Известия НАН Армении. Математика, 38, № 2, 2003, 29–36

НОВЫЙ КЛАСС ДВОИЧНЫХ КОДОВ, ИСПРАВЛЯЮЩИХ ОШИБКИ

А. А. Григорьянц

Российско-Армянский (Славянский) государственный университет
E-mail : ar_grig@freenet.am

Резюме. Новые линейные двоичные коды, исправляющие ошибки, получаются из двух семейств кодов с помощью суммы соответствующих тензорных произведений. Исследуются основные параметры нового кода : размерность и расстояние, в частности получены верхние и нижние границы расстояния. Приведены примеры оптимальных кодов на небольших длинах, полученные с помощью новой конструкции. Некоторые классические конструкции являются частными случаями новой конструкции. Поставлен ряд нерешённых задач.

§1. ВВЕДЕНИЕ

Эта статья является вводной для цикла статей, посвящённых исследованию новой конструкции кодов, исправляющих ошибки, полученные из двух семейств с помощью операций тензорного произведения и суммы кодов. Исследуются параметры (размерность и расстояние) новых кодов и приводятся примеры хороших кодов на небольших длинах, полученные этим путем. Также поставлен ряд нерешённых проблем, которые будут рассмотрены в последующих статьях. Настоящая статья дает ответ на несколько вопросов, приведенных в [1], §18. Некоторые классические конструкции являются частными случаями нашей конструкции.

§2. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Под (n, k, d)-кодами понимаются линейные двоичные коды на длине n, размерности k и с минимальным расстоянием d, т.е. k-мерное подпространство арифметического линейного пространства F_2^n над полем $F_2 = \{0; 1\}$. Наряду с терминологией принятой в алгебраической теории кодирования (см. [1]), будем использовать стандартные понятия линейной и тензорной алгебры.

Пусть $\mathbf{C} = \{C_i\}_{i=1}^s$ и $\mathbf{D} = \{D_i\}_{i=1}^s$ – два семейства линейных двоичных кодов на длине n и n', соответственно. Код на длине nn' задаётся по формуле

$$\mathbf{C} \otimes \mathbf{D} = C_1 \otimes D_1 + \cdots + C_s \otimes D_s \tag{1}$$

являющейся суммой тензорных произведений соответствующих кодов из $\mathbf{C}$ и $\mathbf{D}$. Коды вида (1) назовём **фрактальными кодами**. Основные параметры конструкции $\mathbf{C} \otimes \mathbf{D}$ являются объектом исследования настоящей статьи.

Пусть $S = \{1, ..., s\}$ – множество первых s натуральных чисел, а $\alpha = \{i_1, ..., i_r\}$ – произвольное подмножество S. Положим $|\alpha| = r$. Для произвольного семейства кодов $\mathbf{C} = \{C_i\}_{i=1}^s$ рассмотрим коды

$$C^\alpha = \sum_{i \in \alpha} C_i, \quad C_\alpha = \bigcap_{i \in \alpha} C_i. \tag{2}$$

Таким образом, C^α и C_α суть сумма и пересечение линейных подпространств соответствующих мультииндексу α. Также будем использовать обозначение $C_{12} = C_1 \cap C_2$ и т.п. Параметры кодов C^α и C_α будем обозначать через $(n^\alpha, k^\alpha, d^\alpha)$ и $(n_\alpha, k_\alpha, d_\alpha)$, соответственно. Через $(n'^\alpha, k'^\alpha, d'^\alpha)$ и $(n'_\alpha, k'_\alpha, d'_\alpha)$ обозначим параметры соответствующих кодов для семейства $\mathbf{D}$.

Семейство векторов $\mathbf{e} = \{e_i\} \subset \cup C_\alpha$ называется **базисом** семейства подпространств $\mathbf{C} = \{C_i\}_{i=1}^s$, если $C_\alpha \cap \mathbf{e}$ порождает C_α и $\mathbf{e}$ минимальное (по включению) множество с этим свойством. Легко видеть, что любое семейство подпространств обладает базисом. Однако, базис семейства необязательно линейно независимый. Семейство подпространств, обладающее линейно независимым базисом назовем **ацикличным**.

