

О ПОРЯДКЕ ГРУППЫ АВТОМОРФИЗМОВ СОВЕРШЕННЫХ ДВОИЧНЫХ КОДОВ*)

С. А. Малюгин

Доказывается, что порядок группы автоморфизмов любого нелинейного совершенного двоичного кода длины $n = 2^k - 1$ по крайней мере в два раза меньше порядка группы автоморфизмов кода Хемминга той же длины.

Введение

Любая изометрия векторного пространства $\{0, 1\}^n$ над полем Галуа $GF(2)$ задается отображением $A_\pi^v : x \mapsto \pi(x) \oplus v$, где π — перестановка координат вектора $x \in \{0, 1\}^n$, а v — фиксированный вектор из $\{0, 1\}^n$. Группа автоморфизмов $\text{Aut}(C)$ совершенного кода $C \subset \{0, 1\}^n$ состоит из всех изометрий A_π^v таких, что $A_\pi^v(C) = C$. В $\text{Aut}(C)$ рассматриваются также две подгруппы: группа перестановочных автоморфизмов $\text{Sym}(C) = \{A_\pi^0 \mid A_\pi^0 \in \text{Aut}(C)\}$ и ядро $\text{Ker}(C) = \{A_e^v \mid A_e^v \in \text{Aut}(C)\}$ (здесь e — тождественная перестановка).

О строении группы автоморфизмов произвольного совершенного двоичного кода известно немного. В [9] доказано, что любая конечная группа может быть перестановочной группой автоморфизмов некоторого совершенного кода. В [7, 8] построены совершенные коды любой длины $n > 15$, имеющие тривиальную группу автоморфизмов. В [5, 10] (см. также тезисы [1]) доказано, что порядок группы автоморфизмов любого совершенного кода длины n не превышает порядка группы автоморфизмов кода Хемминга H^n . Этот результат дает ответ на вопрос, поставленный несколько лет назад Ю. Л. Васильевым. В [10] отмечается также, что вопрос существования таких нелинейных совершенных кодов C длины $n \geq 15$, что $|\text{Aut}(C)| = |\text{Aut}(H^n)|$, остается открытым.

В настоящей статье доказывается, что порядок группы автоморфизмов любого нелинейного совершенного кода C по крайней мере в два раза

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 99-01-00531) и Федеральной целевой программы «Интеграция» (проект АО-110).

меньше порядка группы автоморфизмов кода Хемминга той же длины.*)

1. Перечисление орбит пространства $\{0, 1\}^n$, порождаемых группой $\text{Sym}(H^n)$

Для решения поставленной задачи необходимо провести предварительную подготовку. Нам понадобится знать длины всех орбит пространства $\{0, 1\}^n$ веса не больше шести относительно группы перестановочных автоморфизмов кода Хемминга H^n (весом орбиты называем вес составляющих ее векторов). Метод орбит применялся автором в [3] при решении задачи перечисления совершенных кодов длины 15. Используемая там техника применима для любых n , если вес орбит не очень большой. Следует также отметить, что орбиты булевых функций относительно различных групп преобразований изучались рядом авторов [2].

Носителем вектора $\mathbf{u} \in \{0, 1\}^n$ называем множество $[\mathbf{u}]$ всех номеров $i \in \{1, \dots, n\}$ таких, что координата u_i равна 1. В дальнейшем нам потребуется следующее представление кода Хемминга H^n длины $n = 2^k - 1$. Каждому $i = 0, \dots, n$ ставится в соответствие вектор $(i_1, \dots, i_k) \in \{0, 1\}^k$, представляющий число i в двоичной системе счисления. Считаем, что код Хемминга H^n состоит из всех векторов $\mathbf{u} \in \{0, 1\}^n$ таких, что $\bigoplus \{i \mid i \in [\mathbf{u}]\} = 0$. Орбиты пространства $\{0, 1\}^n$ можно задавать с помощью уравнений (см. [3], лемма 1). Каждой орбите веса m ставится в соответствие матрица (b_{pq}) размера $(m - r) \times r$ над полем $GF(2)$ с попарно различными строками ($p = r + 1, \dots, m$; $q = 1, \dots, r$). Тогда носителями векторов из данной орбиты являются всевозможные множества $\{i_1, \dots, i_m\}$ такие, что $i_p = b_{p1}i_1 \oplus \dots \oplus b_{pr}i_r$ ($p = r + 1, \dots, m$), а i_1, \dots, i_r пробегает все линейно независимые наборы из $\{0, 1\}^k$. Аналогичное представление орбит булевых функций рассматривалось в [4].

