

УДК 519.725

НИЖНИЕ ОЦЕНКИ ЧИСЛА m -КВАЗИГРУПП ПОРЯДКА 4 И ЧИСЛА СОВЕРШЕННЫХ ДВОИЧНЫХ КОДОВ*)

Д. С. Кротов

Описана конструкция m -квазигрупп порядка 4, позволяющая получить нижнюю оценку их числа. При помощи этих m -квазигрупп с использованием конструкции К. Фелпса [5] получена нижняя оценка $2^{2^{\frac{n+1}{2}-\log_2(n+1)}} 3^{2^{\frac{n-3}{4}}} 2^{2^{\frac{n+5}{4}-\log_2(n+1)}}$ числа различных совершенных двоичных кодов.

Введение

Совершенным двоичным кодом длины n с расстоянием 3 называется такое подмножество C множества $\{0, 1\}^n$, т. е. множества двоичных слов длины n , что для любого слова v из $\{0, 1\}^n$ имеется только одно слово из C , отличающееся от v не более чем в одной координате. Известно, что такие коды существуют только при $n = 2^t - 1$, где t — произвольное натуральное число.

Пусть $B(n)$ обозначает множество всех совершенных двоичных кодов длины n . Ю. Л. Васильевым в [2] был предложен метод построения двоичных совершенных кодов, из которого следует оценка

$$|B(n)| \geq 2^{2^{\frac{n+1}{2}-\log_2(n+1)}} 2^{2^{\frac{n+5}{4}-\log_2(n+1)}}. \quad (1)$$

В дальнейшем эта оценка улучшалась в [1, 3]. В настоящее время известно много методов построения совершенных двоичных кодов (см., например, [4, 6]), но большинство из них позволяет незначительно улучшить оценку (1).

Метод построения совершенных кодов, предложенный недавно С. А. Малюгиным в [3], заключается в следующем. В качестве i -компоненты берётся такое подмножество совершенного кода, которое можно

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 00-01-00822).

заменить в коде на его сдвиг по i -й координате (полученный инверсией этой координаты) и получить совершенный код. По определению (i, j, k) -компонента является i -, j - и k -компонентой одновременно. Код Хемминга длины n рассматривается как объединение (i, j, k) -компонент. Каждая (i, j, k) -компонента не меняется или заменяется на одну из $2^{(n-3)/4} - 1$ изоморфных ей (i, j, k) -компонент, полученных сдвигом по k -й координате половины вершин из данной (i, j, k) -компоненты. В полученном коде произвольным образом сдвигаются непересекающиеся i - и j -компоненты. Класс кодов, полученный при помощи таких преобразований, позволяет установить оценку

$$|B(n)| \geq 2^{2^{\frac{n+1}{2} - \log_2(n+1)}} 2^{2^{\frac{n-3}{4}}}. \quad (2)$$

Если к каждому слову произвольного кода из $B(n)$ добавить $(n+1)$ -й символ, равный сумме всех предыдущих по модулю 2, либо отрицанию этой суммы, получится двоичный код длины $n+1$ с расстоянием 4. Такие коды будем называть *расширенными совершенными кодами*. Множество расширенных совершенных кодов длины $n+1$ обозначим через $B'(n+1)$. Поскольку $|B'(n+1)| = 2|B(n)|$, задача оценки числа кодов из $B(n)$ эквивалентна задаче оценки числа кодов из $B'(n+1)$.

В настоящей статье используется представление расширенного совершенного кода длины $n+1$ в виде объединения подмножеств (соответствующих (i, j, k) -компонентам совершенного кода с расстоянием 3), каждое из которых задаётся произвольной m -квазигруппой порядка 4, где $m = (n-3)/4$ (в более общем виде представление таких кодов описано К. Фелсом в [5]). Вместо преобразований (i, j, k) -компонент рассматриваются соответствующие преобразования m -квазигрупп: сдвигу независимых i -компонент соответствует выбор функции λ , а замене (i, j, k) -компоненты на изоморфную ей — выбор перестановок элементов носителя m -квазигруппы. В этой терминологии описывается модификация метода Малюгина, которая позволяет уточнить оценку (2): двойка в основании второго множителя заменена на тройку и добавлен третий множитель $2^{2^{\frac{n+5}{4} - \log_2(n+1)}}$. Промежуточным результатом является получение нижней оценки числа m -квазигрупп порядка 4.

В § 1 приведена конструкция Фелпса построения расширенных совершенных кодов и сформулированы теоремы 1 и 2 о нижней оценке числа m -квазигрупп и о нижней оценке числа расширенных совершенных кодов.

