ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 2000. Серия 1. Том 7, № 4, 101–110

УДК 519.72

СОВЕРШЕННЫЕ ДВОИЧНЫЕ КОДЫ И СИСТЕМЫ ТРОЕК ШТЕЙНЕРА С МАКСИМАЛЬНЫМИ ПОРЯДКАМИ ГРУПП АВТОМОРФИЗМОВ*)

Ф. И. Соловьева, С. Т. Топалова

Доказано, что порядок группы автоморфизмов кода Хемминга является единственным максимально возможным порядком среди порядков групп автоморфизмов всех совершенных кодов той же длины. Установлено, что система троек Штейнера порядка n с максимальным порядком группы автоморфизмов, равным порядку полной линейной группы $GL(\log(n+1),2)$, единственна с точностью до изоморфизма и содержится в коде длины n.

Введение

В работах [4, 5] доказано, что порядок группы автоморфизмов произвольного нелинейного совершенного двоичного кода с расстоянием 3 (далее совершенного кода) не больше порядка группы автоморфизмов кода Хемминга той же длины. Там же была получена верхняя оценка порядка группы автоморфизмов произвольной системы Штейнера $S(t, t+1, n)$ и, в частности, системы троек Штейнера $\mathrm{STS}(n)$ порядка n. Оставался открытым вопрос о существовании нелинейного совершенного кода с порядком группы автоморфизмов, равным порядку группы автоморфизмов кода Хемминга той же длины. В настоящей статье дан отрицательный ответ, а именно установлено, что порядок группы автоморфизмов кода Хемминга является единственным максимально возможным порядком среди порядков групп автоморфизмов всех совершенных кодов той же длины. Доказано, что порядок группы автоморфизмов произвольной системы троек Штейнера строго меньше порядка группы автоморфизмов системы троек Штейнера, связанной с кодом Хемминга (известно [2], что кодовые слова веса 3 совершенного двоичного кода длины n, содержащего нулевое слово, образуют систему троек Штейнера $\mathrm{STS}(n)$ порядка

*) Исследование первого автора выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 00–01–00822); исследование второго автора выполнено при финансовой поддержке Болгарского фонда фундаментальных исследований (проект I–803/1998).

n). Из доказанного, как следствие, вытекают такие же утверждения для систем четверок Штейнера и расширенных совершенных кодов.

Авторам стало известно, что С. А. Малюгин [3] другим способом установил следующий факт: порядок группы автоморфизмов кода Хемминга по крайней мере в два раза больше порядка группы автоморфизмов любого нелинейного совершенного кода той же длины.

Обзор известных результатов по группам автоморфизмов совершенных двоичных кодов см. в [4].

1. Определения

Совершенным двоичным кодом C длины n называется такое подмножество n-мерного векторного пространства E^n над $GF(2)$, что шары радиуса 1 (в метрике Хемминга) с центрами в C не пересекаются и в совокупности покрывают E^n (такие коды существуют только при $n = 2^k - 1$, $k > 1$; далее всюду n имеет такой вид). Два кода длины n называются *эквивалентными*, если существует изометрия пространства E^n, отображающая один код в другой. Известно, что каждая такая изометрия представима отображением $A_\pi^v : u \to \pi(u) + v$, где π — подстановка длины n координат и $v \in E^n$. *Группа автоморфизмов* $\mathrm{Aut}(C)$ произвольного кода $C \subseteq E^n$ состоит из всех изометрий A_π^v куба E^n, отображающих код на себя. Пусть $\mathrm{Sym}(C) = \{A_\pi^0 \mid A_\pi^0(C) = C\}$ обозначает *группу подстановочных автоморфизмов* кода C, а $\mathrm{Ker}(C) = \{A_e^v \mid A_e^v(C) = C\}$ — его *ядро* (здесь $\mathbf{0}$ — нулевой вектор пространства E^n, e — тождественная подстановка длины n). Поскольку для кода C, например нелинейного совершенного двоичного кода, являющегося Z_4-линейным (классификацию Z_4-линейных совершенных кодов см. в [1]), может существовать такой автоморфизм A_π^v, т. е. $A_\pi^v(C) = C$, что $\pi(C) \neq C$ и $v + C \neq C$, то не всегда $\mathrm{Aut}(C) = \mathrm{Sym}(C) \times \mathrm{Ker}(C)$, где $\times$ означает полупрямое произведение. Для любого линейного кода C, очевидно, $\mathrm{Aut}(C) = \mathrm{Sym}(C) \times \mathrm{Ker}(C)$. Известно (см., например, [2]), что для кода Хемминга H длины n выполняются соотношения $\mathrm{Aut}(H) \cong GL(\log(n+1), 2) \times H$ и