Далее мы будем рассматривать ненулевые векторы из $\{0, 1\}^k$ как точки конечной проективной геометрии $PG(k - 1, 2)$. Необходимые сведения о конечных геометриях имеются, например, в [6].

Орбиты веса 3. Тройки бывают двух типов: кодовые и некодвые. Известно, что имеется $n(n - 1)/6$ кодовых троек (составляющих систему троек Штейнера) и все они переводятся друг в друга автоморфизмами кода H^n . На геометрическом языке кодовые тройки интерпретируются как прямые в проективной геометрии $PG(k - 1, 2)$. Орбиту этих троек обозначим через O_3^1 .

*) В сентябре 2000 г. автору стало известно, что Ф. И. Соловьева и С. Т. Топалова другим способом установили следующий факт: порядок группы автоморфизмов кода Хемминга строго больше порядка группы автоморфизмов любого другого совершенного кода той же длины.

Для некодовой тройки $[\mathbf{u}] = \{i_1, i_2, i_3\}$ ($\mathbf{u} \in E^n$) векторы i_1, i_2, i_3 линейно независимы в E^k . Следовательно, все такие тройки переводятся друг в друга автоморфизмами и составляют одну орбиту O_3^2 . Число независимых троек из E^k равно $n(n-1)(n-3)/6$.

Орбиты веса 4. Начнем с кодовой четверки $[\mathbf{u}] = \{i_1, i_2, i_3, i_4\}$, $\mathbf{u} \in H^n$. Из определения кода Хемминга следует, что должно выполняться равенство $i_4 = i_1 \oplus i_2 \oplus i_3$. Следовательно, тройка $\{i_1, i_2, i_3\}$ независима и по лемме 1 из [3] множество векторов O_4^1 , носители которых являются кодовыми четверками, образует одну орбиту. Так как такая четверка однозначно определяется по любой содержащейся в ней независимой тройке, то $|O_4^1| = n(n-1)(n-3)/24$.

Некодовые четверки могут быть двух типов. Во-первых, это множество независимых четверок. По определению $\mathbf{u} \in O_4^2$, если $[\mathbf{u}] = \{i_1, i_2, i_3, i_4\}$ для некоторой независимой четверки векторов i_1, i_2, i_3, i_4 . Длина орбиты O_4^2 равна $n(n-1)(n-3)(n-7)/24$.

Во-вторых, есть еще четверки, содержащие кодовые тройки. Множество O_4^3 можно задать следующим образом: $\mathbf{u} \in O_4^3$ тогда и только тогда, когда для некоторой независимой тройки $\{i_1, i_2, i_3\}$ выполняется равенство $[\mathbf{u}] = \{i_1, i_2, i_3, i_4\}$, где $i_4 = i_2 \oplus i_3$. На геометрическом языке каждая такая четверка есть объединение прямой и не лежащей на ней точки. По лемме 1 из [3] они образуют орбиту длины $n(n-1)(n-3)/6$. Так как $|O_4^1| + |O_4^2| + |O_4^3| = \binom{n}{4}$, то множество векторов веса 4 исчерпано.

Орбиты веса 5. Начнем с орбиты O_5^1 , представляющей кодовые пятерки. Если $\mathbf{u} \in O_5^1$, то $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5\}$, где $i_5 = i_1 \oplus i_2 \oplus i_3 \oplus i_4$. Любая четверка векторов, выбранная из пятерки $\{i_1, i_2, i_3, i_4, i_5\}$, является линейно независимой. По лемме 1 из [3] множество O_5^1 составляет одну орбиту. Ее длина равна $n(n-1)(n-3)(n-7)/120$.

Среди орбит некодовых векторов есть орбита O_5^2 , элементы которой представляются объединением кодовой четверки и точки, не лежащей в двумерной плоскости (плоскости Фано), проходящей через эту четверку. Такую орбиту можно задать одним уравнением. Если $\mathbf{u} \in O_5^2$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5\}$, то можно считать, что векторы $\{i_1, i_2, i_3, i_4\}$ линейно независимы, а $i_5 = i_1 \oplus i_2 \oplus i_3$. Для подсчета длины этой орбиты число кодовых четверок нужно умножить на число точек из $\{0, 1\}^n$, не лежащих в данной плоскости Фано. Следовательно, $|O_5^2| = n(n-1)(n-3)(n-7)/24$.