В § 2 описывается метод построения m -квазигрупп порядка 4, позволяющий установить нижнюю оценку их числа.

§ 1. О числе совершенных кодов

Пусть m — произвольное натуральное число, A — конечное множество мощности p и $q : A^m \rightarrow A$ — m -арная операция. Если на любых наборах $c, c' \in A^m$, различающихся ровно в одной координате, $q(c) \neq q(c')$, то пара (A, q) называется m -квазигруппой (порядка p) с носителем A .

Пусть $C_0^0, C_1^0, \dots, C_p^0$ — расширенные совершенные коды, на которые разбивается множество чётных (с чётным числом единиц) слов из $\{0, 1\}^{p+1}$, а $C_0^1, C_1^1, \dots, C_p^1$ — расширенные совершенные коды, на которые разбивается множество нечётных слов из $\{0, 1\}^{p+1}$.

Пусть R — расширенный совершенный код длины $m + 1$ и для каждого $r \in R$ задана m -квазигруппа $(\{0, 1, \dots, p\}, q_r)$.

Лемма 1 ([5]). Множество

$$\bigcup_{r=(r_0, r_1, \dots, r_m) \in R} \left(\bigcup_{j_0=q_r(j_1, \dots, j_m)} \{x = (x_0, x_1, \dots, x_m) \mid x_i \in C_{j_i}^{r_i}\} \right) \quad (3)$$

является расширенным совершенным кодом длины $(p + 1)(m + 1)$.

Обозначим через $Q(m, p + 1)$ множество всех m -квазигрупп порядка $p + 1$ с носителем $\{0, 1, \dots, p\}$. Поскольку в (3) можно выбрать произвольный код R из $B'(m + 1)$ и для каждого r из R можно выбрать произвольную m -квазигруппу из $Q(m, p + 1)$, то справедливо следующее утверждение.

Следствие 1. Если $p = 2^s - 1$ и $m = 2^t - 1$, где s и t — произвольные натуральные числа, то

$$\begin{aligned} |B'((p + 1)(m + 1))| &\geq |B'(m + 1)| \cdot |Q(m, p + 1)|^{|R|} \\ &= |B'(m + 1)| \cdot |Q(m, p + 1)|^{2^{m - \log_2(m + 1)}}. \end{aligned}$$

В следующем параграфе будет доказана

Теорема 1. При любом натуральном m

$$|Q(m, 4)| \geq 3^{m+1} 2^{2^m+1} - 2^{m+3} 3^m.$$

Взяв $p = 3$ и $m = (n - 3)/4$, из следствия 1 и теоремы 1 получаем следующую теорему.

Теорема 2. Пусть t — любое натуральное число и $n = 2^t - 1$. Тогда

$$|B'(n + 1)| \geq \left| B'\left(\frac{n + 1}{4}\right) \right| \cdot 2^{2^{\frac{n+1}{2} - \log_2(n+1)}} 3^{2^{\frac{n-3}{4}} 2^{2^{\frac{n+5}{4} - \log_2(n+1)}} (1 - o(1)).$$

§ 2. Построение m -квазигрупп порядка 4

Пусть $A = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$ — множество двоичных столбцов высоты 2 и \oplus — сложение по модулю два. Для столбца $\begin{bmatrix} a \\ b \end{bmatrix}$ из A элементы a и b будем называть соответственно верхним и нижним битом.

Пусть $\lambda = \lambda(x_1, \dots, x_m)$ — булева функция от m переменных и операция $q_\lambda : A^m \rightarrow A$ задаётся равенством

$$q_\lambda \left(\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}, \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}, \dots, \begin{bmatrix} a_m \\ b_m \end{bmatrix} \right) = \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \oplus \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \oplus \dots \oplus \begin{bmatrix} a_m \\ b_m \end{bmatrix} \oplus \begin{bmatrix} 0 \\ \lambda(a_1, a_2, \dots, a_m) \end{bmatrix}. \quad (4)$$

Лемма 2. Для любой булевой функции λ от m переменных пара (A, q_λ) является m -квазигруппой, причём $q_\lambda \equiv q_{\tilde{\lambda}}$ тогда и только тогда, когда $\lambda \equiv \tilde{\lambda}$.

