

УДК 519.72

О СОВЕРШЕННОМ КОДЕ, СОДЕРЖАЩЕМ В КАЧЕСТВЕ ПОДКОДОВ ЗАДАННЫЙ НАБОР СОВЕРШЕННЫХ КОДОВ

Д. С. Кротов

Предложена конструкция, которая для произвольно заданного набора $\{C_1, C_2, \dots, C_M\}$ совершенных двоичных $(m, 3)$ -кодов (т. е. кодов длины m с исправлением одной ошибки) позволяет построить универсальный совершенный $(nm + n + m, 3)$ -код, $2^{n - \log_2(n+1)} \geq M$, содержащий все коды данного набора в качестве подкодов на параллельных гранях размерности m . Конструкция является обобщением конструкции произведения совершенных кодов, предложенной Молларом, и имеет аналоги для совершенных кодов над произвольным конечным полем и над кольцом Z_4 .

Пусть V_q^n — векторное пространство размерности n над полем $GF(q)$. Зафиксируем в V_q^n некоторый базис. Расстоянием (Хемминга) $d(y, z)$ между векторами $y, z \in V_q^n$ называется число координат, в которых x и y различаются. Подмножество C пространства V_q^n называется совершенным q -ичным кодом длины n с расстоянием 3 (далее просто совершенным кодом), если $|C| = q^{n - \log_q(q^n - n + 1)}$ и расстояние между любыми двумя различными кодовыми векторами не меньше 3 (эти условия эквивалентны плотной упаковке в V_q^n шаров единичного радиуса с центрами в кодовых векторах). Такой код может существовать только при $n = \frac{q^k - 1}{q - 1}$, где k — целое неотрицательное число, и обладает следующим свойством: для любого вектора $x \in V_q^n$ найдется только один кодовый вектор $y \in C$ такой, что $d(x, y) \leq 1$. Сдвигом на вектор $z \in V_q^n$ совершенного кода C^n называется множество $C^n \oplus z = \{c \oplus z \mid c \in C^n\}$, также являющееся совершенным кодом. Код C называется линейным, если он является подпространством векторного пространства V_q^n .

Подмножество \bar{C} пространства V_2^n называется расширенным совершенным двоичным кодом, если расстояние между любыми двумя различными кодовыми векторами не меньше 4, а после удаления последней координаты получается совершенный код.

Линейные совершенные коды были описаны Р. В. Хеммингом (см., например, [3]) для $q = 2$ и Г. С. Шапиро и Д. Л. Злотником [4] в произвольном случае. Первая конструкция нелинейных совершенных кодов была построена Ю. Л. Васильевым [2] для двоичного случая и обобщена Дж. Шонхеймом [7] для случая произвольного q .

Большое число двоичных кодов Васильева достигается возможностью произвольного выбора функции λ , действующей из совершенного кода $C^{(n-1)/2}$ длины $(n-1)/2$ в множество $\{0, 1\}$. При помощи конструкции произведения двух кодов $C^{n'}$ и $C^{n''}$ длин n' и n'' (дающего в результате код длины $n'n'' + n' + n''$), М. Моллар [6] заменил функцию λ на функцию, которая отображает код $C^{n'}$ в векторное пространство $V_2^{n''}$ (а также описал q -ичное обобщение своей конструкции). Ф. И. Соловьева [8] показала, что существуют коды Моллара, которые не описываются конструкцией Васильева.

В предложенной нами конструкции функция λ каждому кодовому слову c' из $C^{n'}$ ставит в соответствие совершенный код $C_{\lambda(c')}^{n''}$ длины n'' . Это позволяет «упаковать» M произвольных совершенных кодов длины n'' в качестве подкодов на параллельных гранях в один «универсальный» совершенный код, длина которого примерно в $\log_2 M$ раз больше n'' . Ни одна из известных автору описанных ранее конструкций не дает такой возможности (отметим, что существует много конструкций совершенных кодов, не упомянутых в данной статье, см., например, [9]). Многократное применение каскадных конструкций позволяет построить код, содержащий все заданные коды в качестве подкодов, но, во-первых, эти подкоды не будут лежать в параллельных гранях, а, во-вторых, при больших M длина такого «универсального» кода будет весьма значительной.

