u \neq u'$, равно

$$d(u, u') = n - \left(\text{число пар } \{u, u'\} \text{ в } \bigcup_{j=1}^{n} V_j\right)$$

(каждая тройка в V_j, $j = 1, 2, \ldots, n$, заменена на три соответствующие пары, так что каждый набор V_j содержит $q+2$ пар). Отсюда вытекает, что если каждая пара номеров кодовых слов встречается в $\bigcup_{j=1}^{n} V_j$ одинаковое число раз, то код является эквидистантным. К построению наборов, обладающих этим свойством, мы и переходим. Сначала построим следующие q наборов V_u, $u = 1, 2, \ldots, q$ (назовем их генераторами):

$$V_u = \{u, 0, -u\} \cup \bigcup_{\substack{v=1,\ldots,q \\ v\neq u}} \{v, -v\}.$$

Очевидно, что в $\bigcup_{u=1}^{q} V_u$ каждая пара $\{v, -v\}$ входит q раз, и по одному разу входит каждая пара $\{v, 0\}$ и пара $\{0, -v\}$, $v = 1, 2, \ldots, q$ (напомним, что каждая тройка $\{u, 0, -u\}$ заменяется на три пары $\{u, -u\}$, $\{u, 0\}$, $\{0, -u\}$).

Проделав все циклические сдвиги наших генераторов, получим $n = q(2q+1)$ наборов V_j, $j = 1, 2, \ldots, n$. Докажем теперь, что каждая пара $\{u, u'\}$, $u \neq u'$ (таких пар всего $q(2q+1)$), входит в $\bigcup_{j=1}^{n} V_j$ одинаковое число раз, а именно $q+2$ раз.

Назовем орбитой $O(\{u,u'\})$ пары $\{u,u'\}$ множество пар, полученных из этой пары всеми ее $2q+1$ сдвигами на пары вида x,x:

$$O(\{u,u'\})=\{\{u+x,u'+x\},\ x\in[-q,q]\}$$

(операция сложения выполняется по модулю $(2q+1)$ в классе вычетов $[-q,q]$). Следующие свойства орбиты очевидны: а) все пары в орбите различны; б) пара $\{v,v'\}$ тогда и только тогда принадлежит орбите $O(\{u,u'\})$, когда $|v-v'|=|u-u'|$. Из свойства б) следует, что орбиты пар $O(\{u,u'\})$ и $O(\{v,v'\})$ либо совпадают, либо не пересекаются. Обозначим через $O(V_1,\ldots,V_q)$ множество орбит (с повторениями), порожденных всеми парами, входящими во все генераторы ($|O(V_1,\ldots,V_q)|=q(q+2)$, так как число генераторов равно q, а число пар в каждом генераторе равно $q+2$). Согласно построению V_j число пар $\{u,u'\}, u\neq u'$, в $\bigcup\limits_{j=1}^{n}V_j$ равно числу орбит из $O(V_1,\ldots,V_q)$, которым принадлежит пара $\{u,u'\}$. Следовательно, для эквидистантности кода достаточно доказать, что каждая пара принадлежит одному и тому же числу таких орбит.

Рассмотрим сначала все пары $\{v,-v\}$, $v=1,\ldots,q$, принадлежащие одному генератору V_u. Нетрудно видеть, что орбиты этих пар не пересекаются, а так как каждая орбита содержит $2q+1$ различных пар, то любая пара $\{u,u'\}$, $u\neq u'$, принадлежит одной такой орбите. Так как все генераторы включают набор пар $\{v,-v\}$, $v=1,\ldots,q$, то любая пара $\{u,u'\}$, $u\neq u'$, принадлежит q таким орбитам. Осталось рассмотреть пары $\{v,0\}$ и $\{0,-v\}$, $v=1,\ldots,q$. Очевидно, что орбиты пар $\{v,0\}$, $v=1,\ldots,q$, не пересекаются, и любая пара $\{u,u'\}$, $u\neq u'$, принадлежит одной такой орбите. Орбиты же пары $\{0,-v\}$ совпадают с орбитами пары $\{v,0\}$, и следовательно, любая пара $\{u,u'\}$, $u\neq u'$, принадлежит $q+2$ орбитам.

Напомним теперь, что наборы V_j были индуцированы столбцами кодовой матрицы, так что обратное преобразование этих наборов в столбцы кодовой матрицы очевидно – каждый набор превращается в столбец длины $2q+1$ кодовой матрицы по следующему правилу: на места, определяемые тройкой набора, ставится нулевой символ, а на места, определяемые парами набора, ставятся одинаковые ненулевые символы (различные пары набора должны содержать различные символы алфавита). Ясно, что такой код является q-ичным посимвольно равномерным ($m=3$, $t=2$) эквидистантным кодом мощности $N=2q+1$ длины $n=q(2q+1)$ с расстоянием $d=q(2q+1)-q-2=2(q^2-1)$. ▲

Из этого утверждения и п. 1 утверждения 4 вытекает

С л е д с т в и е 2. *Если q нечетно и $q\not\equiv 1 \pmod 6$, то минимальная длина q-ичного эквидистантного посимвольно равномерного кода ($m=3$, $t=2$) равна $q(2q+1)$.*

В случае четного q имеет место

У т в е р ж д е н и е 6. *Если q четно, то минимальная длина q-ичного эквидистантного посимвольно равномерного кода ($m=3$, $t=2$) не превосходит $q(2q+1)/2$.*