Следующая орбита — O_5^3 . Ее элементы представляются объединениями двух пересекающихся прямых (или кодовых троек). Она также задается с помощью уравнений. Если $\mathbf{u} \in O_5^3$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5\}$, то $i_4 = i_1 \oplus i_2$ и $i_5 = i_1 \oplus i_2 \oplus i_3$. Число пар пересекающихся кодовых троек равно $n(n-1)(n-3)/8$.

Орбиту O_5^4 можно задать следующим уравнением. Вектор \mathbf{u} принадлежит орбите O_5^4 тогда и только тогда, когда $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5\}$, где набор $\{i_1, i_2, i_3, i_4\}$ линейно независим, а $i_5 = i_1 \oplus i_2$. Следовательно, каждая такая пятерка содержит ровно одну кодовую тройку. Теперь легко найти длину орбиты. Для построения любой пятерки надо взять произвольную из $n(n-1)/6$ кодовых троек, добавить к ней один из $n-3$ не принадлежащих ей элементов, а затем добавить еще один такой элемент, чтобы не получилась пятерка из орбиты O_5^3 , т. е. чтобы этот последний элемент i_4 не совпал ни с одним элементом вида $i_1 \oplus i_3, i_2 \oplus i_3, i_5 \oplus i_3$. Таким образом, для выбора последнего элемента остается $n-7$ вариантов. Это означает, что $|O_5^4| = n(n-1)(n-3)(n-7)/6 \cdot 2$ (делим на 2, так как два последних элемента можно поменять ролями).

Начиная с $n = 31$ появляется еще одна орбита O_5^5 , состоящая из векторов $\mathbf{u} \in \{0, 1\}^n$, носители которых $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5\}$ представляют собой линейно независимые наборы. Длина такой орбиты, очевидно, равна $n(n-1)(n-3)(n-7)(n-15)/5!$.

Так как $|O_5^1| + |O_5^2| + |O_5^3| + |O_5^4| + |O_5^5| = \binom{n}{5}$, то найдены все орбиты веса 5.

Орбиты веса 6. Элементы кодовой орбиты O_6^1 представляются объединениями непересекающихся пар кодовых троек. Если $\mathbf{u} \in O_6^1$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$, то можно считать, что $i_5 = i_1 \oplus i_2$ и $i_6 = i_3 \oplus i_4$, где набор векторов $\{i_1, i_2, i_3, i_4\}$ является линейно независимым. Число неупорядоченных пар непересекающихся прямых равно $n(n-1)(n-3)(n-7)/72$.

Элементы следующей орбиты O_6^2 представляются объединениями трех некомпланарных прямых с выкинутой их общей точкой пересечения. Эту орбиту можно задать двумя уравнениями. Пусть $\mathbf{u} \in O_6^2$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$. Тогда $i_5 = i_1 \oplus i_2 \oplus i_3$ и $i_6 = i_2 \oplus i_3 \oplus i_4$. Точку пересечения можно выбрать n способами. Далее следует выбрать тройку прямых, проходящих через эту точку. Рассмотрим любую $(k-2)$ -мерную гиперплоскость, не содержащую выбранную точку. Любая тройка некомпланарных прямых, проходящих через выбранную точку, пересекает эту гиперплоскость по независимой тройке точек. По предыдущему число независимых троек в $(k-2)$ -мерной гиперплоскости равно $m(m-1)(m-3)/2$, где $m = (n-1)/2$. Поэтому длина орбиты O_6^2 равна $n(n-1)(n-3)(n-7)/48$.

Носители элементов орбиты O_6^3 можно охарактеризовать как плоскости Фано без одной точки, т. е. $\mathbf{u} \in O_6^3$ тогда и только тогда, когда $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$, где тройка векторов i_1, i_2, i_3 линейно независима и $i_4 = i_1 \oplus i_2, i_5 = i_1 \oplus i_3, i_6 = i_2 \oplus i_3$. Как легко видеть, $|O_6^3| = n(n-1)(n-3)/24$.