В § 1 описывается конструкция двоичных совершенных кодов. В § 2 приводится ее обобщение для кодов над произвольным конечным полем. В § 3 описывается аналогичная конструкция построения расширенных совершенных кодов с расстоянием 4 над кольцом Z_4 .

§ 1. Двоичные коды

Обозначим через $E^n = V_2^n$ векторное пространство размерности n над полем $GF(2) = (\{0, 1\}, \oplus, \cdot)$ целых чисел по модулю 2.

Пусть $\{C_1^{n''}, C_2^{n''}, \dots, C_M^{n''}\}$ — множество совершенных двоичных кодов длины n'' , $C^{n'}$ — совершенный двоичный код длины n' и $\lambda : C^{n'} \rightarrow \{1, \dots, M\}$ — функция, при помощи которой каждому вектору $x \in C^{n'}$ ставится в соответствие код $C_{\lambda(x)}^{n''}$. Пусть

$$x = (x_{11}, x_{12}, \dots, x_{1n'}, x_{21}, \dots, x_{2n''}, \dots, x_{n'1}, \dots, x_{n'n''}) \in E^{n'n''},$$

$$p'_i(x) = \sum_{j=1}^{n''} x_{ij} \quad \text{и} \quad p''_j(x) = \sum_{i=1}^{n'} x_{ij}.$$

Тогда обобщенные функции четности [6] определяются следующим образом:

$$p'(x) = (p'_1(x), p'_2(x), \dots, p'_{n'}(x)) \quad \text{и} \quad p''(x) = (p''_1(x), p''_2(x), \dots, p''_{n''}(x)).$$

Теорема 1. Множество

$$C^n = \{(x, p'(x) \oplus c', p''(x) \oplus c'') \mid x \in E^{n'n''}, c' \in C^{n'}, c'' \in C^{n''}_{\lambda(c')}\} \quad (1)$$

является совершенным кодом длины $n = n'n'' + n' + n''$.

Теорема 1 является частным случаем (при $q = 2$) теоремы 2, доказанной в следующем параграфе.

Будем говорить, что совершенный код $C^{n''}$ длины n'' является n'' -подкодом совершенного кода C^n длины $n \geq n''$, если существует такой вектор $y \in E^{n-n''}$, что $\{(y, c'') \mid c'' \in C^{n''}\} \subset C^n$. Поскольку в этом определении фиксируются первые $n - n''$ координат, то все n'' -подкоды кода C^n содержатся в параллельных гранях размерности n'' .

Предложение 1. Любой сдвиг каждого кода $C^{n''}_{\lambda(c')}$, $c' \in C^{n'}$, является n'' -подкодом кода C^n , определенного в (1).

Доказательство. Возьмем произвольные $c' \in C^{n'}$ и $z \in E^{n''}$. Выберем такой вектор x , что $p''(x) = z$ (например, $x_{1j} = z_j$, $x_{ij} = 0$, $i \neq 1$). Тогда из (1) следует, что $(x, p'(x) \oplus c', z \oplus c'') \in C^n$ при $c'' \in C^{n''}_{\lambda(c')}$, т. е. $C^{n''}_{\lambda(c')} \oplus z$ является n'' -подкодом кода C^n . Предложение доказано.

Поскольку при $|C^{n'}| \geq M$ можно выбрать функцию λ , которая отображает $C^{n'}$ на всё множество $\{1, \dots, M\}$, получаем

Следствие 1. Для любого множества $\{C^{n''}_1, \dots, C^{n''}_M\}$ мощности M совершенных кодов длины n'' и целого положительного n' такого, что $2^{n' - \log_2(n'+1)} \geq M$, существует код C^n длины $n = n'n'' + n' + n''$, содержащий в качестве n'' -подкодов все сдвиги каждого кода $C^{n''}_j$, $1 \leq j \leq M$.

ПРИМЕР 1. Пусть $n'' = 1$ и при помощи функции $\lambda : C^{n'} \rightarrow \{0, 1\}$ каждому вектору из $C^{n'}$ ставится в соответствие код длины 1, состоящий из 0 и 1. Тогда конструкция (1) описывает коды Васильева [2].