Обозначим через α_a максимальный по мощности, и следовательно, однозначно определённый мультииндекс, для которого $a \in C_{\alpha_a}$. Для произвольного семейства векторов $\mathbf{a} = \{a_i\}$ положим $\Psi(\mathbf{a}) = \{\alpha_{a_i} : a_i \in \mathbf{a}\}$. Пусть Ψ – произвольное подмножество мультииндексов. Выбирая по одному элементу из каждого мультииндекса в Ψ, получим некоторый мультииндекс. Множество всех таких мультииндексов обозначим через Ψ^*.

Основным результатом настоящей статьи является следующая теорема.

Теорема 1. *Пусть $\mathbf{e} = \{e_i\}$ и $\mathbf{g} = \{g_i\}$ – базисы двух ацикличных семейств подпространств $\mathbf{C}$ и $\mathbf{D}$. Тогда размерность кода (1) вычисляется по формуле*

$$\kappa = \sum_\alpha (-1)^{|\alpha|+1} k_\alpha k'_\alpha. \tag{3}$$

Верхняя граница расстояния кода (1) есть

$$\delta \le \min_\alpha (d_\alpha d'^\alpha, d^\alpha d'_\alpha), \tag{4}$$

где минимум берется по всем α, для которых подпространства C_α и D_α ненулевые. Нижняя граница расстояния кода (1) есть

$$\delta \geq \max\left\{ \min_{\Psi_0 \subset \Psi(\mathbf{e})} \left[\left(\max_{\alpha \in \Psi_0} d'^{\alpha} \right) \left(\max_{\beta \in \Psi_0^*} d^{\beta} \right) \right], \min_{\Psi_0 \subset \Psi(\mathbf{g})} \left[\left(\max_{\alpha \in \Psi_0} d^{\alpha} \right) \left(\max_{\beta \in \Psi_0^*} d'^{\beta} \right) \right] \right\}, \tag{5}$$

где Ψ_0 – произвольное непустое подмножество в $\Psi(\mathbf{e})$.

§3. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1

Сначала докажем несколько вспомогательных лемм.

Лемма 1. *Пусть L и M – два линейных пространства. Тогда для любого вектора $x \in L \otimes M$ существует единственное представление вида*

$$x = \sum_i e_i \otimes b_i, \tag{6}$$

где $\{e_i\}$ – базис в L, а b_i – некоторые векторы из M. В частности, $x = 0$ тогда и только тогда, когда $b_i = 0$ для всех i.

Доказательство. Пусть $\{g_j\}$ – базис в M. Тогда $\{e_i \otimes g_j\}$ формирует базис в $L \otimes M$, и любой $x \in L \otimes M$ единственным образом может быть представлен в виде

$$x = \sum_{i,j} a_{ij}(e_i \otimes g_j) = \sum_i e_i \otimes \sum_j a_{ij} g_j = \sum_i e_i \otimes b_i,$$

где $b_i = \sum_j a_{ij} g_j$. Лемма 1 доказана.

Лемма 2. *Пусть L и M – два линейных пространства. Для любых подпространств $L_1, ..., L_s \subset L$ и $M_1, ..., M_s \subset M$, выполнено следующее равенство*

$$(L_1 \otimes M_1) \cap \cdots \cap (L_s \otimes M_s) = (L_1 \cap \cdots \cap L_s) \otimes (M_1 \cap \cdots \cap M_s). \tag{7}$$

Доказательство. Рассмотрим сперва случай $s = 2$. Отметим, что если $L_{12} = 0$ или $M_{12} = 0$, то $H \equiv (L_1 \otimes M_1) \cap (L_2 \otimes M_2) = 0$. Действительно, пусть, например, $L_{12} = 0$. Тогда для любых базисов $\{e_i^1\}$ в L_1 и $\{e_i^2\}$ в L_2 и для любого вектора $x \in H$ имеем

$$x = \sum_i e_i^1 \otimes b_i = \sum_j e_j^2 \otimes b'_j.$$

Учитывая линейную независимость системы векторов $\{e_i^1, e_j^2\}$, в силу Леммы 1, получим $x = 0$.