$$|\mathrm{Aut}(H)| = 2^{n - \log(n+1)} N_1,$$

где

$$N_1 = |GL(\log(n+1), 2)| = n(n-1)(n-2^2+1)(n-2^3+1)\ldots(n-(n-1)/2) \tag{1}$$

(здесь и далее $\log n$ обозначает логарифм по основанию 2).

Системой Штейнера $S(t, k, n)$ на множестве $N = \{1, 2, \ldots, n\}$ называется такая система k-элементных подмножеств (блоков) из N, что каждое неупорядоченное t-элементное подмножество из N содержится точно в одном блоке системы [2]. Система $S(2, 3, n)$ называется *системой*

троек Штейнера STS(n) порядка n, а ее блоки называются *тройками*. Система $S(3,4,n)$ называется *системой четверок Штейнера* SQS(n) порядка n. Группа автоморфизмов $\mathrm{Aut}(S(t,k,n))$ произвольной системы $S(t,k,n)$ состоит из всех подстановок множества N, переводящих блоки системы в блоки системы.

Стабилизатором элемента x множества $N = \{1,2,\ldots,n\}$ называется подгруппа G_x группы подстановок G, которая действует на N и состоит из всех подстановок группы G, оставляющих неподвижным элемент x. *Стабилизатором* множества $X = \{1,\ldots,i\} \subset N$ называется подгруппа группы подстановок G, которая состоит из всех подстановок, оставляющих неподвижным каждый элемент множества X. Обозначим эту подгруппу через $G_{X(i)}$. Через l_x обозначается длина орбиты элемента x, т. е. число элементов, в которые он переходит под действием группы автоморфизмов.

2. Системы троек Штейнера с группой автоморфизмов максимального порядка

Лемма [4, лемма]. *Если $S(2,3,n)$ имеет автоморфизм с m неподвижными элементами, $m \geqslant 2$, то она содержит подсистему $S(2,3,m)$, $m \leqslant (n-1)/2$.*

Теорема 1. *Пусть* STS(n) *такова, что* $|\mathrm{Aut}(\mathrm{STS}(n))| = N_1$, *где* N_1 *определено в* (1). *Тогда при каждом* $m = 2^k - 1$, $2 \leqslant k \leqslant \log(n+1) - 1$, *справедливы утверждения*:

1) *в* $\mathrm{Aut}(\mathrm{STS}(n))$ *имеется автоморфизм, множество M неподвижных элементов которого состоит из m элементов, а стабилизатор $G_M(m)$ транзитивен*;

2) *в* STS(n) *содержится такое множество систем* STS(3),..., STS(m),..., *что каждая система содержится в последующей системе.*

Доказательство. Сначала докажем, что для любой STS(n) справедливо неравенство $|\mathrm{Aut}(\mathrm{STS}(n))| \leqslant N_1$ (см. теорему 1 из [4]). Отсюда будет понятна структура $\mathrm{Aut}(\mathrm{STS}(n))$ с $|\mathrm{Aut}(\mathrm{STS}(n))| = N_1$. Порядок группы автоморфизмов STS(n) можно подсчитать с помощью известной теоремы теории конечных групп подстановок [7]: если G — конечная группа подстановок, G_x — стабилизатор элемента x, а l_x — длина орбиты элемента x, то $|G| = l_x|G_x|$. В силу этой теоремы $|G| = l_0 \cdot l_1 \cdot l_2 \cdot \ldots \cdot l_{n-1}$, где l_i — длина орбиты $(i+1)$-го элемента относительно стабилизатора $G_{X(i)}$ множества $X = \{1,\ldots,i\}$.