ПРИМЕР 2. Пусть коды $C^{n''}_1, \dots, C^{n''}_M$ являются сдвигами некоторого фиксированного совершенного кода $C^{n''}$: $C^{n''}_l = C^{n''} \oplus z_l$, $z_l \in E^{n''}$. В этом случае (1) совпадает с конструкцией Моллара [6].

ПРИМЕР 3. В работе [1] показано, что число совершенных кодов длины n'' не превосходит $2^{2^{n''} - \frac{3}{2} \log_2 n'' + \log_2 \log_2 n''}$. Из этого факта и следствия 1 вытекает, что существует совершенный код длины

$2^{[n'' - \frac{1}{2} \log_2 n'' + \log_2 \log_2 \varepsilon n'' + 2]} - 1$, содержащий в качестве n'' -подкодов все возможные совершенные коды длины n'' .

ПРИМЕР 4. Пусть $C_1^{n''}$ и $C_2^{n''}$ — произвольные совершенные коды длины n'' . Если взять $n' = 3$, $C^{n'} = \{(000), (111)\}$, $\lambda(000) = 1$ и $\lambda(111) = 2$, то (1) даёт код длины $4n'' + 3$, содержащий в качестве n'' -подкодов оба данных кода.

§ 2. Коды по основанию q

Пусть q — степень простого числа и a_1, a_2, \dots, a_{q-1} — ненулевые элементы поля $GF(q)$. Пусть $\{C_1^{n''}, C_2^{n''}, \dots, C_M^{n''}\}$ — множество совершенных q -ичных кодов длины n'' , $C^{n'}$ — совершенный q -ичный код длины n' и $\lambda : C^{n'} \rightarrow \{1, \dots, M\}$ — функция, при помощи которой каждому вектору $x \in C^{n'}$ ставится в соответствие код $C_{\lambda(x)}^{n''}$. Пусть

$$x = (x_{111}, \dots, x_{(q-1)n'n''}) \in V^{(q-1)n'n''}$$

(индексы перечисляются в лексикографическом порядке). Определим функции

$$p'(x) = (p'_1(x), p'_2(x), \dots, p'_{n'}(x)), \quad p''(x) = (p''_1(x), p''_2(x), \dots, p''_{n''}(x)),$$

полагая

$$p'_i(x) = \sum_{j=1}^{n'} \sum_{l=1}^{q-1} x_{lij}, \quad p''_j(x) = \sum_{i=1}^{n'} \sum_{l=1}^{q-1} a_l x_{lij}.$$

Теорема 2. Множество

$$C^n = \{(x, p'(x) \oplus c', p''(x) \oplus c'') \mid x \in V^{(q-1)n'n''}, c' \in C^{n'}, c'' \in C_{\lambda(c')}^{n''}\} \quad (2)$$

является совершенным кодом длины $n = (q-1)n'n'' + n' + n''$.

ДОКАЗАТЕЛЬСТВО. Из построения (2) легко видеть, что

$$\begin{aligned} |C^n| &= q^{(q-1)n'n''} |C^{n'}| |C^{n''}| = q^{(q-1)n'n''} q^{n' - \log_q(qn' - n' + 1)} q^{n'' - \log_q(qn'' - n'' + 1)} \\ &= q^{(q-1)n'n'' + n' + n'' - \log_q(q((q-1)n'n'' + n' + n'') - (q-1)n'n'' - n' - n'' + 1)} \\ &= q^{n - \log_q(qn - n + 1)}, \end{aligned}$$

т. е. код C^n имеет нужную мощность.

Чтобы найти минимальное кодовое расстояние, рассмотрим векторы $c = (x, p'(x) \oplus c', p''(x) \oplus c'')$ и $\tilde{c} = (\tilde{x}, p'(\tilde{x}) \oplus \tilde{c}', p''(\tilde{x}) \oplus \tilde{c}'')$ из C^n .