Пусть L'_i (M'_i) – произвольное прямое дополнение L_{12} (M_{12}) до L_i (M_i), $i = 1, 2$. Используя дистрибутивность тензорного произведения подпространств относительно суммы, получим

$$H = ((L_{12} \oplus L'_1) \otimes (M_{12} \oplus M'_1)) \cap ((L_{12} \oplus L'_2) \otimes (M_{12} \oplus M'_2)) =$$

$$= L_{12} \otimes M_{12} \oplus (L_{12} \otimes M'_1 \oplus L'_1 \otimes M_1) \cap L_{12} \otimes M_{12} \oplus (L_{12} \otimes M'_2 \oplus L'_2 \otimes M_2).$$

Положим $A = L_{12} \otimes M_{12}$, $B = L_{12} \otimes M'_1 \oplus L'_1 \otimes M_1$, $C = L_{12} \otimes M'_2 \oplus L'_2 \otimes M_2$. Выберем базис $\{e_i^{12}\}$ $(\{g_{i'}^{12}\})$ в L_{12} (M_{12}) и дополним его векторами $\{e_j^1\}$ $(\{g_{j'}^1\})$ до базиса в L_1 (M_1) и векторами $\{e_m^2\}$ $(\{g_{m'}^2\})$ до базиса в L_2 (M_2). Заметим, что система векторов $\{e_p \otimes g_q\}$, где

$$e_p \in \{e_i^{12}\} \cup \{e_j^1\} \cup \{e_m^2\}, \quad g_q \in \{g_{i'}^{12}\} \cup \{g_{j'}^1\} \cup \{g_{m'}^2\}$$

является линейно независимой. Далее, каждое из подпространств A, B, C имеет нулевое пересечение с сумой двух остальных, как линейные оболочки попарно непересекающихся подсистем линейно независимой системы векторов. Откуда, в частности, следует $(A \oplus B) \cap (A \oplus C) = A$. Действительно, для любого $x \in (A \oplus B) \cap (A \oplus C)$ имеем $x = a + b = a' + c$, где $a, a' \in A$, $b \in B$ и $c \in C$. Откуда $a - a' = c - b = 0$, т.е. $a = a'$, $c = b = 0$. Этим завершается доказательство леммы 2 для случая $s = 2$. Доказательство Леммы 2 завершается индукцией по s.

Лемма 3. *Для любого ацикличного семейства подпространств $L_1, ..., L_s \subset L$ линейного пространства верна формула*

$$dim(L_1 + \cdots + L_s) = \sum_{\alpha \in S} (-1)^{|\alpha|+1} dim\, L_\alpha.$$

Доказательство. При $s = 2$ утверждение Леммы 3 совпадает с классической теоремой о размерности суммы подпространств. Общий случай можно доказать индукцией по s с учетом того, что для ацикличного семейства

$$(L_1 + \cdots + L_{s-1}) \cap L_s = (L_1 \cap L_s) + \cdots + (L_{s-1} \cap L_s). \tag{8}$$

Чтобы доказать формулу (8) отметим, что очевидное включение

$$(L_1 + \cdots + L_{s-1}) \cap L_s \supset (L_1 \cap L_s) + \cdots + (L_{s-1} \cap L_s)$$

выполняется и без предположения ацикличности. Для доказательства обратного включения, выберем базис семейства $\{L_i\}$ и рассмотрим разложение произвольного вектора y, принадлежащего подпространству в левой части (8). Все базисные векторы в этом разложении принадлежат L_s в силу линейной независимости. По той же причине каждый из этих векторов принадлежит хотя бы одному из подпространств $L_1, ..., L_{s-1}$. Следовательно, вектор y принадлежит подпространству в правой части (8). Лемма 3 доказана.

Лемма 4. *Для ацикличных семейств подпространств* $\mathbf{C}$ *и* $\mathbf{D}$, *семейство* $\{C_i \otimes D_i\}$ *также ациклично.*

Доказательство. Пусть $\{e_m\}$ – базис в $\mathbf{C}$ и $\{g_j\}$ – базис в $\mathbf{D}$. Поскольку $\mathbf{C}$ и $\mathbf{D}$ ацикличны, то векторы в семействе $\{e_m \otimes g_j\}$ линейно независимы. Выберем из этого семейства подсемейство, взяв для каждого $e_m \in C_{p_m}$ лишь те произведения $e_m \otimes g_j$, для которых $g_j \in D_{p_m}$. Легко видеть, что полученное подсемейство формирует базис семейства подпространств $\{C_i \otimes D_i\}$. Поскольку построенное семейство векторов линейно независимо, то доказательство завершено.