Элементы орбиты O_6^4 можно задать как объединение прямой и таких трех точек, не лежащих на этой прямой, что никакая плоскость, проходящая через любую пару этих точек, не содержит данную прямую. В уравнениях эта комбинация выглядит так. Пусть $\mathbf{u} \in O_6^4$ и $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$. Тогда можно считать, что $i_5 = i_1 \oplus i_2 \oplus i_3$ и $i_6 = i_1 \oplus i_2 \oplus i_3 \oplus i_4$, где четверка i_1, i_2, i_3, i_4 линейно независима. Осталось определить длину орбиты. Для построения элемента такой орбиты нужно взять любую из $n(n-1)/6$ прямых, добавить любую из $n-3$ точек, не лежащих на выбранной прямой, затем добавить такую из $n-7$ точек, которая не лежит в плоскости, проходящей через прямую и ранее выбранную точку, и, наконец, добавить одну из $n-12$ точек, которая не лежит в плоскостях, проходящих через прямую и уже выбранные точки, и не лежит на прямой, проходящей через ранее выбранные две точки. В результате получаем $|O_6^4| = |O_3^1|(n-3)(n-7)(n-12)/6 = n(n-1)(n-3)(n-7)(n-12)/36$.

Носители элементов орбиты O_6^5 можно задать как объединение двух пересекающихся прямых и точки, не лежащей в плоскости этих прямых. Для задания элемента $\mathbf{u} \in O_6^5$, $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$ с помощью уравнений нужно взять независимую четверку i_1, i_2, i_3, i_4 и положить $i_5 = i_1 \oplus i_2$, $i_6 = i_1 \oplus i_3$. В плоскости Фано, состоящей из 7 точек, имеется 21 пара пересекающихся прямых. Кроме этого, в проективном пространстве $PG(k-1, 2)$ имеется $n(n-1)(n-3)/168$ двумерных плоскостей (см. [6], формула (12.2.2)). Поэтому $|O_6^5| = n(n-1)(n-3)(n-7)/8$.

Начиная с $n = 31$ появляется еще несколько новых орбит. Орбита O_6^6 состоит из векторов $\mathbf{u} \in \{0, 1\}^k$ с носителями $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$, где $i_5 = i_1 \oplus i_2 \oplus i_3 \oplus i_4$, а пятерка векторов i_1, i_2, i_3, i_4, i_6 линейно независима. Поэтому к пятерке, соответствующей вектору из орбиты O_5^1 , добавляется еще один независимый элемент i_6 . Пятерка, соответствующая вектору из орбиты O_5^1 , лежит в некотором трехмерном подпространстве. Число трехмерных подпространств в $PG(k-1, 2)$, по той же формуле (12.2.2) из [6], равно $n(n-1)(n-3)(n-7)/20160$. Поэтому $|O_6^6| = |O_5^1|n(n-1)(n-3)(n-7)(n-15)/20160 = n(n-1)(n-3)(n-7)(n-15)/120$.

Орбита O_6^7 состоит из всех векторов с носителями $[\mathbf{u}] = \{i_1, i_2, i_3, i_4, i_5, i_6\}$, где $i_5 = i_1 \oplus i_2 \oplus i_3$, а пятерка i_1, i_2, i_3, i_4, i_6 линейно независима. Другими словами, к пятерке, соответствующей вектору из орбиты O_5^2 , добавляется еще один независимый элемент i_6 . Этот элемент не лежит в трехмерном пространстве, содержащем пятерку. Поэтому он может быть выбран $n-15$ способами. Следовательно, $|O_6^7| = |O_5^2|n(n-1)(n-3)(n-7)(n-15)/20160 \cdot 2 = n(n-1)(n-3)(n-7)(n-15)/48$. Делим на 2, так как элементы i_4 и i_6 можно менять ролями.

Еще одна кодовая орбита O_6^8 задается уравнением $i_6 = i_1 \oplus i_2 \oplus i_3 \oplus$

$i_4 \oplus i_5$, где пятерка i_1, i_2, i_3, i_4, i_5 линейно независима. Очевидно, что $|O_6^8| = n(n-1)(n-3)(n-7)(n-15)/5! \cdot 6$.