(А) Пусть $c' \neq \tilde{c}'$. Тогда $d(c', \tilde{c}') \geq 3$. Если значения выражений $p'_i(x) + c'_i - \sum_{j=1}^{n'} \sum_{l=1}^{q-1} x_{lij} = c'_i$ и $p'_i(\tilde{x}) + \tilde{c}'_i - \sum_{j=1}^{n'} \sum_{l=1}^{q-1} \tilde{x}_{lij} = \tilde{c}'_i$ различны, то наборы

$$\begin{aligned} &(x_{1i1}, \dots, x_{1in''}, \dots, x_{(q-1)i1}, \dots, x_{(q-1)in''}, p'_i(x) + c'_i), \\ &(\tilde{x}_{1i1}, \dots, \tilde{x}_{1in''}, \dots, \tilde{x}_{(q-1)i1}, \dots, \tilde{x}_{(q-1)in''}, p'_i(\tilde{x}) + \tilde{c}'_i) \end{aligned}$$

различаются по крайней мере в одной позиции. А поскольку неравенство $c'_i \neq \tilde{c}'_i$ выполняется не менее чем при трех различных значениях i , то c и \tilde{c} различаются не менее чем в трех координатах. Следовательно, $d(c, \tilde{c}) \geq 3$.

(В) Пусть $c' = \tilde{c}'$ и $c'' \neq \tilde{c}''$. Тогда c'' и \tilde{c}'' принадлежат одному совершенному коду, $d(c'', \tilde{c}'') \geq 3$ и аналогично (А) наборы

$$\begin{aligned} (x_{11j}, \dots, x_{1n'j}, \dots, x_{(q-1)1j}, \dots, x_{(q-1)n'j}, p''_j(x) + c''_j), \\ (\tilde{x}_{11j}, \dots, \tilde{x}_{1n'j}, \dots, \tilde{x}_{(q-1)1j}, \dots, \tilde{x}_{(q-1)n'j}, p''_j(\tilde{x}) + \tilde{c}''_j) \end{aligned}$$

не совпадают по крайней мере при трех различных значениях j . Поэтому $d(c, \tilde{c}) \geq 3$.

(С) Наконец, пусть $c' = \tilde{c}'$, $c'' = \tilde{c}''$, $x \neq \tilde{x}$. Рассмотрим три подслучая.

(С1) x и \tilde{x} различаются в одной координате: $x_{lj} \neq \tilde{x}_{lj}$. Тогда

$$\begin{aligned} p'_i(x) - p'_i(\tilde{x}) &= x_{lj} - \tilde{x}_{lj} \neq 0, \\ p''_j(x) - p''_j(\tilde{x}) &= a_l(x_{lj} - \tilde{x}_{lj}) \neq 0. \end{aligned}$$

Следовательно, $p'(x) \neq p'(\tilde{x})$, $p''(x) \neq p''(\tilde{x})$ и

$$d(c, \tilde{c}) = d(x, \tilde{x}) + d(p'(x), p'(\tilde{x})) + d(p''(x), p''(\tilde{x})) = 1 + 1 + 1 = 3.$$

(С2) x и \tilde{x} различаются в двух координатах: $x_{lj} \neq \tilde{x}_{lj}$ и $x_{l'ij'} \neq \tilde{x}_{l'ij'}$.

Если $i \neq i'$, то

$$\begin{aligned} p'_i(x) - p'_i(\tilde{x}) &= x_{lj} - \tilde{x}_{lj} \neq 0, \\ p'_{i'}(x) - p'_{i'}(\tilde{x}) &= x_{l'ij'} - \tilde{x}_{l'ij'} \neq 0 \end{aligned}$$

и $d(c, \tilde{c}) \geq d(x, \tilde{x}) + d(p'(x), p'(\tilde{x})) = 2 + 2 = 4$.

Если $j \neq j'$, то аналогично имеем $d(c, \tilde{c}) \geq d(x, \tilde{x}) + d(p''(x), p''(\tilde{x})) = 2 + 2 = 4$.

Если $i = i'$ и $j = j'$, то $l \neq l'$ и выражения

$$p'_i(x) - p'_i(\tilde{x}) = x_{lj} - \tilde{x}_{lj} + x_{l'ij} - \tilde{x}_{l'ij},$$

$$\begin{aligned} p''_j(x) - p''_j(\tilde{x}) &= a_l(x_{lj} - \tilde{x}_{lj}) + a_{l'}(x_{l'ij} - \tilde{x}_{l'ij}) \\ &= a_l(x_{lj} - \tilde{x}_{lj} + x_{l'ij} - \tilde{x}_{l'ij}) + (a_{l'} - a_l)(x_{l'ij} - \tilde{x}_{l'ij}) \end{aligned}$$

не могут одновременно быть равны нулю. Поэтому $d(c, \tilde{c}) = d(x, \tilde{x}) + d(p'(x), p'(\tilde{x})) + d(p''(x), p''(\tilde{x})) \geq 2 + 1 = 3$.

