ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 2006. Серия 1. Том 13, № 4. 60–88

УДК 519.72

ОБЗОР МЕТОДОВ ПОСТРОЕНИЯ НЕЛИНЕЙНЫХ СОВЕРШЕННЫХ ДВОИЧНЫХ КОДОВ*)

А. М. Романов

Теория совершенных кодов — область, которая находится на стыке теории кодирования и теории дизайнов или t-схем и является трудной для исследования. Линейные совершенные коды были построены М. Голеем и Р. Хеммингом в конце 40-х годов прошлого века. Нелинейные совершенные коды были открыты Ю. Л. Васильевым в 1961 году. В настоящее время известно достаточно много различных методов построения совершенных кодов. В статье представлен обзор методов построения нелинейных совершенных двоичных кодов и приведены некоторые открытые вопросы теории совершенных кодов.

Введение

Пусть $\mathbb{F}_2^n$ — векторное пространство размерности n над полем Галуа $GF(2)$. Произвольное подмножество $\mathbb{C} \subseteq \mathbb{F}_2^n$ называется *двоичным кодом* длины n. Векторы, принадлежащие коду, называются *кодовыми словами*. *Расстоянием Хемминга* $d(\mathbf{x}, \mathbf{y})$ между векторами $\mathbf{x} \in \mathbb{F}_2^n$ и $\mathbf{y} \in \mathbb{F}_2^n$ называется число координат, в которых векторы $\mathbf{x}$ и $\mathbf{y}$ различаются. Минимально возможное расстояние d между двумя различными кодовыми словами называется *минимальным расстоянием* кода. *Радиусом упаковки* ρ кода $\mathbb{C}$ называется величина $\rho(\mathbb{C}) = \frac{d-1}{2}$. *Радиус покрытия* кода $\mathbb{C}$ равен $r(\mathbb{C}) = \max\limits_{\mathbf{x}\in\mathbb{F}_2^n} \min\limits_{\mathbf{c}\in\mathbb{C}} d(\mathbf{x}, \mathbf{c})$. Код $\mathbb{C}$ называется *совершенным*, если $r(\mathbb{C}) = \rho(\mathbb{C})$. Совершенный код образует совершенную упаковку (также совершенное покрытие) шарами Хемминга радиуса ρ; при этом центрами этих шаров являются кодовые слова. Следовательно, множество $\mathbb{C}$ является совершенным кодом с минимальным расстоянием $d = 2\rho + 1$ тогда и только тогда, когда для каждого вектора $\mathbf{x} \in \mathbb{F}_2^n$ существует единственное кодовое слово $\mathbf{c} \in \mathbb{C}$ такое, что $d(\mathbf{x}, \mathbf{c}) \leqslant \rho$.

Коды $\mathbb{C}_1, \mathbb{C}_2 \subseteq \mathbb{F}_2^n$ называются *изоморфными*, если существует перестановка координат π такая, что $\mathbb{C}_2 = \{\pi(\mathbf{c}) \mid \mathbf{c} \in \mathbb{C}_1\}$. Коды $\mathbb{C}_1$ и $\mathbb{C}_2$

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 05–01–00364).

называются *эквивалентными*, если существует вектор $\mathbf{x} \in \mathbb{F}_2^n$ и перестановка π такие, что $\mathbb{C}_2 = \{\pi(\mathbf{c}) + \mathbf{x} \mid \mathbf{c} \in \mathbb{C}_1\}$. Код называется *линейным*, если его слова образуют линейное подпространство в $\mathbb{F}_2^n$. Линейные совершенные коды с минимальным расстоянием $d = 3$ называются *кодами Хемминга* [38]. С точностью до эквивалентности существует единственный двоичный код Хемминга длины n.

Числа n, M, d называются *параметрами кода*, если его длина равна n, мощность — M, минимальное расстояние — d. Известно, что совершенные двоичные коды с параметрами кодов Хемминга существуют только при $n = 2^s - 1, \quad s = 2, 3, \ldots$. В данной статье будут рассматриваться именно такие коды. Будем предполагать (если не оговорено обратное), что нулевой вектор всегда принадлежит коду. Все нелинейные совершенные двоичные коды имеют параметры кодов Хемминга и существуют при $n \geqslant 15$.

В [67, 68], а также независимо в [14] установлено, что кроме совершенных двоичных кодов с параметрами кодов Хемминга, двоичного кода Голея длины $n = 23$ с минимальным расстоянием 7, троичного кода Голея длины $n = 11$ с минимальным расстоянием 5 и тривиальных кодов (код из одного слова, полный код и двоичный код с повторением нёчетной длины) никакие другие совершенные коды над полями Галуа не существуют. В [61, 36] с точностью до эквивалентности доказана единственность кодов Голея.

У. Хеден [39] обнаружил, что среди совершенных кодов, построенных методом конкатенации (которая определяется перестановкой и тривиальными разбиениями $\mathbb{F}_2^n$ на совершенные коды длины n), существует совершенный код длины $n = 15$, неэквивалентный ни одному из кодов Васильева. Ф. И. Соловьёва [28] привела примеры нетривиальных разбиений $\mathbb{F}_2^n$ на совершенные коды длины n и показала, что из этих нетривиальных разбиений методом конкатенации можно построить совершенные коды, неэквивалентные кодам Васильева и кодам Хедена [39]. К. Фелпс [51] также привёл примеры нетривиальных разбиений $\mathbb{F}_2^n$ на совершенные коды. В [52] он описал конструкцию совершенных двоичных кодов, в которой конкатенация определяется m-арной квазигруппой (перестановку можно рассматривать как некоторую унарную квазигруппу). В [33] построены три совершенных кода длины $n = 15$, которые неэквивалентны кодам Васильева. М. Моллар [48] обобщил конструкцию Васильева. В. А. Зиновьев и А. Лобстейн [47, 15] предложили каскадные конструкции совершенных кодов. Вариации каскадных конструкций можно найти в более ранних работах В. А. Зиновьева, например, в [8]. У. Хеден в [40] построил совершенные коды длины $n = 15$ с ядрами размерности $1, 2, 3$ и в [41] — совершенные коды полного ранга длины $n = 31$ с ядром размерности 21.

Т. Этцион и А. Варди [43] предложили некоторые упорядоченные семейства подмножеств из $\mathbb{F}_2^n$ и назвали их совершенными сегментациями. Используя эти сегментации, они методом конкатенации построили совершенные двоичные коды и показали, что среди этих кодов содержатся новые коды длины $n = 15$. В этой же работе методом сдвига компонент кода Хемминга или свитчингами они также построили совершенные двоичные коды полного ранга с тривиальным ядром и показали, что совершенные двоичные коды полного ранга не могут быть построены конкатенацией.

Свитчинги в совершенных двоичных кодах были открыты Ю. Л. Васильевым [5, 6] и для q-ичных кодов обобщены в работах [64, 59, 27, 58, 18]. Свитчинговые методы широко известны в комбинаторике. Так, например, в системах Штейнера известны свитчинги Паша (Pash). Существует всего 80 попарно неизоморфных систем троек Штейнера порядка 15, все они занумерованы некоторым фиксированным образом [69] (таблица, в которой перечисляются системы троек Штейнера, также содержится в более доступной работе [46]). Как установлено в [37], эти 80 систем троек Штейнера разбиваются на два свитчинговых класса. Один класс содержит системы от № 1 до № 79. Другой класс состоит из одной системы № 80. Что касается числа свитчинговых классов, на которые разбивается множество совершенных двоичных кодов длины n, в настоящее время наиболее изученным является свитчинговый класс кода Хемминга. Кроме того, в [57] приведён пример двух совершенных кодов длины $n = 15$, которые не принадлежат свитчинговому классу кода Хемминга и образуют собственный свитчинговый класс, состоящий из двух кодов. На самом деле, по-видимому, множество совершенных двоичных кодов дины $n = 15$ разбивается на несколько тысяч свитчинговых классов.

Следует заметить, что в [49] недавно решена известная проблема о пополнении характеристических векторов, соответствующих системам троек Штейнера, до совершенных кодов. В ней показано, что характеристические векторы, соответствующие системам троек Штейнера № 79 и № 80, не могут принадлежать ни одному совершенному коду длины $n = 15$.

К. Фелпс и М. Ли Ван [55] заметили, что подмножества кода Хемминга, которые сдвигали Т. Этцион и А. Варди [43] и которые мы называем компонентами, являются смежными классами некоторых подпространств. Используя групповые свойства компонент кода Хемминга, они неконструктивными методами доказали существование в коде Хемминга непересекающихся компонент, отвечающих различным координатам, и тем самым доказали существование совершенных двоичных кодов со всеми допустимыми размерностями ядер. С. В. Августинович и Ф. И. Соловьёва [1] обратили внимание на то, что если в коде Хемминга сдвинуть n непересекающихся компонент по n различным направлениям, то код Хемминга превратится в несистематический код. С. А. Малюгин [20] показал, что для превращения кода Хемминга в несистематический код в нём достаточно сдвинуть 7 компонент. В [24] получены достаточные условия непересекаемости компонент кода Хемминга и построены регулярные разбиения кода Хемминга на компоненты. С использованием этих условий в [25] построены несистематические коды длины $n = 15$, а в [26] — семейство непересекающихся компонент, которое даёт коды полного ранга с тривиальным ядром. В [23] получен критерий непересекаемости компонент двоичного кода Хемминга и построены регулярные разбиения кодов Хемминга на компоненты с новыми параметрами. В [44] построены совершенные двоичные коды полного ранга с большими размерностями ядер исходя из мозаичных замощений $\mathbb{F}_2^n$.