Если ограничение блоков STS(n) на множество X не образует систему троек Штейнера, то согласно лемме на множестве всех элементов, неподвижных относительно $G_{X(i)}$, имеется система троек Штейнера. Занумеруем элементы STS(n) так, что для каждого $i < n$ выполняется

следующее: если относительно стабилизатора $G_{X(i)}$ имеется еще $m-i$ неподвижных элементов, то они имеют номера $i+1,\dots,m$. Таким образом, если $i>1$ и первые i элементов не образуют STS, то $l_i=1$. Отсюда следует, что $l_0\cdot l_1\cdot\ldots\cdot l_{n-1}=l_{m_0}\cdot l_{m_1}\cdot\ldots\cdot l_{m_s}$, где $s<n$, $l_{m_k}\neq 1$ и относительно стабилизатора $G_{X(m_k)}$ нет других неподвижных элементов. В силу того, что относительно $G_{X(m)}$ длина орбиты любого элемента не больше $n-m$, имеем $l_{m_k}\leqslant n-m_k$ и для максимально возможного порядка группы автоморфизмов $\mathrm{STS}(n)$ получаем

$$|\mathrm{Aut}(\mathrm{STS}(n))|\leqslant(n-m_0)(n-m_1)\dots(n-m_s).$$

При выбранном порядке элементов согласно лемме величина m_k равна либо нулю, либо единице, либо порядку STS, причем эти системы содержатся друг в друге, т. е. $\mathrm{STS}(m_{k+1})$ содержит подсистему $\mathrm{STS}(m_k)$, $k=0,1,\dots,s-1$. По лемме имеем $2m_k+1\leqslant m_{k+1}$. Так как $m_0=0$ и $m_1=1$, то $m_k\geqslant 2^k-1$, где $2<k\leqslant\log(n+1)-1$. Поэтому $|\mathrm{Aut}(\mathrm{STS}(n))|\leqslant n(n-2^1+1)(n-2^2+1)\dots(n-2^{\log(n+1)-1}+1)=N_1$.

Отсюда следует, что если $|\mathrm{Aut}(\mathrm{STS}(n))|=N_1$, то имеются автоморфизмы с $m_k=2^k-1$ неподвижными элементами и подсистемы троек Штейнера порядка m_k, содержащиеся друг в друге, где $0\leqslant k\leqslant\log(n+1)-1$. Длина орбиты любого неподвижного элемента в $G_{X(m_k)}$ равна $n-m_k$, т. е. стабилизатор транзитивен. Теорема доказана.

Утверждение 1. *Пусть* $\mathrm{STS}(n)$ *такова, что* $|\mathrm{Aut}(\mathrm{STS}(n))|=N_1$, *где* N_1 *определено в* (1), *и существует автоморфизм с множеством неподвижных элементов* M, $|M|=m$. *Тогда при любом* $m=2^k-1$, $2\leqslant k\leqslant\log(n+1)-1$,

1) *справедливо* $N\setminus M=\bigcup\limits_{i=1}^{(n-m)/(m+1)}A_i$, *где* $|A_i|=m+1$, *и на множестве* $M\cup A_i$ *существует подсистема порядка* $2m+1$; *других подсистем такого порядка, определенных на любом множестве, содержащем* M, *нет*;

2) *существует автоморфизм системы* $\mathrm{STS}(n)$, *оставляющий неподвижным множество* $M\cup A_i$.