(С3) Оставшийся случай $d(x, \tilde{x}) \geq 3$ тривиален. Теорема 2 доказана.

ПРИМЕР 1'. Коды Шонхейма [7] получаются при $n'' = 1$; при помощи функции $\lambda : C^{n'} \rightarrow \{0, 1, \dots, q-1\}$ каждому вектору из $C^{n'}$ поставлен в соответствие тривиальный совершенный код из множества $\{C_l^1\}_{l=0}^{q-1}$, где $C_l^1 = \{a_l\}$, $a_0 = 0$.

ПРИМЕР 2'. В случае, когда в качестве набора кодов длины n'' берется множество $\{C^{n''} + z \mid z \in V_q^{n''}\}$ сдвигов фиксированного кода $C^{n''}$, конструкция (2) описывает q -ичные коды Моллара [6].

§ 3. Конструкция кодов над кольцом Z_4

Рассмотрим модуль Z_4^n размерности n над кольцом $(\{0, 1, 2, 3\}, +, \cdot)$ целых чисел по mod 4, элементы которого будем называть *словами*. Ниже все операции над элементами Z_4 осуществляются по mod 4. Вес Ли $wt(y)$ слова $y = (y_1, \dots, y_n) \in Z_4^n$ определяется как обычная сумма весов его координат: $wt(y) = \sum_{i=1}^n wt(y_i)$, где $wt(0) = 0$, $wt(1) = wt(3) = 1$ и $wt(2) = 2$. Расстоянием Ли между словами y и z из Z_4^n называется число $d(y, z) = wt(y - z)$. Нам понадобится следующая простая

Лемма 1. Пусть $y = (y_1, \dots, y_n)$ и $z = (z_1, \dots, z_n)$ принадлежат Z_4^n . Тогда

$$d(y, z) \geq wt\left(\sum_{i=1}^n y_i - \sum_{i=1}^n z_i\right). \quad (3)$$

ДОКАЗАТЕЛЬСТВО. Если $y = z$, то правая часть из (3) равна 0 и неравенство верно. Если $d(y, z) = 1$, то число в скобках правой части (3) нечетно, вес Ли этого числа равен 1. Поэтому неравенство (3) также выполнено. В оставшихся случаях $d(y, z) \geq 2$, неравенство (3) верно, поскольку вес Ли числа из Z_4 не превосходит 2. Лемма 1 доказана.

Множество $\mathcal{C}^n \subset Z_4^n$ назовем *расширенным совершенным кодом* над Z_4 , если $n = 2^k$, $|\mathcal{C}^n| = 4^{n-\log_4 n-1}$ и для любых $c, \tilde{c} \in \mathcal{C}^n$ либо $d(c, \tilde{c}) \geq 4$, либо $c = \tilde{c}$.

При помощи отображения Грея $0 \rightarrow (0, 0), 1 \rightarrow (0, 1), 2 \rightarrow (1, 1), 3 \rightarrow (1, 0)$, которое каждому числу из Z_4 ставит в соответствие пару чисел из $\{0, 1\}$ (см. [5]), любому расширенному совершенному коду над Z_4 можно поставить в соответствие расширенный совершенный код длины $2n$ над $GF(2)$ с расстоянием 4. Удалив одну координату в этом коде, получим совершенный двоичный код с расстоянием 3.

Расширенный совершенный код \mathcal{C}^n назовем *четным*, если сумма всех координат любого кодового слова равна 0.