Пусть $N(n)$ — число попарно неэквивалентных совершенных двоичных кодов длины n. Тогда $2^{2^{(0,5+o(1))n}} \leqslant N(n) \leqslant 2^{2^{(1+o(1))n}}$. Нижняя оценка получена Ю. Л. Васильевым [5] и неоднократно передоказана многими авторами. Верхняя оценка является тривиальной. Далее говоря о числе неэквивалентных кодов, мы будем иметь ввиду попарную неэквивалентность.

В настоящее время неизвестно даже число неэквивалентных совершенных двоичных кодов длины $n = 15$. Известные оценки числа неэквивалентных совершенных двоичных кодов длины $n = 15$ и числа неэквивалентных расширенных совершенных двоичных кодов длины $n = 16$ приведены в таблице 1.

Таблица 1

	$n = 15$	$n = 15$	$n = 16$	$n = 16$
Ранг 11	1	1	1	1
Ранг 12	18	18	12	12
Ранг 13	758	758	272	272
Ранг 14	?	?	1719	?
Ранг 15	?	51	?	51

Во второй колонке таблицы 1 перечислены неэквивалентные совершенные двоичные коды длины $n = 15$ и ранга 11, 12, 13. Число неэквивалентных совершенных двоичных кодов ранга 14 и 15 неизвестно. Кроме того, в настоящее время не известны никакие теоретические методы, с помощью которых можно было бы построить коды полного ранга длины $n = 15$, не принадлежащие свитчинговому классу кода Хемминга. В третьей колонке таблицы 1 перечислены неэквивалентные совершенные двоичные коды, принадлежащие свитчинговому классу кода Хемминга длины $n = 15$. В четвёртой и пятой колонках соответственно перечислены неэквивалентные расширенные совершенные двоичные коды длины $n = 16$ и неэквивалентные расширенные совершенные двоичные коды, принадлежащие свитчинговому классу расширенного кода Хемминга длины $n = 16$. Приведённые оценки заимствованы из работ [42, 11–13, 21, 22]. В работе [22] приводится нижняя оценка числа неэквивалентных кодов полного ранга, которая по утверждению С. А. Малюгина является точной. Как видно из таблицы 1 число неэквивалентных расширенных совершенных двоичных кодов ранга 14 равно 1719. Все такие коды строятся методом конкатенации; из них 844 кода — исходя из разбиений, 875 кода — исходя из совершенных сегментаций и обобщений [13]. Ранг кода Хемминга длины n равен $n - s$. Можно показать, что все совершенные коды длины n и ранга $n - s + 1$, $n - s + 2$ принадлежат свитчинговому классу кода Хемминга длины n. Вполне вероятно, что в ближайшее время все совершенные двоичные коды длины $n = 15$ будут перечислены при помощи компьютера.

Обзоры работ по совершенным кодам представлены в работах [34, 54, 66].

1. Определения и обозначения

Вес вектора $\mathbf{x} \in \mathbb{F}_2^n$ равен числу единичных координат в $\mathbf{x}$. Через $\mathbb{E}_0^n$ обозначим множество векторов из $\mathbb{F}_2^n$ с чётным весом, а через $\mathbb{E}_1^n$ — с нечётным весом. Через $p(\mathbf{x})$ обозначим *функцию чётности*, т. е.

$$p(\mathbf{x}) = p(x_1, x_2, \dots, x_n) = x_1 + x_2 + \dots + x_n \pmod 2,$$

где $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$. Пусть $\mathbb{C}$ — двоичный код длины n. Тогда множество

$$\mathbb{C}^* = \{(\mathbf{c}|p(\mathbf{c})) \mid \mathbf{c} \in \mathbb{C}\} \in \mathbb{F}_2^{n+1}$$

называется *расширенным кодом* (вертикальная черта $(\cdot|\cdot)$ обозначает конкатенацию). Говорят, что расширенный код $\mathbb{C}^*$ получается из кода $\mathbb{C}$ добавлением проверки на чётность. Если $\mathbb{C}$ — совершенный код, то $\mathbb{C}^*$ называется *расширенным совершенным кодом*.

Размерность $r = r(\mathbb{C})$ линейной оболочки кода $\mathbb{C}$ называется его *рангом*. Код $\mathbb{C}$ называется кодом *полного ранга*, если $r(\mathbb{C}) = n$. *Ядром* кода $\mathbb{C}$ называется подмножество векторов $\ker(\mathbb{C}) \subseteq \mathbb{F}_2^n$ такое, что для любого вектора $\mathbf{x} \in \ker(\mathbb{C})$ справедливо соотношение $\mathbf{x} + \mathbb{C} = \mathbb{C}$ (символ $+$ обозначает сложение по модулю 2). Если нулевой вектор принадлежит коду, то $\ker(\mathbb{C}) \subseteq \mathbb{C}$. Множество $\ker(\mathbb{C})$ является линейным подкодом кода $\mathbb{C}$ и $\ker(\mathbb{C}) = \mathbb{C}$ тогда и только тогда, когда код $\mathbb{C}$ является линейным.

Через $\mathbf{e}_i$ обозначим вектор, в котором i-я координата равна 1, а остальные координаты равны 0. Подмножество $K \subseteq \mathbb{C}$ совершенного кода $\mathbb{C}$ длины n называется *i-компонентой* этого кода, если множество

$$(\mathbb{C} \setminus K) \cup (K + \mathbf{e}_i)$$

является совершенным кодом длины n и для любого собственного подмножества $K' \subset K$ множество $(\mathbb{C} \setminus K') \cup (K' + \mathbf{e}_i)$ не является совершенным кодом длины n. Для каждой координаты i совершенный код единственным образом разбивается на i-компоненты и i-компоненты кода являются его инвариантами. *Сдвигом* множества $K \subseteq \mathbb{F}_2^n$ называется множество $K + \mathbf{x}$, где $\mathbf{x} \in \mathbb{F}_2^n$. *Сдвигом по координате* i-компоненты K кода называется множество $K + \mathbf{e}_i$.

Совершенный код $\mathbb{C}'$ получается из совершенного кода $\mathbb{C}$ *свитчингом* или сдвигом по координате i-компоненты K кода $\mathbb{C}$, если

$$\mathbb{C}' = (\mathbb{C} \setminus K) \cup (K + \mathbf{e}_i).$$

Совершенный код $\mathbb{C}'$ получается из совершенного кода $\mathbb{C}$ последовательностью свитчингов, если существует последовательность совершенных кодов $\mathbb{C} = \mathbb{C}_0, \mathbb{C}_1, \ldots, \mathbb{C}_m$ такая, что код $\mathbb{C}_r$ получается из кода $\mathbb{C}_{r-1}$ ($r \in \{1, 2, \ldots, m\}$) свитчингом i-компоненты кода $\mathbb{C}_{r-1}$ ($i \in \{1, 2, \ldots, n\}$). *Свитчинговым классом* совершенного кода $\mathbb{C}$ называется совокупность всех совершенных кодов, которые получаются из $\mathbb{C}$ последовательностью свитчингов.

2. Конкатенация

Сначала опишем **uv**-конструкцию (её также называют конструкцией Плоткина), которая чрезвычайно проста и неоднократно переоткрыта многими авторами. Пусть $\mathbb{D}$, $\mathbb{C}^0$ — коды дины n с минимальными кодовыми расстояниями d_1, d_0.

Теорема 1. *Множество*

$$\mathbb{C} = \{(\mathbf{u}|\mathbf{u} + \mathbf{v}) \mid \mathbf{u} \in \mathbb{D}, \mathbf{v} \in \mathbb{C}^0\} \tag{1}$$

является кодом длины $2n$, *мощности* $|\mathbb{D}| \cdot |\mathbb{C}^0|$, *с минимальным кодовым расстоянием* $d = \min\{2d_1, d_0\}$.

Пусть $\mathbb{D} = \mathbb{E}_0^{n+1}$, $\mathbb{C}^0$ — расширенный совершенный код длины $n+1$. Тогда код $\mathbb{C}$ является расширенным совершенным кодом длины $2n+2$.

Пусть $\mathbb{C}^0 = \mathbb{C}_0^0, \mathbb{C}_1^0, \ldots, \mathbb{C}_n^0$ — разбиение множества $\mathbb{E}_0^{n+1}$, образованное сдвигами расширенного совершенного кода $\mathbb{C}^0$ (такие разбиения называются *тривиальными*), и π — тождественная перестановка, действующая на множестве $\{0, 1, \ldots, n\}$. Тогда **uv**-конструкцию (1) расширенного совершенного кода $\mathbb{C}$ можно записать в следующем виде

$$\mathbb{C} = \{(\mathbf{u}_i|\mathbf{v}_j) \mid \mathbf{u}_i \in \mathbb{C}_i^0, \mathbf{v}_j \in \mathbb{C}_j^0, j = \pi(i), i = 0, 1, \ldots, n\}.$$

Некоторое обобщение **uv**-конструкции называется методом конкатенации (doubling construction). В случае произвольных кодов эта конструкция в монографии [19] названа симметричной X4-конструкцией. Совершенные коды строятся методом конкатенации, исходя из разбиений или из совершенных сегментаций, которые были введены Т. Этционом и А. Варди. Заметим, что разбиения являются частным случаем совершенных сегментаций.

2.1. Разбиения

Пусть $\mathbb{C}_0^0, \mathbb{C}_1^0, \ldots, \mathbb{C}_n^0$ и $\mathbb{C}_0^1, \mathbb{C}_1^1, \ldots, \mathbb{C}_n^1$ — два возможно различных разбиения множества $\mathbb{E}_0^{n+1}$ на расширенные совершенные коды длины $n+1$ и π — произвольная перестановка, действующая на множестве $\{0, 1, \ldots, n\}$.

Теорема 2 [28, 51, 39]. *Множество*

$$\mathbb{C} = \{(\mathbf{u}_i|\mathbf{v}_j) \mid \mathbf{u}_i \in \mathbb{C}_i^0, \mathbf{v}_j \in \mathbb{C}_j^1, j = \pi(i), i = 0, 1, \ldots, n\}$$

является расширенным совершенным двоичным кодом длины $2(n+1) = 2n+2$.