Доказательство. Пусть Δ — произвольная $\mathrm{STS}(n)$ с $|\mathrm{Aut}(\mathrm{STS}(n))|=N_1$. По теореме 1 стабилизатор G_M транзитивен. Поэтому для любого элемента $x\in N\setminus M$ существует такой автоморфизм φ системы Δ, что $\varphi(M)=M$ и $\varphi(x)=x$, т. е. φ оставляет неподвижными элементы произвольной тройки $(x,y,z)\in\Delta$, где $y\in M$, а $z\in N\setminus M$. Следовательно, φ оставляет неподвижным подмножество $A_1\subset N\setminus M$ мощности $m+1$. По теореме 1 на множестве $M\cup A_1$ определена подсистема порядка $2m+1$.

Если взять автоморфизм, переводящий элемент $x \in A_1$ в любой элемент $y \in (N \setminus M) \setminus A_1$ (что обеспечивается теоремой 1), то получим множество A_2, отличное от A_1 и равномощное ему, и т. д. В силу конечности множества N и того, что число $(n-m)/(m+1)$ целое, получаем разбиение множества $N \setminus M$ и требуемую серию подсистем порядка $2m+1$. Нетрудно видеть, что любая подсистема порядка $2m+1$, определенная на множестве, содержащем множество M, совпадает с одной из полученных подсистем. Утверждение 1 доказано.

Следующее утверждение в статье не используется, но представляет самостоятельный интерес.

Утверждение 2. *Пусть* $\mathrm{STS}(n)$ *такова, что* $|\mathrm{Aut}(\mathrm{STS}(n))| = N_1$, *где* N_1 *определено в* (1). *Тогда при* $m = 2^k - 1$, $2 \leqslant k \leqslant \log(n+1) - 1$, *все подсистемы* $\mathrm{STS}(m)$ *порядка* m *системы* $\mathrm{STS}(n)$ *изоморфны.*

Доказательство. Рассмотрим два произвольных непересекающихся множества A_i и A_j, $i \neq j$, которые удовлетворяют утверждению 1. В силу транзитивности стабилизатора $G_M(m)$ существует автоморфизм φ системы Δ, переводящий произвольный элемент из множества A_i в произвольный элемент множества A_j. При этом $\varphi(A_i) = A_j$ и $\varphi(M) = M$. По утверждению 1 на множествах $M \cup A_i$ и $M \cup A_j$ существуют подсистемы порядка $2m+1$. Так как $\varphi(M \cup A_i) = M \cup A_j$, то подстановка φ переводит подсистему, определенную на множестве $M \cup A_i$, в подсистему, определенную на $M \cup A_j$, т. е. эти подсистемы изоморфны. Отсюда с учетом единственности (с точностью до изоморфизма) $\mathrm{STS}(3)$ и $\mathrm{STS}(7)$ получаем по индукции изоморфизм всех подсистем порядка $2m+1$. Утверждение доказано.

Наряду с координатным представлением вектора $x = (x_1, \ldots, x_n)$ далее будем рассматривать его блочную запись $(i_1, \ldots, i_k)$, где $i_1, \ldots, i_k$ — номера единичных координат вектора x.

В работе [6] указан индуктивный способ построения базы кода Хемминга среди кодовых слов веса 3. $\mathrm{STS}(n)$ будем называть *хеммингово́й*, если она содержится в коде Хемминга длины n. Очевидно, что хеммингова STS порождается базисом своего кода Хемминга, т. е. каждая ее тройка является линейной комбинацией базисных троек.