Д о к а з а т е л ь с т в о. Пусть $q=2s$. Построение наборов V_j весьма похоже на построение наборов при доказательстве утверждения 5, но число генераторов будет в два раза меньше, и поэтому после циклических сдвигов генераторов общее число наборов окажется в два раза меньше, чем в утверждении 5. При этом $s-1$ генераторов входят в число генераторов утверждения 5, а именно

$$V_{2u}=\{2u,0,-2u\}\cup\bigcup_{\substack{v=1,\ldots,q\\ v\neq 2u}}\{v,-v\},\quad u=2,\ldots,s,$$

и лишь один генератор (обозначим его через V_1) строится особым способом:

$$V_1 = \{2s-1, 0, -(2s-1)\},\ \{2s, -2s\},\ \{s, s-2\}, \{s+1, s-1\},$$
$$\{-(s-2), -(s+1)\},\ \{-(s-1), -s\},$$
$$\bigcup_{v=1,\dots,s-3} \{v, 2s-1-v\},\quad \bigcup_{v=1,\dots,s-3} \{-v, -(2s-1-v)\}.$$

Как и в утверждении 5, достаточно доказать, что каждая пара $\{u, u'\}$, $u \neq u'$, принадлежит одному и тому же числу орбит, порожденных всеми парами, входящими в генераторы. Рассмотрим сначала пары $\{2u, 0\}$ и $\{-2u, 0\}$, $u = 2, \dots, s$, входящие в $s-1$ генераторов. Орбиты этих пар совпадают, и поэтому каждая пара $\{u, u'\}$ такая, что $|u-u'| = 4, 6, \dots, 2s$, принадлежит этим двум орбитам. Далее рассмотрим орбиты, принадлежащие парам, входящим в генератор V_1. Орбиты пар $\{s, s-2\}$ и $\{s+1, s-1\}$ совпадают, так как $|s-(s-2)| = |s+1-(s-1)| = 2$, и поэтому любая пара $\{u, u'\}$, $|u-u'| = 2$, принадлежит орбитам этих двух пар. Орбиты пар $\{2s, -2s\}$ и $\{-(s-1), -s\}$ совпадают, так как $|2s+2s| = |-(s-1)+s| = 1$, и поэтому любая пара $\{u, u'\}$, $|u-u'| = 1$, принадлежит орбитам этих двух пар. Орбиты пар $\{2s-1, -(2s-1)\}$ и $\{-(s-2), -(s+1)\}$ совпадают, так как $|2s-1+(2s-1)| = |-(s-2)+(s+1)| = 3$, и поэтому любая пара $\{u, u'\}$, $|u-u'| = 3$, принадлежит орбитам этих двух пар. Орбиты пар $\{v, 2s-1-v\}$ и $\{-v, -(2s-1-v)\}$, $v = 0, 1, \dots, s-3$ (пары $\{0, 2s-1\}$ и $\{0, -(2s-1)\}$ при $v = 0$ получены из тройки $\{2s-1, 0, -(2s-1)\}$), совпадают, и следовательно, любая пара $\{u, u'\}$, $|u-u'| = 5, 7, \dots, 2s-1$, принадлежит двум орбитам.

Кроме того, в утверждении 5 мы доказали, что любая пара $\{u, u'\}$, $u \neq u'$, принадлежит $q-1$ орбитам тех пар из $s-1$ генераторов, которые мы еще не использовали. Поэтому q-ичный код, полученный из $n = q(2q+1)/2$ наборов V_j способом, указанным в утверждении 5, является эквидистантным кодом мощности $N = 2q+1$ и длины $n = q(2q+1)/2$ с расстоянием

$$d = \frac{q(2q+1)}{2} - \frac{q}{2} - 1 = q^2 - 1. \quad \blacktriangle$$

Из этого утверждения и п. 3 утверждения 4 вытекает

С л е д с т в и е 3. *Если q четно и $q \not\equiv 4 \pmod 6$, то минимальная длина q-ичного эквидистантного посимвольно равномерного кода* ($m = 3$, $t = 2$) *равна* $q(2q+1)/2$.

Замечание. Соотношение (11) с учетом равенства $N = (q-1)t + m$ и целочисленности d позволяет получать нижние оценки минимальной длины и для произвольных параметров q, m, t. Для конкретных кодов эти нижние оценки оказываются иногда точными (например, они оказываются таковыми для всех троичных кодов из теоремы 1, лежащих на границе Джонсона, при условии, что $(k-\lambda)(2v-3(k-\lambda))$ и $v(v-1)$ взаимно просты).

СПИСОК ЛИТЕРАТУРЫ

1. *Бассальыго Л.А.* Новые верхние границы для кодов, исправляющих ошибки // Пробл. передачи информ. 1965. Т. 1. № 4. С. 41–44.
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.
3. *Beth T., Jungnickel D., Lenz B.* Design Theory. Cambridge: Cambridge Univ. Press, 1999.
4. *Sinha K., Sinha N.* A Class of Optimal Quaternary Codes // Ars Combin. 2010. V. 94. P. 61–64.

5. *Бассалыго Л.А., Зиновьев В.А.* Замечание об уравновешенных неполных блок-схемах, почти разрешимых блок-схемах и q-ичных равновесных кодах // Пробл. передачи информ. 2017. Т. 53. № 1. С. 55–58.
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.
7. *Семаков Н.В., Зиновьев В.А., Зайцев Г.В.* Класс максимальных эквидистантных кодов // Пробл. передачи информ. 1969. Т. 5. № 2. С. 84–87.

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

Поступила в редакцию
07.02.2020
После доработки
11.06.2020
Принята к публикации
14.06.2020