Последняя девятая орбита веса 6 появляется начиная с $n = 63$. Носителями векторов этой орбиты являются независимые шестерки $i_1, i_2, i_3, i_4, i_5, i_6$. Ее длина равна $n(n-1)(n-3)(n-7)(n-15)(n-31)/720$.

Так как $\sum_{m=1}^9 |O_6^m| = \binom{15}{6}$, то все орбиты веса 6 перечислены.

Подводя итог, выпишем все найденные орбиты и их длины в следующей таблице:

O_m^i	Длина
O_3^1	$n(n-1)/6$
O_3^2	$n(n-1)(n-3)/6$
O_4^1	$n(n-1)(n-3)/24$
O_4^2	$n(n-1)(n-3)(n-7)/24$
O_4^3	$n(n-1)(n-3)/6$
O_5^1	$n(n-1)(n-3)(n-7)/120$
O_5^2	$n(n-1)(n-3)(n-7)/24$
O_5^3	$n(n-1)(n-3)/8$
O_5^4	$n(n-1)(n-3)(n-7)/12$
O_5^5	$n(n-1)(n-3)(n-7)(n-15)/120$
O_6^1	$n(n-1)(n-3)(n-7)/72$
O_6^2	$n(n-1)(n-3)(n-7)/48$
O_6^3	$n(n-1)(n-3)/24$
O_6^4	$n(n-1)(n-3)(n-7)(n-12)/36$
O_6^5	$n(n-1)(n-3)(n-7)/8$
O_6^6	$n(n-1)(n-3)(n-7)(n-15)/120$
O_6^7	$n(n-1)(n-3)(n-7)(n-15)/48$
O_6^8	$n(n-1)(n-3)(n-7)(n-15)/720$
O_6^9	$n(n-1)(n-3)(n-7)(n-15)(n-31)/720$

2. Основной результат

Группа автоморфизмов кода Хемминга H^n является полупрямым произведением двух своих подгрупп: группы перестановочных автоморфизмов и ядра. Следовательно, $|\text{Aut}(H^n)| = |\text{Sym}(H^n)||H^n| = n(n-1)(n-3) \dots (n-2^{k-1}+1)2^{n-k}$, где $k = \log_2(n+1)$. Пользуясь результатами первого раздела, докажем, что код Хемминга длины n является

единственным (с точностью до эквивалентности) совершенным кодом, порядок группы автоморфизмов которого равен $|\text{Aut}(H^n)|$.

Системой троек Штейнера $\text{STS}(n)$ на множестве $\{1, \dots, n\}$ называется такое семейство его трехэлементных подмножеств, что любая пара элементов из $\{1, \dots, n\}$ содержится в единственном множестве из семейства $\text{STS}(n)$. *Группой автоморфизмов* $\text{Aut}(\text{STS}(n))$ системы троек Штейнера $\text{STS}(n)$ называется множество всех перестановок, которые переводят семейство $\text{STS}(n)$ в себя. Две системы троек Штейнера называются *эквивалентными*, если существует перестановка, переводящая одну систему в другую. Примером системы троек Штейнера является семейство носителей всех векторов веса 3 совершенного кода C , которое в дальнейшем будем обозначать через $\text{STS}(C)$.

Ключевым при доказательстве основного результата является следующее утверждение.

Лемма 1. Пусть для совершенного кода C длины n имеют место равенства $\text{STS}(C) = \text{STS}(H^n)$ и $\text{Sym}(C) = \text{Sym}(H^n)$. Тогда множества векторов веса не больше шести, содержащиеся в кодах C и H^n , одинаковы.

ДОКАЗАТЕЛЬСТВО. Обозначим через $A_{m,n}$ число векторов веса m в коде Хемминга H^n . По теореме Шапиро–Злотника число векторов веса m в любом другом совершенном коде длины n тоже равно $A_{m,n}$. Так как $\text{Sym}(C) = \text{Sym}(H^n)$, то множество векторов веса m в коде C состоит из орбит O_m^i , которые перечислены в таблице.

Пусть $m = 4$. Так как $|O_4^1| < |O_4^3|$, $|O_4^1| < |O_4^2|$ и $A_{4,n} = |O_4^1|$, то множества векторов веса 4, содержащиеся в кодах C и H^n , одинаковы.