Теорема 2. *Если порядок группы автоморфизмов произвольной системы троек Штейнера порядка* n *равен порядку линейной группы* $GL(\log(n+1), 2)$, *то эта система хеммингова и с точностью до изоморфизма единственна.*

Доказательство будем проводить по индукции. По теореме 1 имеем последовательность, составленную из вложенных друг в друга подсистем Δ^m порядка $m = 2^k - 1$ и автоморфизмов с неподвижными

элементами множества $M = \{1, \ldots, m\}$ при всех $m = 2^k - 1$, $2 \leqslant k \leqslant \log(n+1) - 1$. Рассмотрим подсистемы Δ^m на M и Δ^{2m+1} на $M' = \{1, 2, \ldots, 2m+1\}$, $\Delta^m \subset \Delta^{2m+1}$.

Если $m = 3$, то Δ^3 и Δ^7 хемминговы и единственны с точностью до изоморфизма.

Пусть подсистема Δ^m является хемминговой, единственной и порождена базой B^m мощности $m - \log(m+1)$. Из определения STS следует, что для любой тройки (x, y, z) из Δ^{2m+1} либо $(x, y, z) \in \Delta^m$, либо $x \in M$, а $y, z \in M' \setminus M$. Следовательно, пара $(x, 2m+1)$ однозначно определяет тройку $(x, x', 2m+1) \in \Delta^{2m+1}$ при любом $x \in M$ и некотором $x' \in M' \setminus M$. Множество всех таких троек обозначим через B. Эти тройки линейно независимы и, как видно, вместе с базой B^m системы Δ^m образуют линейно независимое множество троек $B^{2m+1} = B^m \cup B$ мощности $2m - \log(m+1)$.

Докажем, что B^{2m+1} является базой для Δ^{2m+1}. Это очевидно для $(x, y, z) \in \Delta^m$, поскольку B^m является базой для системы Δ^m, где $B^m \subset B^{2m+1}$. Пусть $(x, y, z) \notin \Delta^m$ и $x \in M$. Тогда $y, z \in M' \setminus M$. В силу транзитивности стабилизатора тройки (x, y, z) найдется автоморфизм с неподвижными элементами тройки (x, y, z) и элементом $2m+1$. По утверждению 1 этот автоморфизм оставляет неподвижным семиэлементное множество X, содержащее элементы $x, y, z, 2m+1$, и существует подсистема $\Delta^7 \subset \Delta^{2m+1}$ порядка 7, определенная на X. Эта подсистема хемминга, и поэтому тройка (x, y, z) является линейной комбинацией троек из Δ^7. В частности, нетрудно видеть, что

$$(x, y, z) = (a, z, 2m+1) \oplus (b, y, 2m+1) \oplus (x, a, b),$$

где $(x, a, b) \in \Delta^m$, $a, b \in X$ и по предположению индукции является линейной комбинацией троек из B^m, а $(a, z, 2m+1), (b, y, 2m+1) \in B$. В силу произвольности тройки $(x, y, z) \in \Delta^{2m+1}$ получаем, что Δ^{2m+1} порождается множеством $B^{2m+1} = B^m \cup B$.

Докажем, что B^{2m+1} не может породить вектор веса меньше 3. Для суммы любых троек из B^m это ясно из предположения индукции. Сумма любых троек из B имеет вес не меньше 4. Так как каждая тройка из $\Delta^{2m+1} \setminus \Delta^m$ содержит две ненулевые координаты из множества $M' \setminus M$ и одну из M, то сумма произвольного числа троек из B^m с тройками из B имеет вес не меньше 3. Следовательно, B^{2m+1} порождает линейный код длины n (напомним, что n — длина кода Хемминга) с минимальным расстоянием 3, а код Хемминга единствен (см. [2]). Поэтому система Δ^{2m+1} хемминга и единственна. Следовательно, в силу произвольности m система Δ^n хемминга и единственна с точностью до изоморфизма. Теорема 2 доказана.

3. Совершенные двоичные коды с группой автоморфизмов максимального порядка

Напомним, что совокупность кодовых слов, находящихся на расстоянии 3 от фиксированного кодового слова v любого совершенного двоичного кода, образует STS в коде $C + v$. Эту систему обозначим через Δ_v, систему Δ_0 — через $\Delta = \mathrm{STS}(C)$, а любую подсистему порядка m системы Δ_v — через Δ_v^m.