Пусть $\{\mathcal{C}_1^{n''}, \mathcal{C}_2^{n''}, \dots, \mathcal{C}_M^{n''}\}$ — множество четных расширенных совершенных кодов длины n'' , $\mathcal{C}^{n'}$ — четный расширенный совершенный

код длины n' и $\lambda : \mathcal{C}^{n'} \rightarrow \{1, \dots, M\}$ — функция, при помощи которой каждому слову $x \in \mathcal{C}^{n'}$ ставится в соответствие код $\mathcal{C}_{\lambda(x)}^{n''}$. Пусть

$$x = (x_{11}, x_{12}, \dots, x_{1n''}, x_{21}, \dots, x_{2n''}, \dots, x_{n'1}, \dots, x_{n'n''}) \in Z_4^{n'n''};$$

$$p'(x) = (p'_1(x), p'_2(x), \dots, p'_{n'}(x)), \quad p''(x) = (p''_1(x), p''_2(x), \dots, p''_{n''}(x)),$$

где

$$p'_i(x) = - \sum_{j=1}^{n''} x_{ij}, \quad p''_j(x) = - \sum_{i=1}^{n'} x_{ij}.$$

Теорема 3. Множество

$$\mathcal{C}^n = \{x \mid x \in Z_4^{n'n''}, p'(x) = c' \in \mathcal{C}^{n'}, p''(x) = c'' \in \mathcal{C}_{\lambda(c')}^{n''}\} \quad (4)$$

является четным расширенным совершенным кодом длины $n = n'n''$.

ДОКАЗАТЕЛЬСТВО. Найдем мощность кода \mathcal{C}^n . Кодовое слово c' из $\mathcal{C}^{n'}$ можно выбрать $|\mathcal{C}^{n'}| = 4^{n' - \log_4 n' - 1}$ способами; кодовое слово c'' из $\mathcal{C}_{\lambda(c')}^{n''}$ можно выбрать $4^{n'' - \log_4 n'' - 1}$ способами; x_{ij} можно выбрать произвольными для $i = 1, \dots, n' - 1, j = 1, \dots, n'' - 1$. Далее, из равенств $p'_i(x) = c'_i, i = 1, \dots, n' - 1$, однозначно определяются $x_{in''}$ при $i = 1, \dots, n' - 1$; из равенств $p''_j(x) = c''_j, j = 1, \dots, n'' - 1$ однозначно определяются $x_{n'j}$ при $j = 1, \dots, n'' - 1$; равенством $\sum_{i=1}^{n'} \sum_{j=1}^{n''} x_{ij} = 0$, обеспечивающим четность кода \mathcal{C}^n , задается $x_{n'n''}$ (справедливость равенств $p'_{n'}(x) = c'_{n'}$ и $p''_{n''}(x) = c''_{n''}$ следует из четности кодов $\mathcal{C}^{n'}$ и $\mathcal{C}_{\lambda(c')}^{n''}$). Поэтому

$$|\mathcal{C}^n| = 4^{n' - \log_4 n' - 1} 4^{n'' - \log_4 n'' - 1} 4^{(n'-1)(n''-1)} = 4^{n'n'' - \log_4 n'n'' - 1} = 4^{n - \log_4 n - 1}.$$

Покажем, что $d(c, \tilde{c}) \geq 4$ для любых различных кодовых слов c и \tilde{c} из \mathcal{C}^n , где $p'(c) = c', p''(c) = c''$ и $p'(\tilde{c}) = \tilde{c}', p''(\tilde{c}) = \tilde{c}''$.

(А) Пусть $c' \neq \tilde{c}'$. Тогда $d(c', \tilde{c}') \geq 4$ и из леммы 1 следует, что

$$\begin{aligned} d(c, \tilde{c}) &= \sum_{i=1}^{n'} d((c_{i1}, \dots, c_{in''}), (\tilde{c}_{i1}, \dots, \tilde{c}_{in''})) \\ &\geq \sum_{i=1}^{n'} wt \left(\sum_{j=1}^{n''} c_{ij} - \sum_{j=1}^{n''} \tilde{c}_{ij} \right) = \sum_{i=1}^{n'} wt(c'_i - \tilde{c}'_i) \geq 4. \end{aligned}$$