При построении кодов У. Хеден [39] использовал смешанные коды, но принято считать, что коды Хедена строятся методом конкатенации из тривиальных разбиений. Ф. И. Соловьёва [28] построила нетривиальные разбиения двумя способами: в первом случае она использовала конструкцию Васильева, во втором — метод конкатенации. К. Фелпс [51] нашел 6 неэквивалентных разбиений $\mathbb{F}_2^7$ на коды Хемминга длины $n=7$ и указал на возможность построения нетривиальных разбиений с использованием компонент совершенных кодов.

В [53] К. Фелпс перечислил все неэквивалентные разбиения $\mathbb{F}_2^7$ на коды Хемминга длины $n=7$ и все неэквивалентные разбиения $\mathbb{E}_0^8$ на расширенные коды Хемминга длины $n=8$. Число неэквивалентных разбиений $\mathbb{F}_2^7$ оказалось равным 11, а число неэквивалентных разбиений $\mathbb{E}_0^8$

— равным 10. В [53] он также перечислил все неэквивалентные расширенные совершенные коды длины $n = 16$, которые получаются методом конкатенации из разбиений $\mathbb{E}_0^8$. Общее число таких кодов равно 963. Приведём таблицу 2 из [53], в которой неэквивалентные расширенные совершенные двоичные коды длины $n = 16$, построенные методом конкатенации, классифицированы в соответствии с их рангом и размерностью ядра.

Т а б л и ц а 2

Размерность ядра	11	9	8	7	6	5	4	3	2
Ранг 11	1								
Ранг 12		2	2	3					
Ранг 13			7	11	38	34	20		
Ранг 14			1	4	48	210	374	172	36

Нетривиальные разбиения предложены также в [32, 62]. В [63] показано, что любой совершенный код может принадлежать некоторому нетривиальному разбиению $\mathbb{F}_2^n$ на совершенные коды длины n.

2.2. Совершенные сегментации

Прежде чем описывать метод построения совершенных кодов, основанный на совершенных сегментациях, приведём необходимые и достаточные условия, полученные Т. Этционом и А. Варди, из которых, в частности, следует, что совершенные двоичные коды полного ранга не могут быть построены конкатенацией.

Пусть $\mathbb{C}$ — совершенный двоичный код длины n такой, что существует вектор $\mathbf{w} \in \mathbb{C}^\perp$ ($\mathbb{C}^\perp$ — дуальный код) веса $t + 1 = 2^{s-1}$. Без ограничения общности будем считать, что ненулевые элементы находятся в первых $t + 1$ позициях вектора $\mathbf{w}$. Таким образом, для каждого вектора $(\mathbf{u}|\mathbf{v}) \in \mathbb{C}$ такого, что $\mathbf{v} \in \mathbb{F}_2^t$, вектор $\mathbf{u}$ имеет чётный вес. Пусть

$$T(\mathbf{u}) = \{\mathbf{v} \in \mathbb{F}_2^t \mid (\mathbf{u}|\mathbf{v}) \in \mathbb{C}\}, \quad H(\mathbf{v}) = \{\mathbf{u} \in \mathbb{E}_0^{t+1} \mid (\mathbf{u}|\mathbf{v}) \in \mathbb{C}\}.$$

Теорема 3 [43]. *Код $\mathbb{C}$ является совершенным тогда и только тогда, когда выполняются следующие два условия*:

1. *Если* $\mathbf{u} \in \mathbb{E}_0^{t+1}$, *то* $T(\mathbf{u})$ *— совершенный код длины* t.

2. *Если* $\mathbf{v} \in \mathbb{F}_2^t$, *то* $H(\mathbf{v})$ *— расширенный совершенный код длины* $t + 1$.

Доказательство. Сначала докажем достаточность условий. Пусть $\mathbf{c}_1 = (\mathbf{x}_1|\mathbf{y}_1)$ и $\mathbf{c}_2 = (\mathbf{x}_2|\mathbf{y}_2)$ — два различных кодовых слова из $\mathbb{C}$,

$\mathbf{x}_1$, $\mathbf{x}_2 \in \mathbb{E}_2^{t+1}$ и $\mathbf{y}_1, \mathbf{y}_2 \in \mathbb{F}_2^t$. Если $\mathbf{x}_1 = \mathbf{x}_2$, то $\mathbf{y}_1, \mathbf{y}_2 \in T(\mathbf{x}_1)$ и, следовательно, $d(\mathbf{c}_1, \mathbf{c}_2) \geqslant 3$. Аналогично, если $\mathbf{y}_1 = \mathbf{y}_2$, то $\mathbf{x}_1, \mathbf{x}_2 \in H(\mathbf{y}_1)$ и $d(\mathbf{c}_1, \mathbf{c}_2) \geqslant 4$. Теперь если $\mathbf{x}_1 \neq \mathbf{x}_2$ и $\mathbf{y}_1 \neq \mathbf{y}_2$, то $d(\mathbf{c}_1, \mathbf{c}_2) = d(\mathbf{x}_1, \mathbf{x}_2) + d(\mathbf{y}_1, \mathbf{y}_2) \geqslant 3$. Далее оценим мощность множества $\mathbb{C}$.

$$|\mathbb{C}| = \sum_{\mathbf{u} \in \mathbb{E}_2^{t+1}} |T(\mathbf{u})| = 2^t \cdot 2^{t-(s-1)} = 2^{n-s}.$$

Следовательно, множество $\mathbb{C}$ является совершенным кодом.

Теперь докажем необходимость. Очевидно, что

$$d(T(\mathbf{u})) = \min_{\mathbf{v}_1, \mathbf{v}_2 \in T(\mathbf{u})} d(\mathbf{v}_1, \mathbf{v}_2) \geqslant 3.$$

В силу соотношений, следующих из границы сферической упаковки, имеем $|T(\mathbf{u})| \leqslant 2^{t-(s-1)}$. Если $|T(\mathbf{u}^*)| < 2^{t-(s-1)}$ для некоторого $\mathbf{u}^*$, то

$$|\mathbb{C}| = \sum_{\mathbf{u} \in \mathbb{E}_2^{t+1}} |T(\mathbf{u})| \leqslant (2^t - 1) \cdot 2^{t-(s-1)} + |T(\mathbf{u}^*)| < 2^{n-s}.$$

Это противоречит тому, что код $\mathbb{C}$ является совершенным. Таким образом, $|T(\mathbf{u})| = 2^{t-(s-1)}$ и $T(\mathbf{u})$ является совершенным кодом. Аналогично доказывается, что $H(\mathbf{v})$ является расширенным совершенным кодом. Теорема 3 доказана.

Пусть $\mathbb{V} \subseteq \mathbb{F}_2^n$, а $\mathcal{A} = \{A_1, A_2, \dots, A_k\}$ и $\mathcal{B} = \{B_1, B_2, \dots, B_k\}$ — упорядоченные семейства подмножеств множества $\mathbb{V}$. Пусть $\mathbf{v} \in \mathbb{V}$. Тогда

$$\Lambda_A(\mathbf{v}) = \{i \mid \mathbf{v} \in A_i\}, \quad \Lambda_B(\mathbf{v}) = \{i \mid \mathbf{v} \in B_i\},$$

где $A_i \in \mathcal{A}$, $B_i \in \mathcal{B}$, $i = 1, 2, \dots, k$. Будем говорить, что семейства $\mathcal{A}, \mathcal{B}$ образуют *совершенную сегментацию* порядка k множества $\mathbb{V}$, если множества

$$\bigcup_{i \in \Lambda_B(\mathbf{v})} A_i \quad \text{и} \quad \bigcup_{i \in \Lambda_A(\mathbf{v})} B_i$$

являются совершенными кодами длины n для всех $\mathbf{v} \in \mathbb{V}$.

Очевидно, что разбиение $\mathbb{F}_2^n$ на совершенные коды длины n является совершенной сегментацией пространства $\mathbb{F}_2^n$ порядка $n+1$ и имеет наименьший порядок среди всех совершенных сегментаций. Приведём пример совершенной сегментации пространства $\mathbb{F}_2^n$ более высокого порядка [43].

Пусть $\mathbb{C}_1$ и $\mathbb{C}_2$ — два изоморфных кода Хемминга длины $n = 2^s - 1$ и $\mathbb{C}' = \mathbb{C}_1 \cap \mathbb{C}_2$ имеет мощность 2^{n-s-1}. Тогда $\mathbb{C}_1 = \mathbb{C}' \cup (\mathbf{c}_1 + \mathbb{C}')$ и $\mathbb{C}_2 = \mathbb{C}' \cup (\mathbf{c}_2 + \mathbb{C}')$ для некоторых $\mathbf{c}_1 \in \mathbb{C}_1 \setminus \mathbb{C}'$ и $\mathbf{c}_2 \in \mathbb{C}_2 \setminus \mathbb{C}'$. Положим

$A_1 = \mathbb{C}'$, $A_2 = \mathbf{c}_1 + \mathbb{C}'$, $A_3 = \mathbf{c}_2 + \mathbb{C}'$, $A_4 = \mathbf{c}_1 + \mathbf{c}_2 + \mathbb{C}'$,
$B_1 = \mathbb{C}_1$, $B_2 = \mathbb{C}_2$, $B_3 = \mathbf{c}_1 + \mathbb{C}_2$, $B_4 = \mathbf{c}_2 + \mathbb{C}_1$.