Утверждение 3. *Пусть C — произвольный совершенный код. Тогда все автоморфизмы системы $\Delta = \mathrm{STS}(C)$, оставляющие неподвижным вектор $v \in C$, являются автоморфизмами системы Δ_v.*

Доказательство. Рассмотрим произвольный подстановочный автоморфизм φ кода C и, следовательно, системы троек Δ с неподвижными элементами тройки v. Для автоморфизма φ системы Δ и $u \in \Delta_v$ имеем $v + u \in C$ и $\varphi(v + u) = \varphi(v) + \varphi(u) = v + \varphi(u) \in C$. Отсюда следует, что $\varphi(u) \in \Delta_v$. Поэтому все автоморфизмы Δ, оставляющие неподвижным v, являются автоморфизмами системы Δ_v.

Утверждение 4. *Пусть C — произвольный совершенный код с группой автоморфизмов максимального порядка. Тогда для любого автоморфизма систем $\Delta = \mathrm{STS}(C)$ и Δ_v с множеством неподвижных элементов $X, |X| = 7$, и любой тройки $v \in \Delta$ с элементами из X справедливо равенство $\Delta^7 = \Delta_v^7$, где подсистемы Δ^7, Δ_v^7 определены на X, $\Delta^7 \subset \Delta$, $\Delta_v^7 \subset \Delta_v$.*

Доказательство. Рассмотрим автоморфизм системы Δ с семиэлементным множеством неподвижных элементов X и тройки $v, u \in \Delta$ такие, что $v, u \subset X, u \neq v$. По теореме 1 существуют подсистемы $\Delta_v^7 \subset \Delta_v$ и $\Delta_u^7 \subset \Delta_u$, построенные на X, где $v \in \Delta_v^7$ и $u \in \Delta_u^7$.

Поскольку STS(7) единственна с точностью до изоморфизма и является хемминговой, то нетрудно проверить, исходя из ее строения, что для любого $w \in \Delta_v^7, w \neq v$, множество $v + \Delta_v^7$ содержит четверку $X \setminus w$, которая по определению Δ_v принадлежит коду C. Пусть $\Delta_v^7 \neq \Delta_u^7$. Тогда найдется пара (i, j) такая, что $(i, j, k) \in \Delta_v^7$ и $(i, j, l) \in \Delta_u^7$, где $k \neq l$. Отсюда и из предыдущего следует, что $X \setminus \{i, j, k\} \in C$ и $X \setminus \{i, j, l\} \in C$, но $d(X \setminus \{i, j, k\}, X \setminus \{i, j, l\}) = w(\{k, l\}) = 2$. Это противоречит плотной упакованности кода C. Следовательно, $\Delta_v^7 = \Delta_u^7$ и в силу произвольности выбора $u, v \in \Delta^7$ имеем $\Delta^7 = \Delta_v^7$. Утверждение доказано.

В [5, предложение 4] (см. также [4, предложение 2]) доказано, что

$$|\mathrm{Aut}(C)| = |T(C)| \cdot |\mathrm{Sym}(C)|, \tag{2}$$

где $T(C)$ — множество таких векторов $v \in E^n$, что существует подстановка $\pi_v \in S_n$ такая, что $\pi_v(C) + v = C$ (здесь π_v не обязана принадлежать $\mathrm{Sym}(C)$).

Утверждение 5. *Пусть v — произвольная вершина нелинейного совершенного кода C такого, что $|\mathrm{Aut}(C)| = |\mathrm{Aut}(H)|$. Тогда $\Delta = \Delta_v$.*

Доказательство. Сначала докажем индукцией по $m = 2^k - 1$, где $3 \leqslant k \leqslant \log(n+1)$, что для любого $v \in C$, $w(v) = 3$, справедливо равенство $\Delta^m = \Delta_v^m$. Затем убедимся, что $\Delta = \Delta_v$ для любого $v \in C$.