Доказательство. Пусть наборы

$$c = \left(\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}, \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}, \dots, \begin{bmatrix} a_m \\ b_m \end{bmatrix} \right), \quad c' = \left(\begin{bmatrix} a'_1 \\ b'_1 \end{bmatrix}, \begin{bmatrix} a'_2 \\ b'_2 \end{bmatrix}, \dots, \begin{bmatrix} a'_m \\ b'_m \end{bmatrix} \right)$$

из A^m различаются только в i -й координате.

Если $a_i \neq a'_i$, то $q_\lambda(c)$ и $q_\lambda(c')$ различаются в верхнем бите.

Если $a_i = a'_i$ и $b_i \neq b'_i$, то $\lambda(a_1, a_2, \dots, a_m) = \lambda(a'_1, a'_2, \dots, a'_m)$ и $q_\lambda(c)$, $q_\lambda(c')$ различаются в нижнем бите.

Таким образом, по определению (A, q_λ) является m -квазигруппой.

Если $\lambda(a_1, \dots, a_m) \neq \tilde{\lambda}(a_1, \dots, a_m)$, то

$$q_\lambda \left(\begin{bmatrix} a_1 \\ 0 \end{bmatrix}, \begin{bmatrix} a_2 \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} a_m \\ 0 \end{bmatrix} \right) \neq q_{\tilde{\lambda}} \left(\begin{bmatrix} a_1 \\ 0 \end{bmatrix}, \begin{bmatrix} a_2 \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} a_m \\ 0 \end{bmatrix} \right).$$

Лемма 2 доказана.

Рассмотрим оператор $\pi : A \rightarrow A$, определяемый равенством

$$\pi \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \oplus b \\ a \end{bmatrix}.$$

Легко проверяются следующие свойства этого оператора:

(а) оператор π является линейным, т. е.

$$\pi \left(\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \oplus \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} \right) = \pi \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \oplus \pi \begin{bmatrix} a_2 \\ b_2 \end{bmatrix};$$

(б) $\pi \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$ тогда и только тогда, когда $\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$;

(с) $\pi^2 = \pi^{-1}$ и $\pi^3 = \pi^0$ — тождественный оператор.

Пусть $\lambda = \lambda(x_1, \dots, x_m)$ — булева функция от m переменных, $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_m)$ — набор операторов из $\{\pi^0, \pi^1, \pi^2\}$, $\alpha \in \{0, 1\}$ и операция $q_{\lambda, \alpha, \sigma}$ задаётся равенством

$$q_{\lambda, \alpha, \sigma} \left(\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}, \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}, \dots, \begin{bmatrix} a_m \\ b_m \end{bmatrix} \right) = q_{\lambda} \left(\sigma_1 \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}, \sigma_2 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}, \dots, \sigma_m \begin{bmatrix} a_m \\ b_m \end{bmatrix} \right) \oplus \begin{bmatrix} \alpha \\ 0 \end{bmatrix}. \quad (5)$$

Лемма 3. Для любой булевой функции λ от m переменных, любого $\alpha \in \{0, 1\}$ и любого набора $\sigma \in \{\pi^0, \pi^1, \pi^2\}^m$ пара $(A, q_{\lambda, \alpha, \sigma})$ является m -квазигруппой, причём $q_{\lambda, \alpha, \sigma} \equiv q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}}$ тогда и только тогда, когда $\lambda \equiv \tilde{\lambda}$, $\alpha = \tilde{\alpha}$ и $\sigma = \tilde{\sigma}$.

Доказательство. Так как произвольные наборы

$$\left(\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}, \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}, \dots, \begin{bmatrix} a_m \\ b_m \end{bmatrix} \right), \quad \left(\begin{bmatrix} a'_1 \\ b'_1 \end{bmatrix}, \begin{bmatrix} a'_2 \\ b'_2 \end{bmatrix}, \dots, \begin{bmatrix} a'_m \\ b'_m \end{bmatrix} \right)$$

из A^m различаются в тех же координатах, что и наборы

$$\left(\sigma_1 \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}, \sigma_2 \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}, \dots, \sigma_m \begin{bmatrix} a_m \\ b_m \end{bmatrix} \right), \quad \left(\sigma_1 \begin{bmatrix} a'_1 \\ b'_1 \end{bmatrix}, \sigma_2 \begin{bmatrix} a'_2 \\ b'_2 \end{bmatrix}, \dots, \sigma_m \begin{bmatrix} a'_m \\ b'_m \end{bmatrix} \right),$$

то по лемме 2 пара $(A, q_{\lambda, \alpha, \sigma})$ является m -квазигруппой.