Несложно убедиться в том, что $\{A_1, A_2, A_3, A_4\}$ и $\{B_1, B_2, B_3, B_4\}$ образуют совершенную сегментацию множества $\mathbb{V} = \mathbb{C}_1 \cup (\mathbf{c}_2 + \mathbb{C}_1)$. Кроме того, любые два разбиения $A_5, A_6, \ldots, A_{n+3}$ и $B_5, B_6, \ldots, B_{n+3}$ множества $\mathbb{F}_2^n \backslash \mathbb{V}$ на совершенные коды дополняют $\{A_1, A_2, A_3, A_4\}$ и $\{B_1, B_2, B_3, B_4\}$ до совершенной сегментации пространства $\mathbb{F}_2^n$.

Теорема 4 [43]. *Пусть семейства $\mathcal{A}$ и $\mathcal{B}$ образуют совершенную сегментацию множества $\mathbb{F}_2^n$. Тогда множество*

$$\mathbb{C} = \{(\mathbf{u}|\mathbf{v}) \mid \mathbf{u} \in A_i^*, \mathbf{v} \in B_i, i = 1, 2, \ldots, k\}$$

является совершенным двоичным кодом длины $2n+1$ (символ $*$ обозначает расширение кода добавлением проверки на чётность).

Доказательство. Пусть множества $T(\mathbf{u})$ и $H(\mathbf{v})$ определены очевидным образом по первым $n+1$ координатам кода $\mathbb{C}$. Ясно, что множеством всех элементов из $\mathcal{B}$, которые содержат заданный вектор $\mathbf{v} \in \mathbb{F}_2^n$, является $\Lambda_{B(\mathbf{v})}$. Следовательно, $H(\mathbf{v}) = \bigcup\limits_{i \in \Lambda_{B(\mathbf{v})}} A_i^* = (\bigcup\limits_{i \in \Lambda_{B(\mathbf{v})}} A_i)^*$. Аналогично, $T(\mathbf{u}) = \bigcup\limits_{i \in \Lambda_{A(\mathbf{u})}} B_i$. Таким образом, код $\mathbb{C}$ является совершенным в силу теоремы 3. Теорема 4 доказана.

3. Конструкция Фелпса

К. Фелпс обобщил конкатенативную конструкцию, которая удваивала длину кода, и вместо перестановок предложил использовать квазигруппы; при этом длина кода стала увеличиваться многократно. Пусть $\mathbb{C}_0^0, \mathbb{C}_1^0, \ldots, \mathbb{C}_n^0$ и $\mathbb{C}_0^1, \mathbb{C}_1^1, \ldots, \mathbb{C}_n^1$ — разбиения соответственно множеств $\mathbb{E}_0^{n+1}$ и $\mathbb{E}_1^{n+1}$ на расширенные совершенные коды длины $n+1 = 2^{s_1}$. Пусть $\mathbb{R}$ — расширенный совершенный код длины $m+1 = 2^{s_2}$. Для каждого кодового слова $\mathbf{r} \in \mathbb{R}$ определим m-арную квазигруппу $q_{\mathbf{r}}(a_0, a_1, \ldots, a_{m-1}) = a_m$ порядка $n+1$.

Теорема 5 [52]. *Множество*

$$\mathbb{C} = \{(\mathbf{c}_0|\mathbf{c}_1|\cdots|\mathbf{c}_m) \mid \mathbf{c}_i \in \mathbb{C}_{j_i}^{r_i},\ \mathbf{r} = (r_0, \ldots, r_m) \in \mathbb{R},\ q_{\mathbf{r}}(j_0, \ldots, j_{m-1}) = j_m\}$$

является расширенным совершенным двоичным кодом длины $2^{s_1+s_2}$.

Доказательство. Мощность $|\mathbb{C}_{j_i}^{r_i}| = 2^{n-s_1}$ и $|\mathbb{R}| = 2^{m-s_2}$. Для каждого $\mathbf{r} \in \mathbb{R}$ можно построить

$$|\mathbb{C}_{j_i}^{r_i}|^{m+1}(n+1)^m = (2^{n-s_1})^{m+1}(2^{s_1})^m = 2^{nm-s_1+n}$$

кодовых слов. В результате получим

$$2^{nm-s_1+n}2^{m-s_2} = 2^{2^{s_1+s_2}-(s_1+s_2)}$$

кодовых слов, которые принадлежат коду $\mathbb{C}$. Следовательно, остаётся показать, что $d(\mathbf{x},\mathbf{y}) \geqslant 4$ для любых различных $\mathbf{x},\mathbf{y} \in \mathbb{C}$.

Пусть векторы $\mathbf{x} = (\mathbf{x}_0|\mathbf{x}_1|\cdots|\mathbf{x}_m)$ и $\mathbf{y} = (\mathbf{y}_0|\mathbf{y}_1|\cdots|\mathbf{y}_m)$ принадлежат коду $\mathbb{C}$. Тогда

$$d(\mathbf{x},\mathbf{y}) \geqslant \sum_{i=0}^{m} d(\mathbf{x}_i,\mathbf{y}_i),$$

где $\mathbf{x}_i,\mathbf{y}_i$ — векторы длины $n+1$. Пусть $r_i = p(\mathbf{x}_i)$ и $r'_i = p(\mathbf{y}_i)$, $i = 0,1,\ldots,m$. Тогда векторы $\mathbf{r} = (r_0,r_1,\ldots,r_m)$ и $\mathbf{r}' = (r'_0,r'_1,\ldots,r'_m)$ принадлежат коду $\mathbb{R}$. Если $d(\mathbf{x}_i,\mathbf{y}_i) = 0$, то $r_i = r'_i$. Если $r_i \neq r'_i$, то $d(\mathbf{x}_i,\mathbf{y}_i) \geqslant 1$. Следовательно, если $d(\mathbf{r},\mathbf{r}') \geqslant 4$, то $d(\mathbf{x}_i,\mathbf{y}_i) \geqslant 1$ для четырёх значений i. Таким образом,

$$\sum_{i=0}^{m} d(\mathbf{x}_i,\mathbf{y}_i) \geqslant 4 \text{ при } \mathbf{r} \neq \mathbf{r}'.$$

Если $\mathbf{r} = \mathbf{r}'$, то чётность векторов $\mathbf{x}_i$ и $\mathbf{y}_i$ одинакова и $d(\mathbf{x}_i,\mathbf{y}_i) \geqslant 2$ при $\mathbf{x}_i \neq \mathbf{y}_i$. Допустим, что $\mathbf{x}_i \in \mathbb{C}^{r_i}_{j_i}$ и $\mathbf{y}_i \in \mathbb{C}^{r_i}_{k_i}$, где $i = 0,1,\ldots,m$. Тогда равенство $d(\mathbf{x}_i,\mathbf{y}_i) = 0$ означает, что $j_i = k_i$; так как $\mathbf{j} = (j_0,j_1,\ldots,j_m)$ и $\mathbf{k} = (k_0,k_1,\ldots,k_m)$ могут совпадать только в $m-1$ позициях, то $d(\mathbf{x}_i,\mathbf{y}_i) \geqslant 2$ по крайней мере для двух значений i. Следовательно, $d(\mathbf{x},\mathbf{y}) \geqslant 4$ за исключением случая, когда $\mathbf{j} = \mathbf{k}$. Однако в этом случае если $\mathbf{x}_i \neq \mathbf{y}_i$, то $d(\mathbf{x}_i,\mathbf{y}_i) \geqslant 4$ и $d(\mathbf{x},\mathbf{y}) \geqslant 4$. Теорема 5 доказана.

В конструкции Фелпса квазигруппу можно заменить на МДР код (код с максимально допустимым расстоянием) или на латинский куб. Заметим, что m-арной квазигруппе $q_{\mathbf{r}}(a_0,a_1,\ldots,a_{m-1}) = a_m$ порядка $n+1$ соответствует $(n+1)$-ичный МДР код длины $m+1$, мощности $(n+1)^m$, с минимальным кодовым расстоянием 2, или m-мерный латинский куб порядка $n+1$.

4. Обобщённая каскадная конструкция

Каскадные конструкции широко известны в теории самокорректирующихся кодов [30, 9]. Основная идея каскадных конструкций заключается в том, что q_A-ичные коды (т. е. коды, определённые над алфавитом $\{0,1,\ldots,q_A-1\}$) при помощи морфизма переводятся в q_B-ичные коды.

Обобщённую каскадную конструкцию совершенных двоичных кодов представим так, как это сделано в [15].

Пусть $\mathbb{A}$ — q_A-ичный код с параметрами (n_A, K_A, d_A), $\mathbb{B}$ — q_B-ичный код с параметрами $(n_B, K_B = q_A, d_B)$. Перенумеруем кодовые слова кода $\mathbb{B}$ (тем самым, каждой букве алфавита $\{0, 1, \ldots, q_A - 1\}$ поставим в соответствие некоторое кодовое слово из $\mathbb{B}$), т. е. $\mathbb{B} = \{\mathbf{b}(0), \ldots, \mathbf{b}(q_A - 1)\}$. Для каждого вектора $\mathbf{a} = (a_1, \ldots, a_{n_A}) \in \mathbb{A}$ пусть $\mathbf{a}(\mathbb{B}) = (\mathbf{b}(a_1)| \cdots | \mathbf{b}(a_{n_A}))$, где вертикальная черта обозначает конкатенацию. В этих обозначениях множество $\mathbb{C} = \{\mathbf{a}(\mathbb{B}) \mid \mathbf{a} \in \mathbb{A}\}$ представляет собой q_B-ичный код с параметрами $n_C = n_A n_B, K_C = K_A, d_C \geqslant d_A d_B$. Коды $\mathbb{A}$, $\mathbb{B}$ и $\mathbb{C}$ называются соответственно *внешним*, *внутренним* и *каскадным* кодами. Далее, для удобства будем использовать обозначение $d_{B,1} = d_B$. Предположим, что $\mathbb{B} = \bigcup\limits_{i=0}^{q_1-1} \mathbb{B}_i$, где $\mathbb{B}_i$ — различные q_B-ичные $(n_B, K_1, d_{B,2})$-коды. Ясно, что $K_B = q_1 K_1$. , Кроме того, предположим, что $\mathbb{B}_i = \bigcup\limits_{j=0}^{q_2-1} \mathbb{B}_{i,j}$ при каждом $i = 0, 1, \ldots, q_1 - 1$, где $\mathbb{B}_{i,j}$ — различные q_B-ичные $(n_B, K_2,\ d_{B,3})$-коды, причём $K_1 = q_2 K_2$. Пусть $q_3 = K_2$. Код $\mathbb{B}$ полностью разбивается на подкоды $\mathbb{B}_{i,j}$. Поэтому любое кодовое слово $\mathbf{b}$ из $\mathbb{B}$ принадлежит ровно одному подкоду $\mathbb{B}_{i,j}$. Если $\mathbf{b}$ имеет, скажем, номер k в $\mathbb{B}_{i,j}$, то легко убедиться, что множество троек

$$(i, j, k) \in \{0, \ldots, q_1 - 1\} \times \{0, \ldots, q_2 - 1\} \times \{0, \ldots, q_3 - 1\}$$

взаимно однозначно соответствует множеству кодовых векторов $\mathbf{b}$; иначе говоря, $\mathbf{b} = \mathbf{b}(i, j, k)$.