Пусть $m = 7$, где $m = 2^3 - 1$. Поскольку $|\mathrm{Aut}(C)| = |\mathrm{Aut}(H)|$, то теореме 1 найдется автоморфизм системы Δ с семью неподвижными точками, среди которых содержатся элементы тройки v. Тогда по утверждению 4 для любого $v \in C$ имеем $\Delta^7 = \Delta_v^7$.

Пусть утверждение верно для $(m-1)/2 = 2^k - 1$, где $k < \log(n+1)$. Докажем, что $\Delta^m = \Delta_v^m$. По теореме 1 найдутся автоморфизм с неподвижным множеством $M = \{1, 2, ..., m\}$, где $m = 2^{k+1} - 1$, и подсистема $\Delta^m \subset \Delta$ на множестве M, причем $v \in \Delta^m$. По утверждению 3 все автоморфизмы системы Δ, оставляющие неподвижным слово $v \in \Delta$, являются автоморфизмами системы Δ_v. Следовательно, Δ_v содержит подсистему Δ_v^m на M. Подсистемы Δ^m и Δ_v^m содержат соответственно подсистемы $\Delta^{(m-1)/2}$ и $\Delta_v^{(m-1)/2}$, построенные на $M_1 = \{1, 2, ..., (m-1)/2\}$ и совпадающие по предположению индукции.

Рассмотрим произвольный элемент $i \in M_1$. По теореме 1 найдется автоморфизм φ систем Δ и Δ_v с неподвижными элементами тройки v и элементом i, т. е. $\varphi(v) = v$, $\varphi(i) = i$, и по утверждению 1 это множество может быть дополнено до множества X неподвижных элементов мощности 7, на котором существует подсистема систем Δ и Δ_v.

Рассмотрим два случая.

1) Пусть $|M_1| > 7$, т. е. $X \subset M_1$, и существует тройка $(i, j, p) \in \Delta^{(m-1)/2} = \Delta_v^{(m-1)/2}$, $j, p \notin X$. В силу транзитивности стабилизатора множества X можно выбрать автоморфизм φ систем Δ и Δ_v таким, что $\varphi(X) = X$, $\varphi(j) = m$, где $m \in M \setminus M_1$. Тогда тройка $\varphi(i, j, p) = (i, \varphi(p), m) \in \Delta^m \cap \Delta_v^m$. Поскольку $i \in M_1$ и $|M_1| = (m-1)/2$, имеем $(m-1)/2$ различных троек в $\Delta^m \cap \Delta_v^m$, содержащих элемент m. Легко проверить, что это множество вместе с базой хемминговой подсистемы $\Delta^{(m-1)/2} = \Delta_v^{(m-1)/2}$ образует линейно независимое множество троек B^m в $\Delta^m \cap \Delta_v^m$, где $|B^m| = m - \log(m+1)$. Поскольку по теореме 2 подсистемы Δ^m и Δ_v^m групповые, то B^m является их базой. Поэтому $\Delta^m = \Delta_v^m$.

2) Пусть $|M_1| = 7$, т. е. $X = M_1$ и $m = 15$. Аналогично случаю 1 найдем тройки $(i, \varphi(p), 15) \in \Delta^{15} \cap \Delta_v^{15}$ для $i \in \{l, s, q\}$, где $v = (l, s, q)$. Это множество вместе с базой групповой подсистемы $\Delta^7 = \Delta_v^7$ дает только тройки с элементами из M_1. Они, очевидно, принадлежат системе $\Delta \cap \Delta_v$. В частности, все тройки, содержащие элементы l, s или q, принадлежат системе $\Delta \cap \Delta_{(l,s,q)}$.