Доказательство Теоремы 1. Применив Лемму 3 к (1) с учётом лемм 2 и 4, получим (3). Чтобы доказать (4), возьмём в коде (1) вектор веса $d_\alpha d'^\alpha$ (или $d'_\alpha d^\alpha$). Пусть $x \in C_\alpha$ – вектор минимального веса d_α, а $y \in D^\alpha$ – вектор минимального веса d'^α. Тогда $y = y_{i_1} + \cdots + y_{i_t}$, где $t = |\alpha|$ и $y_{i_j} \in D_{i_j}$, так что вектор $x \otimes y = x \otimes y_{i_1} + \cdots + x \otimes y_{i_t}$ принадлежит коду (1) и имеет вес $d_\alpha d'^\alpha$. Второй случай разбирается аналогично.

Докажем теперь (5). Для этого рассмотрим произвольный вектор $x = \sum e_i \otimes b_i$ кода $\mathbf{C} \otimes \mathbf{D}$ (см. лемму 1). Положим

$$\Psi_0 = \{\alpha : \ \alpha = \alpha_{e_i} \quad b_i \neq 0\}.$$

Рассмотрим стандартное матричное представление для вектора, принадлежащего тензорному произведению пространств, а именно, если $a = (a^1, ..., a^n)$ и $c = (c^1, ..., c^n)$ векторы из F^n и $F^{n'}$ соответственно, то координаты вектора $a \otimes c$ запишем в матрицу (a_{ij}), где $a_{ij} = a^i c^j$. Тогда любой вектор $y \in F^{nn'} = F^n \otimes F^{n'}$ можно представить матрицей, равной сумме матриц соответствующих разложимым тензорам, входящим в представление вектора y. Строки соответствующие ненулевым позициям вектора $b = \cup b_i$ в матричном представлении вектора x являются линейными комбинациями векторов e_i. С другой стороны, эти линейные комбинации принадлежат каждому из подпространств C^β, где $\beta \in \Psi_0^*$ и, следовательно, имеют вес не меньший, чем d^β для всех β (более того, этот вес не меньше чем расстояние кода $\bigcap_{\beta \in \Psi_0^*} C^\beta$).

Вес вектора b не меньше чем d'^α для любого $\alpha \in \Psi_0$, поскольку вектор $b_i \in D^\alpha$ для некоторого $\alpha \in \Psi_0$. Поскольку вес вектора x равен сумме весов ненулевых строк соответствующей матрицы, а вектор x можно представить в виде $x = \sum a_i \otimes g_i$. Поэтому, применяя предыдущие рассуждения для этого представления, завершаем доказательство неравенства (5) и теоремы 1.

§4. ПРИМЕРЫ

Примеры этого параграфа показывают, что класс фрактальных кодов содержит некоторые очень хорошие коды. Кроме того, ряд классических конструкций являются частными случаями конструкции (1). Интересно найти условия, при которых верхняя граница (4) достигается для конструкции (1).

Пример 1. Код Голея. Рассмотрим следующие пары кодов :

$$C_1=\begin{pmatrix} \cdot&\cdot&\cdot&1&1&\cdot&1&1\\ \cdot&\cdot&1&1&\cdot&1&\cdot&1\\ \cdot&1&1&\cdot&1&\cdot&\cdot&1\\ 1&1&\cdot&1&\cdot&\cdot&\cdot&1 \end{pmatrix},\quad C_2=\begin{pmatrix} 1&\cdot&1&1&\cdot&\cdot&\cdot&1\\ \cdot&1&\cdot&1&1&\cdot&\cdot&1\\ \cdot&\cdot&1&\cdot&1&1&\cdot&1\\ \cdot&\cdot&\cdot&1&\cdot&1&1&1 \end{pmatrix},$$

$$D_1=\begin{pmatrix}1&1&1\end{pmatrix},\quad D_2=\begin{pmatrix}\cdot&1&1\\1&1&\cdot\end{pmatrix},$$

где C_1, C_2 суть (8,4,4)-коды, D_1 есть (3,1,3)-код, а D_2 — (3,2,2)-код. В этом случае $\mathbf{C}\otimes\mathbf{D}$ является (24,12,8)-кодом Голея с порождающей матрицей $\mathbf{C}\otimes\mathbf{D}=$