При $l = 1, 2, 3$ рассмотрим q_l-ичный $(n_A, K_{A,l}, d_{A,l})$-код $\mathbb{A}_l$ и кодовое слово $\mathbf{a}^{(l)} = (a_1^{(l)}, \ldots, a_{n_A}^{(l)}) \in \mathbb{A}_l$. При каждом $s = 1, \ldots, n_A$ тройка чисел $(a_s^{(1)}, a_s^{(2)}, a_s^{(3)})$ задаёт кодовое слово $\mathbf{b} = \mathbf{b}(a_s^{(1)}, a_s^{(2)}, a_s^{(3)}) \in \mathbb{B}$. Пусть

$$\mathbb{C} = \Big\{ \Big(\mathbf{b}(a_1^{(1)}, a_1^{(2)}, a_1^{(3)}) \mid \cdots \mid \mathbf{b}(a_{n_A}^{(1)}, a_{n_A}^{(2)}, a_{n_A}^{(3)}) \Big) \ \mid\ \mathbf{a}^{(l)} \in \mathbb{A}_l,\ 1 \leqslant l \leqslant 3 \Big\}.$$

Теорема 6 [9]. *Множество $\mathbb{C}$ является q_B-ичным кодом с параметрами $n_C = n_A n_B,\ K_C = \prod\limits_{i=1}^{3} K_{A,i},\ d_C \geqslant \min\limits_{1 \leqslant i \leqslant 3} \{d_{A,i} d_{B,i}\}$.*

Конструкция, описанная в теореме 6, называется *обобщённой каскадной* конструкцией q_B-ичного кода.

Пусть $n_A = 2^u \geqslant 4$ и $n_B = 2^m \geqslant 4$. Пусть $\mathbb{B} = \mathbb{F}_2^{n_B}$, т. е. $\mathbb{B}$ — двоичный безызбыточный $(n_B, 2^{n_B}, 1)$-код. Рассмотрим разбиение кода $\mathbb{B}$ на множества B_0 и B_1, соответственно состоящие из всех чётных и из всех нечётных векторов. Множества B_0 и B_1 являются $(n_B, 2^{n_B - 1}, 2)$-кодами.

Рассмотрим разбиение множества $\mathbb{B}_i$, $i = 0, 1$, на 2^m расширенных совершенных кодов $\mathbb{B}_{i,j}$ мощности 2^{n_B-1-m} с минимальным расстоянием 4. Таким образом, получаем $q_1 = 2$, $q_2 = n_B$, $q_3 = 2^{n_B-1-m}$ и $d_{B,1} = 1$, $d_{B,2} = 2$, $d_{B,3} = 4$.

Наконец, в качестве внешних кодов $\mathbb{A}_1$, $\mathbb{A}_2$ и $\mathbb{A}_3$ выберем следующие коды:

$\mathbb{A}_1$ — двоичный $(n_A, 2^{n_A-1-u}, 4)$-код;

$\mathbb{A}_2$ — n_B-ичный $(n_A, n_B^{n_A-1}, 2)$-код ($\mathbb{A}_2$ — любой МДР код с $n_B^{n_A-1}$ кодовыми словами и с минимальным расстоянием 2);

$\mathbb{A}_3$ — q_3-ичный $(n_A, q_3^{n_A}, 1)$-код (т. е. $\mathbb{A}_3 = \mathbb{F}_{q_3}^{n_A}$), где $q_3 = 2^{n_B-1-m}$.

Результирующий двоичный код $\mathbb{C}$ имеет следующие параметры:

$$n_C = n_A n_B = 2^{m+u},\ K_C = 2^{n_A-1-u} n_B^{n_A-1} (2^{n_B-1-m})^{n_A} = 2^{n_C-1-(m+u)},$$
$$d_C \geqslant \min\{4 \cdot 1, 2 \cdot 2, 1 \cdot 4\} = 4$$

(на самом деле, $d_C = 4$). Если в коде $\mathbb{C}$ удалить любую позицию, то получится совершенный двоичный $(2^{m+u} - 1, K_C, 3)$-код.

Теорема 7 [47]. *Если коды $\mathbb{B}, \mathbb{B}_i, \mathbb{B}_{i,j}, \mathbb{A}_1, \mathbb{A}_2, \mathbb{A}_3$ подставить в обобщённую каскадную конструкцию, то получится совершенный двоичный $(n = 2^{m+u} - 1, 2^{n-(m+u)}, 3)$-код.*

Обобщённая каскадная конструкция является специальным случаем более общей конструкция Фелпса. Известны и другие каскадные конструкции, которые, в свою очередь, являются специальными случаями более общей обобщённой каскадной конструкциии, например, в [10]. В [15] предложены некоторые вариации обобщённой каскадной конструкции. Результаты из [17] близки к результатам из [15].

В [11, 12] установлено, что число неэквивалентных совершенных двоичных кодов длины $n = 15$ и число неэквивалентных расширенных совершенных двоичных кодов длины $n = 16$, которые могут быть построены обобщённой каскадной конструкцией, соответственно равно 777 и 285, т. е. это коды ранга 11, 12, 13.

5. Коды Васильева

Пусть $\mathbb{C}$ — совершенный двоичный код длины $n = 2^s - 1$, $s = 1, 2, \ldots$, $p(\mathbf{u})$ — функция чётности, λ — булева функция, зависящая от n переменных.

Теорема 8 [5]. *Множество*

$$\mathbb{V} = \{(\mathbf{u}|\mathbf{u}+\mathbf{v}|p(\mathbf{u}) + \lambda(\mathbf{v})) \mid \mathbf{u} \in \mathbb{F}_2^n,\ \mathbf{v} \in \mathbb{C}\}$$

является совершенным двоичным кодом длины $2n+1$.

Пусть булева функция $\lambda \equiv 0$. Рассмотрим код Васильева

$$\mathbb{V}_0 = \{(\mathbf{u}|p(\mathbf{u})|\mathbf{u}+\mathbf{v}) \mid \mathbf{u} \in \mathbb{F}_2^n,\ \mathbf{v} \in \mathbb{C}\}. \tag{2}$$

Нетрудно заметить, что код $\mathbb{V}_0$ может быть построен с помощью **uv**-конструкции. Пусть $R_{n+1} = \{(\mathbf{u}|p(\mathbf{u})|\mathbf{u}) \mid \mathbf{u} \in \mathbb{F}_2^n\}$. Тогда код $\mathbb{V}_0$ представим в виде

$$\mathbb{V}_0 = \bigcup_{\mathbf{c}\in\mathbb{C}} \left(R_{n+1} + (\mathbf{0}|\mathbf{c})\right),$$

где $\mathbf{0}$ — нулевой вектор длины $n+1$. Подмножества $(R_{n+1} + (\mathbf{0}|\mathbf{c}))$ являются $(n{+}1)$-компонентами кода Васильева $\mathbb{V}_0$ и образуют регулярное разбиение этого кода. Таким образом, коды Васильева образуют подкласс в свитчинговом классе кода $\mathbb{V}_0$. Формула (2) также позволяет строить коды Хемминга; часть кодов из свитчингового класса кода Хемминга являются кодами Васильева. Вероятно, не все коды $\mathbb{V}_0$ принадлежат свитчинговым классам кодов Хемминга, но этот вопрос остаётся открытым и, по-видимому, является трудным для решения.

Если исходный совершенный код $\mathbb{C}$ длины n является кодом полного ранга, то конструкция Васильева позволяет построить код $\mathbb{V}$ длины $2n+1$, который также будет кодом полного ранга. Действительно, пусть векторы $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathbb{C}$ являются линейно независимыми. Тогда векторы $(\mathbf{e}_i|\mathbf{e}_i|1)$, $(\mathbf{0}|\mathbf{v}_i|0)$, $i = 1, 2, \ldots, n$, $(\mathbf{0}|\mathbf{v}'|1)$, $\mathbf{v}' \in \mathbb{C}$, $\lambda(\mathbf{v}') = 1$ принадлежат коду Васильева $\mathbb{V}$ длины $2n+1$ и являются линейно независимыми.