Пусть $m = 5$. В этом случае $A_{5,n} = |O_5^1|$. Из таблицы следует, что $A_{5,n} < |O_5^2|$ и $A_{5,n} < |O_5^4|$. При $n > 15$ выполняется также неравенство $A_{5,n} < |O_5^5|$. Поэтому орбиты O_5^2 , O_5^4 и O_5^5 не могут пересекаться с кодом C . Для оставшейся орбиты O_5^3 равенство $A_{5,n} = |O_5^3|$ не выполняется ни при каких $n = 2^k - 1$. Поэтому множества векторов веса 5, содержащиеся в кодах C и H^n , одинаковы.

Пусть $m = 6$. В этом случае $A_{6,n} = |O_6^1| + |O_6^8| = n(n-1)(n-3)(n-5)(n-7)/720$. Очевидно, что $A_{6,n} < |O_6^4|$. Кроме этого, при $n > 15$ выполняются неравенства $A_{6,n} < |O_6^6|$ и $A_{6,n} < |O_6^7|$, а при $n > 31$ также имеем $A_{6,n} < |O_6^9|$. Поэтому орбиты O_6^4 , O_6^6 , O_6^7 и O_6^9 не содержат векторов кода C . При $n > 63$ имеет место неравенство $|O_6^2| + |O_6^3| + |O_6^5| < |O_6^8|$. Отсюда непосредственно следует, что при $n > 63$ орбита O_6^8 должна содержаться в коде C . Так как $|O_6^1| < |O_6^2|$, $|O_6^1| < |O_6^5|$ и $|O_6^1| > |O_6^3|$, то орбиты O_6^2 , O_6^3 и O_6^5 не могут содержать векторов из кода C . Для $n = 15$, $n = 31$ и $n = 63$ в справедливости леммы можно легко убедиться непосредственным перебором всех вариантов распределения орбит с суммой длин $A_{6,n}$. Лемма доказана.

Прежде чем переходить к доказательству основного результата — теоремы 2, установим его аналог для систем троек Штейнера.

Теорема 1. Пусть для системы троек Штейнера $\text{STS}(n)$ ($n = 2^k - 1$, $k \geq 4$) верно неравенство $|\text{Aut}(\text{STS}(n))| > |\text{Aut}(\text{STS}(H^n))|/(n-7)$. Тогда системы $\text{STS}(n)$ и $\text{STS}(H^n)$ эквивалентны.

Доказательство. На множестве $Q = \{0, 1, \dots, n\}$ определим бинарную операцию \oplus следующим образом: $0 \oplus i = i \oplus 0 = i$, $i \oplus i = 0$ ($i \in Q$) и для всех $i_1 \neq 0$, $i_2 \neq 0$, $i_1 \neq i_2$ полагаем $i_3 = i_1 \oplus i_2$ тогда и только тогда, когда тройка $\{i_1, i_2, i_3\}$ принадлежит $\text{STS}(n)$. Легко проверяется, что относительно такой операции Q становится абелевой квазигруппой (т. е. кроме свойств, указанных выше, имеют место тождества $i \oplus j = j \oplus i$ и уравнения $i \oplus x = j$ однозначно разрешимы при любых $i, j \in Q$). Пусть G — группа автоморфизмов квазигруппы Q (т. е. группа всех взаимно однозначных отображений $\pi: Q \rightarrow Q$ таких, что $\pi(x \oplus y) = \pi(x) \oplus \pi(y)$ для всех $x, y \in Q$). Очевидно, что $|G| = |\text{Aut}(\text{STS}(n))|$. Рассмотрим в множестве $\{1, \dots, n\}$ любую тройку i_1, i_2, i_3 , не лежащую в $\text{STS}(n)$. Полагаем $Q_1 = \{0, i_1\}$ и $Q_2 = \{0, i_1, i_2, i_1 \oplus i_2\}$. Пусть Q_3 — наименьшая подквазигруппа в Q , содержащая тройку i_1, i_2, i_3 . Тогда $|Q_3| = 8$. Докажем этот факт от противного, т. е. предположим, что $|Q_3| > 8$. Так как множество $Q_3 \setminus \{0\}$ определяет подсистему в системе $\text{STS}(n)$, то $|Q_3| \geq 16$. Для некоторого фиксированного элемента $i_4 \in Q \setminus Q_3$ рассмотрим наименьшую подквазигруппу Q_4 , содержащую множество $\{i_1, i_2, i_3, i_4\}$. Продолжая индуктивно этот процесс, построим множество $\{i_1, \dots, i_m\}$ и цепочку вложенных подквазигрупп $Q_1 \subset Q_2 \subset \dots \subset Q_m = Q$ таких, что $i_p \in Q_p \setminus Q_{p-1}$ ($p = 2, \dots, m$). Очевидно, что любой автоморфизм $\pi \in G$ однозначно определяется по своим значениям на множестве $\{i_1, \dots, i_m\}$. При этом $\pi(i_1)$ может принимать не более n ненулевых значений; при фиксированном $\pi(i_1)$ величина $\pi(i_2)$ принимает не более $n-1$ значений из множества $Q \setminus \pi(Q_1)$; при фиксированных $\pi(i_1)$ и $\pi(i_2)$ величина $\pi(i_3)$ принимает не более $n-3$ значений из множества $Q \setminus \pi(Q_2)$ и т. д. Отсюда следует оценка $|G| \leq n(n-1)(n-3)(n-5)\dots(n-2^{k-1}-1)$ ($k = \log_2(n+1)$). А это противоречит тому, что $|G| = |\text{Aut}(\text{STS}(n))| > |\text{Aut}(\text{STS}(H^n))|/(n-7)$.