$$\begin{pmatrix}
\cdot&\cdot&\cdot&1&1&\cdot&1&1&\cdot&\cdot&\cdot&1&1&\cdot&1&1&\cdot&\cdot&\cdot&1&1&\cdot&1&1\\
\cdot&\cdot&1&1&\cdot&1&\cdot&1&\cdot&\cdot&1&1&\cdot&1&\cdot&1&\cdot&\cdot&1&1&\cdot&1&\cdot&1\\
\cdot&1&1&\cdot&1&\cdot&\cdot&1&\cdot&1&1&\cdot&1&\cdot&\cdot&1&\cdot&1&1&\cdot&1&\cdot&\cdot&1\\
1&1&\cdot&1&\cdot&\cdot&\cdot&1&1&1&\cdot&1&\cdot&\cdot&\cdot&1&1&1&\cdot&1&\cdot&\cdot&\cdot&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&1&\cdot&\cdot&\cdot&1&1&\cdot&1&1&\cdot&\cdot&\cdot&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&1&\cdot&\cdot&1&\cdot&1&\cdot&1&1&\cdot&\cdot&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&1&\cdot&1&\cdot&\cdot&1&\cdot&1&1&\cdot&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&1&1&1&\cdot&\cdot&\cdot&1&\cdot&1&1&1\\
1&\cdot&1&1&\cdot&\cdot&\cdot&1&1&\cdot&1&1&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\
\cdot&1&\cdot&1&1&\cdot&\cdot&1&\cdot&1&\cdot&1&1&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\
\cdot&\cdot&1&\cdot&1&1&\cdot&1&\cdot&\cdot&1&\cdot&1&1&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&1&\cdot&1&1&1&\cdot&\cdot&\cdot&1&\cdot&1&1&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot
\end{pmatrix}$$

В данном примере верхняя граница (4) достигается. Вычислим также нижнюю границу (5). Имеем $\Psi(\mathbf{e})=\{1,2,12\}$ и $\Psi(\mathbf{g})=\{1,2\}$. Для соответствующих возможных значений для Ψ_0 и Ψ_0^* и для соответствующих значений внутренних максимумов в (5), имеем таблицу

$\Psi_0\subset\Psi(\mathbf{e})$	$\{1\}$	$\{2\}$	$\{12\}$	$\{1,12\}$	$\{2,12\}$	$\{1,2\}$	$\{1,2,12\}$
Ψ_0^*	$\{1\}$	$\{2\}$	$\{1,2\}$	$\{1,12\}$	$\{2,12\}$	$\{12\}$	$\{12\}$
m_1	12	8	4	12	8	6	6

$\Psi_0\subset\Psi(\mathbf{g})$	$\{1\}$	$\{2\}$	$\{1,12\}$
Ψ_0^*	$\{1\}$	$\{2\}$	$\{12\}$
m_2	12	8	4,

где
$$m_1 = (\max_{\alpha\in\Psi_0} d'^{\alpha})(\max_{\beta\in\Psi_0^*} d^{\beta}), \quad m_2 = (\max_{\alpha\in\Psi_0} d^{\alpha})(\max_{\beta\in\Psi_0^*} d'^{\beta}).$$

Отсюда следует, что нижняя граница (5) в этом примере равна $\max(4,4) = 4$.

Пример 2. (21,12,5)-код. Выбросив в кодах C_1 и C_2 примера 1 последний столбец, получим (7,4,3)-коды, имеющие один вектор веса 7 в пересечении. Оставив без изменения коды D_1 и D_2, в качестве $\mathbf{C}\otimes\mathbf{D}$ мы получим (21,12,5)-код. В этом случае граница (4) равна 6 и не достигается. Тем не менее полученный код является оптимальным. Известен лишь БЧХ-код с такими параметрами. Нижняя граница расстояния в этом коде равна $\max(3,4) = 4$.

Пример 3. (21,8,9)-код. Выбросив в коде C_2 примера 1 предпоследний столбец и последнюю строку, а в коде C_1 предпоследний столбец и первую строку, мы получим пару непересекающихся (7,3,4)-кодов. Соответствующий $\mathbf{C}\otimes\mathbf{D}$ код имеет параметры (21,9,8). Граница (4) опять достигается, и мы по прежнему имеем оптимальный код. Код с такими же параметрами можно также получить из (23,12,7)-кода Голея выбрасыванием слов нечетного веса и укорочением. Нижняя граница расстояния (5) в этом случае равна $\max(4,6) = 6$.