Ю. Л. Васильевым и Ф. И. Соловьёвой [5–7, 65, 29] изучались графы минимальных расстояний укороченных совершенных двоичных кодов длины $n-1$ (во всех векторах кода удаляется координата с фиксированным номером; такое множество укороченных векторов называется *проекцией* кода). Компонентам связности графа минимальных расстояний соответствуют i-компоненты кода. Пусть $N_K(\mathbb{C})$ — число i-компонент совершенного кода $\mathbb{C}$ длины $n = 2t+1 = 2^s - 1$ ($i \in \{1, 2, \ldots, n\}$ и i фиксировано). В [29] показано, что $2 \leqslant N_K(\mathbb{C}) \leqslant 2^{t-(s-1)}$ при $s \geqslant 3$. Таким образом, совершенный код всегда разбивается не менее чем на две i-компоненты, причём мощность самой большой компоненты совершенного кода длины n может быть равна 2^{n-s-1}, а мощность самой маленькой компоненты — 2^t. В [65] при $s \geqslant 3$ построены коды с компонентами мощности $2^{n-s-(k-r)}$, где $k = 2^r - 1, r = 2, \ldots, s-1$ (при помощи компьютера несложно обнаружить компоненты и других мощностей, в частности, компоненты, мощность которых не выражается в виде степени двойки). Вопрос о том, какова может быть мощность компонент совершенных кодов, остаётся открытым.

В [31] установлено, что коды длины n и ранга $n-s+1$ являются кодами Васильева, а коды длины n и ранга $n-s+2$ могут быть построены с помощью конструкции Фелпса (m-арных квазигрупп порядка 4 и тривиальных разбиений множеств $\mathbb{E}_0^4$ и $\mathbb{E}_1^4$ на расширенные коды Хемминга длины $n=4$). Коды длины n и ранга $n-s+1$, $n-s+2$ можно назвать "почти линейными". По-видимому, число таких кодов невелико, а оценка их числа близка к оценке Васильева.

6. Коды Моллара

Введём обобщённые функции чётности $p_1(\mathbf{x}), p_2(\mathbf{x})$ так, как это сделано в [48]. Пусть компоненты вектора $\mathbf{x} \in \mathbb{F}_2^{n_1 n_2}$ имеют двойную нумерацию $\mathbf{x} = (x_{11}, \ldots, x_{1n_2}, x_{21}, \ldots, x_{n_1 n_2})$ и упорядочены в лексикографическом порядке. Расположим их в виде матрицы

$$\begin{vmatrix} x_{11} & x_{12} & \ldots & x_{1n_2} \\ x_{21} & x_{22} & \ldots & x_{2n_2} \\ \vdots & \vdots & & \vdots \\ x_{n_1 1} & x_{n_1 2} & \ldots & x_{n_1 n_2} \end{vmatrix} \tag{3}$$

и положим

$$p_1(\mathbf{x}) = \left(\sum_{j=1}^{n_2} x_{1j}, \ldots, \sum_{j=1}^{n_2} x_{n_1 j} \right) \in \mathbb{F}_2^{n_1},$$

$$p_2(\mathbf{x}) = \left(\sum_{i=1}^{n_1} x_{i1}, \ldots, \sum_{i=1}^{n_1} x_{i n_2} \right) \in \mathbb{F}_2^{n_2}.$$

Функция $p_1(\mathbf{x})$ определяется суммой элементов в строках матрицы (3), функция $p_2(\mathbf{x})$ — суммой элементов в столбцах.

Пусть $\mathbb{C}$, $\mathbb{C}'$ — совершенные двоичные коды длин n_1, n_2, и пусть f является вектор-функцией, отображающей множество $\mathbb{C} \subseteq \mathbb{F}_2^{n_1}$ в $\mathbb{F}_2^{n_2}$.

Теорема 9 [48]. *Множество*

$$\mathbb{M} = \{(\mathbf{x}|\mathbf{c} + p_1(\mathbf{x})|\mathbf{c}' + p_2(\mathbf{x}) + f(\mathbf{c})) \mid \mathbf{x} \in \mathbb{F}_2^{n_1 n_2}, \mathbf{c} \in \mathbb{C}, \mathbf{c}' \in \mathbb{C}'\}$$

является совершенным двоичным кодом длины $n_1 n_2 + n_1 + n_2$.

Доказательство. Заметим, что $n_1 = 2^{s_1} - 1$ и $n_2 = 2^{s_2} - 1$ при некоторых s_1 и s_2. Следовательно, $n = n_1 n_2 + n_1 + n_2 = 2^{s_1+s_2} - 1$. Число векторов в множестве $\mathbb{M}$ равно

$$|\mathbb{M}| = 2^{n_1 n_2} \frac{2^{n_1}}{n_1+1} \frac{2^{n_2}}{n_2+1} = \frac{2^n}{n+1}.$$

Таким образом, если $\mathbb{M}$ является кодом, исправляющим одну ошибку, то $\mathbb{M}$ является совершенным кодом. Пусть $\mathbf{a}$ и $\bar{\mathbf{a}}$ — два различных вектора из $\mathbb{M}$. Мы должны показать, что $d(\mathbf{a},\bar{\mathbf{a}}) \geqslant 3$. Для некоторых $\mathbf{x},\bar{\mathbf{x}},\mathbf{c},\bar{\mathbf{c}},\mathbf{c}',\bar{\mathbf{a}}'$ мы можем записать:

$$\mathbf{a} = (\mathbf{x}|\mathbf{c} + p_1(\mathbf{x})|\mathbf{c}' + p_2(\mathbf{x}) + f(\mathbf{c})),$$

$$\bar{\mathbf{a}} = (\bar{\mathbf{x}}|\bar{\mathbf{c}} + p_1(\bar{\mathbf{x}})|\bar{\mathbf{c}}' + p_2(\bar{\mathbf{x}}) + f(\bar{\mathbf{c}})).$$

a) Если $\mathbf{x} = \bar{\mathbf{x}}$, то $p_1(\mathbf{x}) = p_2(\bar{\mathbf{x}})$ и $d(\mathbf{a},\bar{\mathbf{a}}) = d(\mathbf{c},\bar{\mathbf{c}}) + d(\mathbf{c}',\bar{\mathbf{c}}') \geqslant 3$.

b) Если $d(\mathbf{x},\bar{\mathbf{x}}) = 1$, то $d(p_1(\mathbf{x}),p_1(\bar{\mathbf{x}})) = d(p_2(\mathbf{x}),p_2(\bar{\mathbf{x}})) = 1$. Если $\mathbf{c} \neq \bar{\mathbf{c}}$, то $d(\mathbf{c} + p_1(\mathbf{x}),\bar{\mathbf{c}} + p_1(\bar{\mathbf{x}})) \geqslant 2$ и $d(\mathbf{a},\bar{\mathbf{a}}) \geqslant 3$. Если $\mathbf{c} = \bar{\mathbf{c}}$, то $d(\bar{\mathbf{c}}' + p_2(\bar{\mathbf{x}}) + f(\bar{\mathbf{c}}),\mathbf{c}' + p_2(\mathbf{x}) + f(\mathbf{c}))$ и $d(\mathbf{a},\bar{\mathbf{a}}) \geqslant 3$.

c) Если $d(\mathbf{x},\bar{\mathbf{x}}) = 2$, то $d(p_1(\mathbf{x}),p_1(\bar{\mathbf{x}}))$ и $d(p_2(\mathbf{x}),p_2(\bar{\mathbf{x}}))$ равны 0 или 2, но не могут быть равны нулю одновременно. Следовательно, равенства $\mathbf{c} + p_1(\mathbf{x}) = \bar{\mathbf{c}} + p_1(\bar{\mathbf{x}})$ и $\mathbf{c}' + p_2(\mathbf{x}) + f(\mathbf{c}) = \bar{\mathbf{c}}' + p_2(\bar{\mathbf{x}}) + f(\bar{\mathbf{c}})$ несовместны и $d(\mathbf{a},\bar{\mathbf{a}}) \geqslant 3$.

d) Случай $d(\mathbf{x},\bar{\mathbf{x}}) \geqslant 3$ является тривиальным. Теорема 9 доказана.

Если в конструкции Васильева длина кода удваивается, то в конструкции Моллара она возрастает многократно. При $n_2 = 1$ конструкция Моллара превращается в конструкцию Васильева.

7. Свитчинговый класс кода Хемминга

Через $\mathbb{H}_s$ обозначим код Хемминга длины $n = 2^s - 1, s = 2,3,\ldots$. Проверочная матрица H_s кода Хемминга $\mathbb{H}_s$ состоит из всех ненулевых двоичных вектор-столбцов высоты s.

Известны три различных определения i-компонент кода Хемминга. Одно определение дано Т. Этционом и А. Варди [43], другое — К. Фелпсом и М. Ли Ваном [55], третье — А. М. Романовым [24]. Во всех трёх определениях для каждого $i \in \{1,2,\ldots,n\}$ определяется некоторая главная i-компонента, а все i-компоненты кода Хемминга являются некоторыми сдвигами этой главной i-компоненты, которая содержит нулевой вектор. Пусть K_r является i_r-компонентой кода Хемминга $\mathbb{H}_s$, $i_r \in \{1,2,\ldots,n\}$, $1 \leqslant r \leqslant m$. Если $K_r \cap K_{r'} = \varnothing$ при любых различных $r,r' \in \{1,2,\ldots,m\}$, то семейство $\mathcal{K} = \{K_1,K_2,\ldots,K_m\}$ i_r-компонент кода Хемминга $\mathbb{H}_s$ называется *допустимым.* Если $\mathcal{K}$ — допустимое семейство компонент кода $\mathbb{H}_s$, то можно показать, что множество

$$\mathbb{H}_s(\mathcal{K}) = \left(\mathbb{H}_s \setminus \bigcup_{r=1}^{m} K_r\right) \bigcup \left(\bigcup_{r=1}^{m} (K_r + \mathbf{e}_{i_r})\right)$$

является совершенным двоичным кодом длины $n = 2^s - 1$ (см. [43, 55, 24]). Таким образом, построение кодов Хемминга методом свитчингов сводится к построению допустимых семейств компонент кода (это утверждение справедливо и для произвольных совершенных кодов). Так как все i-компоненты кода Хемминга являются сдвигами некоторой главной i-компоненты, то построение допустимого семейства компонент кода Хемминга сводится к построению множества пар $(i_1, \mathbf{c}_1), (i_2, \mathbf{c}_2), \ldots, (i_m, \mathbf{c}_m)$, где векторы $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m$ определяют сдвиги главной компоненты и являются представителями компонент $K_1, K_2, \ldots, K_m$. Далее представим конструкции совершенных двоичных кодов полного ранга с тривиальным ядром, предложенные в [43, 26].