Покажем, что если справедливо по крайней мере одно из неравенств $\alpha \neq \tilde{\alpha}$, $\sigma \neq \tilde{\sigma}$, $\lambda \neq \tilde{\lambda}$, то при некоторых значениях аргумента $q_{\lambda, \alpha, \sigma} \neq q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}}$. Будем различать три случая.

1. Пусть $\alpha \neq \tilde{\alpha}$. Тогда на нулевом наборе значения $q_{\lambda, \alpha, \sigma}$ и $q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}}$ различаются в верхнем бите.

2. Пусть $\alpha = \tilde{\alpha}$, $\sigma_i \neq \tilde{\sigma}_i$ при некотором i . Пусть

$$c = \left(\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \sigma_i^{-1} \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right)$$

— набор, в котором значение i -й координаты отлично от нуля. Тогда

$$q_{\lambda, \alpha, \sigma}(c) = \begin{bmatrix} 0 \\ 1 \oplus \lambda(0, \dots, 0) \end{bmatrix} \oplus \begin{bmatrix} \alpha \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ 1 \oplus \lambda(0, \dots, 0) \end{bmatrix}.$$

Поскольку $\sigma_i \neq \tilde{\sigma}_i$, оператор $\tilde{\sigma}_i \sigma_i^{-1}$ равен π или π^{-1} . Поэтому $\tilde{\sigma}_i \sigma_i^{-1} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ равно $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ или $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ по свойству (b). Следовательно,

$$q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}}(c) = \begin{bmatrix} 1 \\ \dots \end{bmatrix} \oplus \begin{bmatrix} \tilde{\alpha} \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \oplus 1 \\ \dots \end{bmatrix} \neq q_{\lambda, \alpha, \sigma}(c).$$

3. Пусть $\alpha = \tilde{\alpha}$, $\sigma = \tilde{\sigma}$ и $\lambda(a_1, \dots, a_m) \neq \tilde{\lambda}(a_1, \dots, a_m)$ при некоторых a_1, \dots, a_m . Тогда при $c = \left(\sigma_1^{-1} \begin{bmatrix} a_1 \\ 0 \end{bmatrix}, \sigma_2^{-1} \begin{bmatrix} a_2 \\ 0 \end{bmatrix}, \dots, \sigma_m^{-1} \begin{bmatrix} a_m \\ 0 \end{bmatrix} \right)$ имеем

$$q_{\lambda, \alpha, \sigma}(c) = \begin{bmatrix} \dots \\ \lambda(a_1, \dots, a_m) \end{bmatrix} \neq q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}}(c) = \begin{bmatrix} \dots \\ \tilde{\lambda}(a_1, \dots, a_m) \end{bmatrix}.$$

Лемма 3 доказана.

Булева функция $\lambda(x_1, x_2, \dots, x_m)$ называется *линейной*, если она представима в виде $\alpha_0 \oplus \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \dots \oplus \alpha_m x_m$, где $\alpha_0, \alpha_1, \dots, \alpha_m$ — константы, равные 0 или 1. Число линейных булевых функций от m переменных равно 2^{m+1} .

Лемма 4. Пусть $\varphi \in \{\pi, \pi^2\}$ и $q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}} = \varphi q_{\lambda, \alpha, \sigma}$, где $q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}}$ и $q_{\lambda, \alpha, \sigma}$ определяются равенствами (5) и (4). Тогда функция λ линейна.

Доказательство. Из (4) и (5) следует, что

$$q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}} \left(\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}, \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}, \dots, \begin{bmatrix} a_m \\ b_m \end{bmatrix} \right) = \begin{bmatrix} L(a_1, \dots, a_m, b_1, \dots, b_m) \\ \dots \end{bmatrix},$$

$$q_{\lambda, \alpha, \sigma} = \begin{bmatrix} L_1(a_1, \dots, a_m, b_1, \dots, b_m) \\ L_2(a_1, \dots, a_m, b_1, \dots, b_m) \oplus \lambda(l_1(a_1, b_1), l_2(a_2, b_2), \dots, l_m(a_m, b_m)) \end{bmatrix},$$

где $L, L_1, L_2, l_1, \dots, l_m$ — линейные функции, отличные от констант.

По условию имеем $\varphi \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \oplus b \\ a \end{bmatrix}$ или $\varphi \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \oplus b \end{bmatrix}$. Поэтому

$$\varphi q_{\lambda, \alpha, \sigma} = \begin{bmatrix} L_0(a_1, \dots, a_m, b_1, \dots, b_m) \oplus \lambda(l_1(a_1, b_1), l_2(a_2, b_2), \dots, l_m(a_m, b_m)) \\ \dots \end{bmatrix},$$

где $L_0 = L_1 \oplus L_2$ или $L_0 = L_2$.