Пример 4. (28,22,4)-код. Возьмем в качестве C_1 (7,3,4)-код C_2 из примера 3, в качестве C_2 (7,6,2)-код всех слов чётного веса, а в качестве C_3 (7,7,1)-код всех кодовых слов на длине 7. Далее, положим D_1 – (4,4,1)-код всех слов на длине 4, D_2 – (4,3,2)-код всех слов чётного веса, а D_3 – (4,1,4)-код. Тогда $\mathbf{C}\otimes\mathbf{D}$ является (28,22,4)-кодом. Граница (4) достигается, и поэтому этот код оптимален. Отметим, что код с такими же параметрами можно получить из (31,26,3)-кода Хемминга, выбрасыванием слов нечётного веса и укорочением. Для вычисления нижней границы (5) заметим, что в этом случае $\Psi(\mathbf{e}) = \{123, 23, 3\}$ и $\Psi(\mathbf{g}) = \{1, 12, 123\}$. Поскольку ситуация симметрична относительно $\mathbf{e}$ и $\mathbf{g}$, то достаточно рассмотреть только первый случай. Имеем следующую таблицу :

$\Psi_0 \subset \Psi(\mathbf{e})$	$\{123\}$	$\{23\}$	$\{3\}$	$\{123, 23\}$	$\{123, 3\}$	$\{23, 3\}$	$\{123, 23, 3\}$
Ψ_0^*	$\{1, 2, 3\}$	$\{2, 3\}$	$\{3\}$	$\{12, 13, 2, 23, 3\}$	$\{13, 23, 3\}$	$\{23, 3\}$	$\{12, 13, 23, 3\}$
m_1	4	4	4	4	4	4	4.

Отсюда следует, что нижняя граница равна 4 и совпадает с верхней границей.

Пример 5. Конструкция $|u|u+v|$. (см [1], §2.9). Возьмём в качестве C_1 и C_2 произвольные коды. В качестве D_1 возьмем (2,1,2)-код, а в качестве D_2 (2,1,1)-код (векторы (0,0) и (0,1)). В этом случае $\mathbf{C}\otimes\mathbf{D}$ является конструкцией $|u|u+v|$.

Верхняя граница расстояния достигается и равна $\min(2d_1, d_2)$, где d_1 и d_2 – расстояния кодов C_1 и C_2, соответственно. В этом случае нижняя и верхняя границы совпадают.

Пример 6. Конструкция $|a+x|b+x|a+b+x|$. (см. [1], §18.7.4). Опять коды C_1 и C_2 произвольны, а D_1 и D_2 однозначно определённые (3,1,3)-код и (3,2,2)-код, соответственно. Тогда $\mathbf{C} \otimes \mathbf{D}$ есть конструкция $|a+x|b+x|a+b+x|$. Верхняя граница расстояния в этом случае достигается не всегда (см. предыдущие примеры). Возможность получить код Голея с помощью конструкции $|a+x|b+x|a+b+x|$ впервые указал Турин [2] (см. также [3]). В этом случае нижняя граница зависит от конфигурации семейства $\{C_i\}$.

Таким образом, как видно из предыдущих примеров, коды Голея, Хамминга, Рида-Маллера, а также многие оптимальные коды на коротких составных длинах являются фрактальными кодами. В связи с этим интересна следующая задача (см. [4]) : Выяснить при каких условиях, код на составной длине является фрактальным или эквивалентен фрактальному коду.

В заключение хотелось бы выразить свою признательность академику Г. Г. Хачатряну, благодаря которому автор познакомился с основами и проблематикой алгебраической теории кодирования.

Abstract. New linear error-correcting binary codes are obtained from two families of codes by summation of the corresponding tensor products. The basic parameters of the new codes, such as dimension and distance are studied, in particular, lower and upper bounds for code distance are obtained. Examples of optimal codes of small lengths obtained by the new construction are considered. Some classical constructions turn to be special cases of the new construction. Some unsolved problems are posed.

ЛИТЕРАТУРА

1. F. J. MacWilliams, N. J. Sloane, The Theory of Error-Correcting Codes, Bell Labor. Murray Hill, NJ 07974 USA, 1977.
2. E. F. Assmus, H. F. Mattson, R. J. Turyn, “Research to develop the algebraic theory of codes”, Report AFCRL-67-0365, Air Force Cambridge Res. Labs., Bedford, Mass, 1967.
3. R. T. Curtis, “A new combinatorial approach to M_{24}”, Math. Proc. Camb. Phil. Soc. vol. 79, pp. 25 – 41, 1976.
4. Angela I. Barbero, “An algorithm for characterizing linear bidimensional product codes”, In : Arithmetic, Geometry and Coding Theory, pp. 9 – 21, de Gruyter, Berlin, 1996.

Поступила 7 ноября 2002