(В) Пусть $c' = \tilde{c}'$ и $c'' \neq \tilde{c}''$. Тогда $c'', \tilde{c}'' \in \mathcal{C}_{\lambda(c')}^{n''} = \mathcal{C}_{\lambda(\tilde{c}')}^{n''}$. Поэтому $d(c'', \tilde{c}'') \geq 4$ и аналогично случаю (А) получаем

$$d(c, \tilde{c}) \geq \sum_{j=1}^{n''} wt \left(\sum_{i=1}^{n'} c_{ij} - \sum_{i=1}^{n'} \tilde{c}_{ij} \right) = \sum_{j=1}^{n''} wt(c''_j - \tilde{c}''_j) \geq 4.$$

(С) Наконец, пусть $c' = \tilde{c}'$, $c'' = \tilde{c}''$. Запишем разность $c - \tilde{c}$ в виде матрицы

$$\begin{pmatrix} c_{11} - \tilde{c}_{11} & c_{12} - \tilde{c}_{12} & \dots & c_{1n''} - \tilde{c}_{1n''} \\ c_{21} - \tilde{c}_{21} & c_{22} - \tilde{c}_{22} & \dots & c_{2n''} - \tilde{c}_{2n''} \\ \dots & \dots & \dots & \dots \\ c_{n'1} - \tilde{c}_{n'1} & c_{n'2} - \tilde{c}_{n'2} & \dots & c_{n'n''} - \tilde{c}_{n'n''} \end{pmatrix}.$$

Сумма элементов любой строки или столбца этой матрицы равна нулю. Поэтому строка или столбец не может содержать только один ненулевой элемент. Таким образом, поскольку матрица ненулевая, она содержит не менее четырех ненулевых элементов. Поэтому кодовые слова c и \tilde{c} различаются по крайней мере в четырех координатах. Теорема 3 доказана.

ПРИМЕР 4'. Пусть $\mathcal{C}_1^{n''}$ и $\mathcal{C}_2^{n''}$ — два произвольных четных расширенных совершенных кода длины n'' . Если взять $n' = 2$, $\mathcal{C}^{n'} = \{(00), (22)\}$, $\lambda(00) = 1$, $\lambda(22) = 2$, то (4) дает код длины $2n''$, содержащий оба данных кода в качестве n'' -подкодов.

ПРИМЕР 5. Индуктивное построение линейного расширенного совершенного кода над Z_4 (циклическое представление этого кода можно найти, например, в [5]) получается, если в качестве $\mathcal{C}^{n'}$ и $\mathcal{C}_i^{n''}$ брать линейные коды, полученные на предыдущих шагах (не применяя к ним операций сдвига или перестановки координат), а в качестве базы взять $\mathcal{C}^2 = \{(00), (22)\}$.

ЗАМЕЧАНИЕ 1. Все утверждения данного параграфа остаются в силе, если вместо Z_4 рассматривать множество двоичных пар $E^2 = \{00, 01, 10, 11\}$ со сложением по mod 2 и расстоянием Хемминга. Это дает модификацию конструкции для расширенных совершенных двоичных кодов.

ЛИТЕРАТУРА

1. **Августинович С. В.** Об одном свойстве совершенных двоичных кодов // Дискрет. анализ и исслед. операций. 1995. Т. 2, № 1. С. 4–6.
2. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Наука, 1962. Вып. 8. С. 337–339.
3. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
4. **Шапиро Г. С., Злотник Д. Л.** К математической теории кодов с исправлением ошибок // Кибернетический сб. М.: Изд-во иностр. лит., 1962. Вып. 5. С. 7–32.

5. **Hammons A. R., Jr., Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P.** The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory. 1994. V. 40, N 2. P. 301–319.
6. **Mollard M.** A generalized parity function and its use in the construction of perfect codes // SIAM J. Algebraic Discrete Methods. 1986. V. 7, N 1. P. 113–115.
7. **Schönheim J.** On linear and nonlinear single-error-correcting q -nary perfect codes // Inform. and Control. 1968. V. 12, N 1. P. 23–26.
8. **Solov'eva F. I.** A combinatorial construction of perfect binary codes // Proc. of Fourth Intern. workshop on algebraic and coding theory. Novgorod, Russia, 1994. P. 171–174.
9. **Solov'eva F. I.** Constructions of perfect binary codes // Preprint 98-042. Sonderforschungsbereich «Diskrete Strukturen in der Mathematik». Univ. Bielefeld, Germany, 1998.

Адрес автора:

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

Статья поступила
9 июня 1999 г.