Чтобы убедиться в том, что система $\text{STS}(n)$ эквивалентна системе $\text{STS}(H^n)$, следует проверить закон ассоциативности $(i_1 \oplus i_2) \oplus i_3 = i_1 \oplus (i_2 \oplus i_3)$ (в этом случае квазигруппа Q будет абелевой группой). Но, как легко заметить, свойство ассоциативности эквивалентно тому, что любые три элемента $i_1, i_2, i_3 \in \{1, \dots, n\}$ содержатся в некоторой восьмизначной подквазигруппе $Q_1 \subset Q$. Так как порядок всех элементов из Q равен двум, то Q является векторным пространством над полем $GF(2)$. Поэтому Q изоморфно пространству $\{0, 1\}^k$. Теорема доказана.

Неравенство $|\text{Aut}(\text{STS}(n))| \leq |\text{Aut}(\text{STS}(H^n))|$ для любой системы троек Штейнера $\text{STS}(n)$ доказано в [5, 10] (см. также [11]).

Теорема 2. Для любого нелинейного совершенного кода C длины n справедливо неравенство $|\text{Aut}(C)| \leq |\text{Aut}(H^n)|/2$.

Доказательство. Докажем, что если для совершенного кода C длины n справедливо неравенство $|\text{Aut}(C)| > |\text{Aut}(H^n)|/2$, то C эквивалентен коду H^n . Так как порядок групп автоморфизмов у эквивалентных кодов один и тот же, то после переноса кода на подходящий вектор можно считать, что код C , удовлетворяющий приведенному выше неравенству, содержит $\mathbf{0}$. Из предложений 3 и 4 из [10] следует неравенство $|\text{Sym}(C)| \geq |\text{Aut}(C)|/2^{n-\log_2(n+1)} > |\text{Sym}(H^n)|/2$. Так как $\text{Sym}(C)$ является подгруппой группы $\text{Aut}(\text{STS}(C))$, то при $n \geq 15$ получаем $|\text{Aut}(\text{STS}(C))| > |\text{Sym}(H^n)|/2 > |\text{Aut}(\text{STS}(H^n))|/(n-7)$. Из теоремы 1 следует, что система троек Штейнера $\text{STS}(C)$ эквивалентна системе троек Штейнера $\text{STS}(H^n)$. В частности, $|\text{Aut}(\text{STS}(C))| = |\text{Sym}(H^n)|$. Кроме того, порядок группы $\text{Aut}(\text{STS}(C))$ должен делиться на порядок подгруппы $\text{Sym}(C)$. Поэтому из предыдущего неравенства следует, что $\text{Sym}(C) = \text{Aut}(\text{STS}(C))$. Сделав подходящую перестановку координат кода C , будем считать, что $\text{STS}(C) = \text{STS}(H^n)$. Следовательно, $\text{Sym}(C) = \text{Sym}(H^n)$. По лемме 1 у кодов C и H^n совпадают множества векторов веса не больше шести. Фиксируем в C любой вектор \mathbf{u}_1 веса 3. Тогда $\text{STS}(C \oplus \mathbf{u}_1) = \text{STS}(H^n)$. Для кода $C \oplus \mathbf{u}_1$ справедлива та же оценка $|\text{Aut}(C \oplus \mathbf{u}_1)| > |\text{Aut}(H^n)|/2$. Поэтому $|\text{Sym}(C \oplus \mathbf{u}_1)| > |\text{Sym}(H^n)|/2$ и т. д. Повторяя этот процесс, для любой конечной последовательности векторов $\mathbf{u}_1, \dots, \mathbf{u}_m$ веса три из кода C получаем код $C' = C \oplus \mathbf{u}_1 \oplus \dots \oplus \mathbf{u}_m$ такой, что множества векторов веса не больше шести, содержащиеся в кодах C' и H^n , одинаковы. В частности, для некоторого $\mathbf{v} \in C$ будем иметь $\mathbf{v} \oplus \mathbf{u}_1 \oplus \dots \oplus \mathbf{u}_m = \mathbf{0}$. Следовательно, $\mathbf{u}_1 \oplus \dots \oplus \mathbf{u}_m \in C$ для любых векторов $\mathbf{u}_1, \dots, \mathbf{u}_m$ веса 3 из C . Так как такие векторы принадлежат также коду H^n , то можно взять базис кода Хемминга H^n из векторов веса 3 и в качестве $\mathbf{u}_1, \dots, \mathbf{u}_m$ рассматривать всевозможные подсемейства этого базиса. Следовательно, $H^n \subseteq C$, что влечет $H^n = C$. Теорема доказана.