7.1. Коды полного ранга

Прежде чем приступить к описанию конструкции кодов полного ранга, предложенной в [43], введём необходимые обозначения и определения. Пусть $h_1, h_2, \ldots, h_n$ — столбцы проверочной матрицы H_s кода Хемминга $\mathbb{H}_s$, упорядоченные произвольным, но фиксированным образом. Пусть $\mathbf{z} \in \mathbb{F}_2^s$ и $\mathbf{z} \neq \mathbf{0}$. Тогда существует $i \in \{1, 2, \ldots, n\}$ такое, что $\mathbf{z} = h_i^T$, где h_i^T — транспонированный вектор-столбец матрицы H_s (далее символ, обозначающий транспонирование, мы будем опускать). Пусть функция $\varphi(\mathbf{z})$ такова, что $\varphi(\mathbf{z}) = i$ (если столбцы проверочной матрицы упорядочены в лексикографическом порядке, то каждому числу, представленному в двоичной системе счисления, функция φ сопоставляет это же число, но представленное в десятичной системе счисления). Вектор $\mathbf{z}$ индуцирует разбиение столбцов $h_1, h_2, \ldots, h_{\varphi(\mathbf{z})-1}, h_{\varphi(\mathbf{z})+1}, \ldots, h_n$ на t пар (h_i, h_j) таких, что $h_i + h_j = \mathbf{z}$. Определим функцию $\nu_{\mathbf{z}}(i)$. Положим $j = \nu_{\mathbf{z}}(i)$, $i = \nu_{\mathbf{z}}(j)$. Для того чтобы полученное разбиение столбцов было единственным, будем считать, что $i < j$. Определим подмножество $I \subset \{1, 2, \ldots, n\} \setminus \{\varphi(\mathbf{z})\}$ мощности t такое, что $h_i + h_{\nu_{\mathbf{z}}(i)} = \mathbf{z}$, и будем считать, что $i < \nu_{\mathbf{z}}(i)$ при любом $i \in I$. Далее определим подмножества

$$A(\mathbf{z}) = \left\{ (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n \mid \forall i \in I,\ x_i = x_{\nu_{\mathbf{z}}(i)} \text{ и } x_{\varphi(\mathbf{z})} = \sum_{i \in I} x_i \right\},$$

$$B(\mathbf{z}) = \left\{ (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n \mid \forall i \in I,\ x_i = x_{\nu_{\mathbf{z}}(i)} \text{ и } x_{\varphi(\mathbf{z})} = 1 + \sum_{i \in I} x_i \right\}. \quad (4)$$

Подмножество $A(\mathbf{z})$ является главной i-компонентой кода Хемминга $\mathbb{H}_s$, $i = \varphi(\mathbf{z})$ [43]. Подмножество $B(\mathbf{z})$ является сдвигом по координате i-компоненты $A(\mathbf{z})$, т. е. $B(\mathbf{z}) = A(\mathbf{z}) + \mathbf{e}_i$.

Пусть $s \geqslant 4$, $k \leqslant s$, и пусть векторы $\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_k$ являются линейно независимыми.

Теорема 10 [43]. *Существуют кодовые слова* $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k \in \mathbb{H}_s$ *такие, что* $(\mathbf{c}_i + A(\mathbf{z}_i)) \cap (\mathbf{c}_j + A(\mathbf{z}_j)) = \varnothing$ *при любых различных* $i, j \in \{1, 2, \ldots, k\}$.

Доказательство. Определим отображение ξ ненулевых векторов из $\mathbb{F}_2^s$ на векторы веса 1 из $\mathbb{F}_2^n$. Для любого вектора $\mathbf{z} \in \mathbb{F}_2^s \setminus \{\mathbf{0}\}$ положим $\xi(\mathbf{z}) = (x_1, x_2, \ldots, x_n)$, где

$$x_i = \begin{cases} 1 & \text{при } i = \varphi(\mathbf{z}), \\ 0 & \text{при } i \neq \varphi(\mathbf{z}). \end{cases}$$

Используя введённые обозначения, определим векторы $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k$:

$$\begin{aligned} \mathbf{c}_1 &= \xi(\mathbf{z}_1) + \xi(\mathbf{z}_1 + \mathbf{z}_2 + \mathbf{z}_3) + \xi(\mathbf{z}_1 + \mathbf{z}_2 + \mathbf{z}_4) + \xi(\mathbf{z}_1 + \mathbf{z}_3 + \mathbf{z}_4), \\ \mathbf{c}_2 &= \xi(\mathbf{z}_1) + \xi(\mathbf{z}_2) + \xi(\mathbf{z}_1 + \mathbf{z}_3 + \mathbf{z}_4) + \xi(\mathbf{z}_2 + \mathbf{z}_3 + \mathbf{z}_4), \\ \mathbf{c}_4 &= \xi(\mathbf{z}_1) + \xi(\mathbf{z}_2) + \xi(\mathbf{z}_3) + \xi(\mathbf{z}_4) + \xi(\mathbf{z}_1 + \mathbf{z}_2 + \mathbf{z}_3) + \\ &\quad \xi(\mathbf{z}_1 + \mathbf{z}_2 + \mathbf{z}_4) + \xi(\mathbf{z}_1 + \mathbf{z}_3 + \mathbf{z}_4) + \xi(\mathbf{z}_2 + \mathbf{z}_3 + \mathbf{z}_4). \end{aligned} \tag{5}$$

Так как $s \geqslant 4$, то всегда можно выбрать 4 линейно независимых вектора $\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4$. Пусть $j \in \{1, 2, \ldots, k\} \setminus \{1, 2, 4\}$. Если j нечётно, то

$$\mathbf{c}_j = \sum_{i=1}^{j} \xi(\mathbf{z}_i) + \xi(\mathbf{z}_1 + \mathbf{z}_2 + \cdots + \mathbf{z}_j). \tag{6}$$

Если j чётно, то

$$\mathbf{c}_j = \sum_{i=1}^{j} \xi(\mathbf{z}_i) + \xi(\mathbf{z}_1 + \mathbf{z}_2 + \cdots + \mathbf{z}_{\frac{j}{2}}) + \xi(\mathbf{z}_{\frac{j}{2}+1} + \mathbf{z}_{\frac{j}{2}+2} + \cdots + \mathbf{z}_j). \tag{7}$$

Заметим, что синдром $H_s \xi(\mathbf{z})^T = \mathbf{z}$. Следовательно, легко показать, что $H_s \mathbf{c}_j^T = \mathbf{0}$ при всех j и векторы $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k$ принадлежат коду $\mathbb{H}_s$. Так как векторы $\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_k$ являются линейно независимыми, то вес вектора $\mathbf{c}_j$ равен числу слагаемых в формуле. Подсчёт слагаемых в формулах показывает, что все векторы $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k$ имеют чётный вес.

Теперь предположим, что $(\mathbf{c}_i + A(\mathbf{z}_i)) \cap (\mathbf{c}_j + A(\mathbf{z}_j)) \neq \varnothing$. Тогда $\mathbf{c}_i + \mathbf{x} = \mathbf{c}_j + \mathbf{y}$ для некоторых $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in A(\mathbf{z}_i)$ и $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in A(\mathbf{z}_j)$.

Чётность вектора $\mathbf{x}+\mathbf{y}$ определяется формулой

$$p(\mathbf{x}+\mathbf{y}) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i = x_{\varphi(\mathbf{z}_i)} + y_{\varphi(\mathbf{z}_j)}. \tag{8}$$

Второе равенство следует из формулы (4). Без ограничения общности будем считать, что $i < j$. Пусть $\mathbf{c}_i = (a_1, a_2, \ldots, a_n)$ и $\mathbf{c}_j = (a'_1, a'_2, \ldots, a'_n)$. Из формул (5)–(7) следует, что

$$a_{\varphi(\mathbf{z}_i)} = a'_{\varphi(\mathbf{z}_i)} = 1,\ a_{\varphi(\mathbf{z}_j)} = 0,\ a'_{\varphi(\mathbf{z}_j)} = 1,\ a_{\varphi(\mathbf{z}_i+\mathbf{z}_j)} = a'_{\varphi(\mathbf{z}_i+\mathbf{z}_j)} = 0.$$

Следовательно,

$$x_{\varphi(\mathbf{z}_i)} = y_{\varphi(\mathbf{z}_i)},\ x_{\varphi(\mathbf{z}_j)} = 1 + y_{\varphi(\mathbf{z}_j)},\ x_{\varphi(\mathbf{z}_i+\mathbf{z}_j)} = y_{\varphi(\mathbf{z}_i+\mathbf{z}_j)}. \tag{9}$$

Подставив (9) в (8), получим $p(\mathbf{x}+\mathbf{y}) = x_{\varphi(\mathbf{z}_i)} + x_{\varphi(\mathbf{z}_j)} + 1$. Так как векторы $\mathbf{c}_i$ и $\mathbf{c}_j$ имеют чётный вес, то $p(\mathbf{x}+\mathbf{y}) = p(\mathbf{c}_i + \mathbf{c}_j) = 0$. Противоречие. Следовательно, $(\mathbf{c}_i + A(\mathbf{z}_i)) \cap (\mathbf{c}_j + A(\mathbf{z}_j)) = \varnothing$. Теорема 10 доказана.