Допустим, что существуют $(i,j,p) \in \Delta_v^{15}$ и $(i',j,p) \in \Delta^{15}$, где $i \neq i'$, $i,i' \in M^7 \setminus \{l,s,q\}$. Тогда найдется $(l,i,i') \in \Delta^{15}$, где $v \cap (l,i,i') = \{l\}$. Так как $v = (l,s,q)$, то $(l,s,q) + (i,j,p) = (l,s,q,i,j,p) \in C$. Выше доказано, что все тройки, содержащие элементы l, i или i', принадлежат системе $\Delta \cap \Delta_{(l,i,i')}$. Отсюда и из $(i',j,p) \in \Delta^{15}$ следует, что $(i',j,p) \in \Delta_{(l,i,i')}$. По определению $\Delta_{(l,i,i')}$ имеем $(l,i,i')+(i',j,p) = (l,i,j,p) \in C$. Но $d((l,s,q,i,j,p),(l,i,j,p)) = 2$. Противоречие. Следовательно, $\Delta^{15} = \Delta_v^{15}$, что завершает индуктивный шаг.

Из $|\mathrm{Aut}(C)| = |\mathrm{Aut}(H)|$ и (2) вытекает, что код C *вершинно-транзитивен*, т. е. $T(C) = C$. Следовательно, каждое слово кода C может перейти в нулевое слово посредством некоторого автоморфизма C. Поэтому любые STS Δ_x и Δ_y совпадают для кодовых слов x и y, находящихся на расстоянии 3. В силу того, что характеристический граф совершенного кода связен, следует $\Delta = \Delta_v$ для каждого $v \in C$. Утверждение 5 доказано.

Теорема 3. *Произвольный совершенный код C с группой автоморфизмов максимального порядка эквивалентен коду Хемминга той же длины.*

Доказательство. В силу вершинной транзитивности кода C для каждого слова $v \in C$ существует подстановка φ такая, что $v+\varphi(C) = C$, т. е. $v+C = \varphi(C)$. Поэтому $\Delta_v = \varphi(\Delta)$ и по утверждению 5 подстановка φ является автоморфизмом системы Δ. Так как мощность группы автоморфизмов максимальна, то все автоморфизмы системы Δ являются подстановочными автоморфизмами кода C. Следовательно, φ — подстановочный автоморфизм кода C. Поэтому $v + C = C$ для каждого $v \in C$, что означает линейность кода. Теорема доказана.

Нетрудно видеть, что из приведенных выше результатов в качестве следствия получаются аналогичные результаты для расширенных совершенных кодов и систем четверок Штейнера.

Авторы выражают глубокую признательность Ю. Л. Васильеву за постановку задачи, а также ему и С. В. Августиновичу за ценные замечания, позволившие улучшить текст статьи.

ЛИТЕРАТУРА

1. **Кротов Д. С.** Z_4-линейные совершенные коды // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, № 4. С. 78–90.
2. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
3. **Малюгин С. А.** О порядке группы автоморфизмов совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, № 4. С. 91–100.

4. **Соловьева Ф. И., Топалова С. Т.** О группах автоморфизмов совершенных двоичных кодов и систем Штейнера // Проблемы передачи информации. 2000. Т. 36, вып. 4. С. 3–8.
5. **Solov'eva F. I., Topalova S. T.** On the automorphism groups of perfect binary codes // Algebraic and Combinatorial Coding Theory. Seventh Intern. workshop (Bansko, 18-24 June 2000). Proc. Bulgaria: Inst. of Math. and Inform., 2000. P. 283–287.
6. **Solov'eva F. I.** Structure of i-components of perfect binary codes // Discrete Appl. Math. (To appear.)
7. **Wielandt H.** Finite permutation groups. New York: Acad. Press Inc., 1964.

Адреса авторов:

Ф. И. Соловьева
Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск, Россия.
С. Т. Топалова
Institute of Mathematics
and Informatics Bulgarian
Academy of Sciences, II.K.
3235000 V. Tyrnovo, Bulgaria

Статья поступила
18 сентября 2000 г.