Таким образом, из равенства $q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}} = \varphi q_{\lambda, \alpha, \sigma}$ следует, что

$$\begin{aligned} \lambda(l_1(a_1, b_1), l_2(a_2, b_2), \dots, l_m(a_m, b_m)) \\ = L(a_1, \dots, a_m, b_1, \dots, b_m) \oplus L_0(a_1, \dots, a_m, b_1, \dots, b_m) \end{aligned}$$

и λ — линейная функция. Лемма 4 доказана.

Лемма 5. Если $\varphi \in \{\pi^0, \pi, \pi^2\}$, то

а) множество A с операцией $q_{\lambda, \alpha, \sigma, \varphi} = \varphi q_{\lambda, \alpha, \sigma}$ является m -квазигруппой;

б) если хотя бы одна из функций $\lambda, \tilde{\lambda}$ нелинейна, то $q_{\lambda, \alpha, \sigma, \varphi} \equiv q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}, \tilde{\varphi}}$ тогда и только тогда, когда $\lambda \equiv \tilde{\lambda}, \alpha = \tilde{\alpha}, \sigma = \tilde{\sigma}$ и $\varphi = \tilde{\varphi}$.

Доказательство. а) Из леммы 3 и обратимости оператора φ вытекает, что $(A, q_{\lambda, \alpha, \sigma, \varphi})$ является m -квазигруппой.

б) Пусть

$$q_{\lambda, \alpha, \sigma, \varphi} = q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}, \tilde{\varphi}}. \quad (6)$$

Не уменьшая общности, допустим, что функция λ нелинейна. Поскольку

$$\tilde{\varphi}^{-1} q_{\lambda, \alpha, \sigma, \varphi} = \tilde{\varphi}^{-1} \varphi q_{\lambda, \alpha, \sigma} \quad \text{и} \quad \tilde{\varphi}^{-1} q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}, \tilde{\varphi}} = q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}},$$

то из (6) следует, что

$$\tilde{\varphi}^{-1} \varphi q_{\lambda, \alpha, \sigma} = q_{\tilde{\lambda}, \tilde{\alpha}, \tilde{\sigma}}. \quad (7)$$

Если $\varphi \neq \tilde{\varphi}$, то $\tilde{\varphi}^{-1} \varphi \in \{\pi, \pi^2\}$, и (7) противоречит нелинейности функции λ по лемме 4.

Если $\varphi = \tilde{\varphi}$, то $\tilde{\varphi}^{-1} \varphi = \pi^0$ — тождественный оператор. Пользуясь леммой 3 и (7), получаем, что $\lambda \equiv \tilde{\lambda}, \alpha = \tilde{\alpha}$ и $\sigma = \tilde{\sigma}$. Лемма 5 доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. По лемме 5 все m -квазигруппы вида $(A, q_{\lambda, \alpha, \sigma, \varphi})$, где λ — нелинейная функция, различны. Число таких m -квазигрупп равно

$$(2^{2^m} - 2^{m+1}) \cdot 2 \cdot 3^m \cdot 3. \quad (8)$$

По лемме 4 среди них нет m -квазигрупп вида $(A, q_{\lambda, \alpha, \sigma})$, где λ — линейная функция. Все такие m -квазигруппы различны по лемме 3, и их число равно

$$2^{m+1} \cdot 2 \cdot 3^m. \quad (9)$$

Сложив (8) и (9), получим утверждение теоремы.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьёва Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами $\tilde{\alpha}$ -компонент // Проблемы передачи информации. 1997. Т. 33, вып. 3. С. 15–21.
2. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Наука, 1962. Вып. 8. С. 337–339.
3. **Малюгин С. А.** О нижней оценке числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций. 1999. Т. 6, № 4. С. 44–48.
4. **Cohen G., Honkala I., Litsyn S., Lobstein A.** Covering codes. North-Holland: Elsevier, 1998.
5. **Phelps K. T.** A general product construction for error correcting codes // SIAM J. Algebraic Discrete Methods, 1984. V. 5, N 2. P. 224–228.
6. **Solov'eva F. I.** Constructions of perfect binary codes // Preprint 98–042. Univ. Bielefeld, 1998. 12 p.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск, Россия.
E-mail: dkrotov@mail.ru

Статья поступила
10 января 2000 г.