Для любого кода C длины n можно построить расширенный код \tilde{C} длины $n+1 = 2^k$, добавляя к векторам кода C проверку на четность.

Из теоремы 2 непосредственно получаем

Следствие. Для любого расширенного нелинейного совершенного кода \tilde{C} длины $n+1$ справедливо неравенство $|\text{Aut}(\tilde{C})| \leq |\text{Aut}(\tilde{H}^n)|/2$.

Автор выражает благодарность А. А. Евдокимову, обратившему внимание автора на обзор [2] и использование метода орбит в исследовании свойств кодов, а также А. Д. Коршунову за замечания по оформлению работы.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И.** Новые конструкции и свойства совершенных кодов // Междунар. конф. «Дискретный анализ и исследование операций»: Материалы конф. (Новосибирск, 26 июня — 1 июля 2000). Новосибирск: Изд-во Ин-та математики, 2000. С. 5–10.
2. **Кузнецов Ю. В., Шкарин С. А.** Коды Рида-Маллера // Математические вопросы кибернетики. М.: 1996. Вып. 6. С. 5–50.
3. **Малюгин С. А.** О перечислении совершенных двоичных кодов длины 15 // Дискрет. анализ и исслед. операций. Сер. 2. 1999. Т. 6, № 2. С. 48–73.
4. **Нечипорук Э. И.** О синтезе схем с помощью линейных преобразований // Докл. АН СССР. 1958. Т. 123, № 4. С. 610–612.
5. **Соловьева Ф. И., Топалова С. Т.** О группах автоморфизмов совершенных двоичных кодов и систем Штейнера // Проблемы передачи информации. (Принято к печати.)
6. **Холл М.** Комбинаторика. М.: Мир, 1970.
7. **Avguistinovich S. V., Solov'eva F. I.** Perfect binary codes with trivial automorphism group // Proc. of IEEE Intern. Workshop on Inform. Theory. Killarney, Ireland, 1998 (June). P. 114–115.
8. **Malyugin S. A.** Perfect codes with trivial automorphism group // Proc. Second Intern. Workshop on Optimal Codes and Related Topics. Sozopol, Bulgaria, 1998 (June). P. 163–167.
9. **Phelps K. T.** Every finite group is the automorphism group of some perfect code // J. Combin. Theory. Ser. A. 1986. V. 43, N 1. P. 45–51.
10. **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.
11. **Solov'eva F. I., Topalova S. T.** On the automorphism groups of Steiner systems // Междунар. конф. «Дискретный анализ и исследование операций»: Материалы конф. (Новосибирск, 26 июня — 1 июля 2000). Новосибирск: Изд-во Ин-та математики, 2000. С. 90.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск,
Россия

Статья поступила

31 июля 2000 г.