Далее опишем предложенную в [26] конструкцию кодов полного ранга с тривиальным ядром. Пусть столбцы проверочной матрицы H_s упорядочены в антилексикографическом порядке. Векторы $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{s-1}$ определяются строками матрицы $\begin{vmatrix} O_{s-1} & H_{s-1} \end{vmatrix}$, где через O_{s-1} обозначена матрица, состоящая из нулей, размера $(s-1) \times (t+1)$, а H_{s-1} — проверочная матрица кода Хемминга $\mathbb{H}_{s-1}$. Вектор $\mathbf{c}_s$ является нулевым вектором. Координатное множество $\{i_1, i_2, \ldots, i_s\}$ определяется следующим образом: $i_1 = 2^{s-1}, i_2 = 2^{s-2}, \ldots, i_{s-1} = 2, i_s = 1$. В [26] с помощью достаточных условий непересекаемости компонент кода Хемминга, полученных в [24], установлено, что так определённое множество пар порождает допустимое семейство $\mathcal{K}$ компонент кода Хемминга $\mathbb{H}_s$, и код $\mathbb{H}_s(\mathcal{K})$ является кодом полного ранга с тривиальным ядром.

7.2. Условия непересекаемости компонент кода Хемминга

Если $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, то *носителем* вектора $\mathbf{x}$ называется множество $[\mathbf{x}] = \{i \mid x_i = 1\}$. Пусть вектор $\mathbf{w} \in \mathbb{H}_s$ таков, что его носитель $[\mathbf{w}]$ является $(s-2)$-мерной плоскостью конечной проективной геометрии $PG_{s-1}(2)$. Пусть $\mathbb{H}_{s-1}(\mathbf{w}) = \{\mathbf{u} \mid \mathbf{u} \in \mathbb{H}_s, [\mathbf{u}] \subseteq [\mathbf{w}]\}$. Множество $\mathbb{H}_{s-1}(\mathbf{w})$ можно считать подкодом кода Хемминга $\mathbb{H}_s$.

Пусть $i = \varphi(\mathbf{z}_i), j = \varphi(\mathbf{z}_j)$. Тогда запись $k = i + j$ означает, что $\mathbf{z}_k = \mathbf{z}_i + \mathbf{z}_j$ и $k = \varphi(\mathbf{z}_k)$. Через $R_i + \mathbf{u}$ обозначим i-компоненту кода $\mathbb{H}_s$, $\mathbf{u} \in \mathbb{H}_s$.

Теорема 11 [23]. *При любых различных* $i, j \notin [\mathbf{w}]$ *и* $\mathbf{u}, \mathbf{v} \in \mathbb{H}_{s-1}(\mathbf{w})$

компоненты $R_i+\mathbf{u}$ *и* $R_j+\mathbf{v}$ *не пересекаются тогда и только тогда, когда* $\mathbf{u}+\mathbf{v}\notin R_k\cap\mathbb{H}_{s-1}(\mathbf{w})$, *где* $k=i+j$.

В теореме 11 представлен критерий непересекаемости компонент кода Хемминга, который обобщает достаточные условия непересекаемости компонент кода Хемминга, полученные в [24].

Теорема 12 [24]. *При любых различных* $i,j\notin[\mathbf{w}]$ *и* $\mathbf{u},\mathbf{v}\in\mathbb{H}_{s-1}(\mathbf{w})$ *компоненты* $R_i+\mathbf{u}$ *и* $R_j+\mathbf{v}$ *не пересекаются тогда, когда множество* $\{[\mathbf{u}+\mathbf{v}]\setminus k\}$ *содержит нечётное число элементов,* $k=i+j$.

Эти достаточные условия непересекаемости компонент кода Хемминга $\mathbb{H}_s$ при $s=4$ являются и необходимыми.

Теперь приведём определение i-компоненты кода Хемминга, которое используется в [24] для доказательства теоремы 12. Без ограничения общности будем считать, что столбцы проверочной матрицы H_s упорядочены в антилексикографическом порядке и ненулевые элементы находятся в последних t позициях вектора $\mathbf{w}$ ($t=\frac{n-1}{2}=2^{s-1}-1$). Тогда код Хемминга $\mathbb{H}_s$ представим в виде

$$\mathbb{H}_s=\{(\mathbf{u}|p(\mathbf{u})|\mathbf{u}+\mathbf{v})\mid \mathbf{u}\in\mathbb{F}_2^t,\mathbf{v}\in\mathbb{H}_{s-1}\}$$

и код $\mathbb{H}_{s-1}$ может быть получен удалением в векторах из подмножества $\mathbb{H}_s(\mathbf{w})$ первых $t+1$ координат.

Пусть $STS(\mathbb{H}_{s-1})$ — система троек Штейнера, порождённая словами веса 3 кода $\mathbb{H}_{s-1}$. Для любых i,j, $1\leqslant i\leqslant t+1$, $1\leqslant j\leqslant t+1$, положим

$$\pi_{i,j}=\begin{cases} k & \text{при } \{i,j,k\}\in STS(\mathbb{H}_{s-1}),\\ i & \text{при } j=t+1,\\ j & \text{при } i=t+1,\\ t+1 & \text{при } i=j.\end{cases}$$

Для любого i, $1\leqslant i\leqslant t+1$, определим перестановку координат в $\mathbb{F}_2^{t+1}$. Положим $\pi_i=(\pi_{i,1},\pi_{i,2},\ldots,\pi_{i,t+1})$. Через $\pi_i(\mathbf{u})$ обозначим слово, которое получается из слова $\mathbf{u}=(u_1,u_2,\ldots,u_{t+1})\in\mathbb{F}_2^{t+1}$ после применения к буквам слова $\mathbf{u}$ перестановки π_i. Определим отображение ψ_i векторов из $\mathbb{F}_2^{t+1}$ на векторы из $\mathbb{F}_2^t$, положив

$$\psi_i(u_1,\ldots,u_{i-1},u_i,u_{i+1},\ldots,u_{t+1})=(u_1,\ldots,u_{i-1},u_{i+1},\ldots,u_{t+1}).$$

Пусть $1\leqslant i\leqslant t+1$. Тогда $R_i=\{(\mathbf{u}|\psi_i(\pi_i(\mathbf{u})))\mid \mathbf{u}\in\mathbb{E}_0^{t+1}\}$. Согласно [24] подмножество R_i является главной i-компонентой кода Хемминга $\mathbb{H}_s$, $s\geqslant 4$.

7.3. Несистематические коды

В этом разделе опишем конструкцию несистематических совершенных двоичных кодов при всех допустимых длинах, начиная с $n = 15$.

Совершенный код $\mathbb{C}$ длины $n = 2^s - 1$, содержащий 2^{n-s} слов, называется *систематическим*, если множество координат $\{1, 2, \ldots, n\}$ можно разбить на два подмножества $\{i_1, i_2, \ldots, i_s\}$ и $\{i_{s+1}, i_{s+2}, \ldots i_n\}$ (которые соответственно называются информационными и проверочными) так, что после удаления во всех кодовых словах $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{C}$ информационных символов u_{i_s}, $i_s \in \{i_1, i_2, \ldots, i_s\}$, полученное множество векторов длины $n - s$ совпадает с множеством $\mathbb{F}_2^{n-s}$. В противном случае код $\mathbb{C}$ называется *несистематическим*.

Опишем конструкцию несистематического кода длины $n = 15$, предложенную в [25]. Пусть столбцы проверочной матрицы H_s упорядочены в антилексикографическом порядке. Допустимое семейство компонент, которое задаёт несистематический код длины $n = 15$, определяется множеством пар $(i_1, \mathbf{c}_1), (i_2, \mathbf{c}_2), \ldots, (i_7, \mathbf{c}_7)$, где $\mathbf{c}_1 = (\mathbf{0}|\mathbf{v}_1)$, $\mathbf{c}_2 = (\mathbf{0}|\mathbf{v}_2)$, $\mathbf{c}_3 = (\mathbf{0}|\mathbf{v}_3)$, $\mathbf{c}_4 = (\mathbf{0}|\mathbf{v}_4)$, $\mathbf{c}_5 = (\mathbf{0}|\mathbf{v}_5)$, $\mathbf{c}_6 = (\mathbf{0}|\mathbf{v}_6)$, $\mathbf{c}_7 = (\mathbf{0}|\mathbf{v}_7)$, $\mathbf{0}$ — нулевой вектор длины 8. Векторы $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_7$ определяются плоскостью Фано и могут иметь, например, вид: $[\mathbf{v}_1] = \{1, 2, 7\}$, $[\mathbf{v}_2] = \{1, 3, 6\}$, $[\mathbf{v}_3] = \{1, 4, 5\}$, $[\mathbf{v}_4] = \{2, 3, 5\}$, $[\mathbf{v}_5] = \{2, 4, 6\}$, $[\mathbf{v}_6] = \{3, 4, 7\}$, $[\mathbf{v}_7] = \{5, 6, 7\}$. Тогда координатное множество $\{i_1, i_2, \ldots, i_7\}$ должно быть выбрано следующим образом: $i_1 = 8, i_2 = 6, i_3 = 7, i_4 = 3, i_5 = 1, i_6 = 2, i_7 = 5$.

С помощью теоремы 12 несложно проверить, что так определённое множество пар $(i_1, \mathbf{c}_1), (i_2, \mathbf{c}_2), \ldots, (i_7, \mathbf{c}_7)$ задаёт допустимое семейство $\mathcal{K}$ компонент кода Хемминга $\mathbb{H}_4$. Сдвиг компонент из семейства $\mathcal{K}$ даёт несистематический совершенный двоичный код длины $n = 15$. Как показано С. А. Малюгиным [20], для того чтобы построить несистематический код любой допустимой длины $n \geqslant 31$, к указанным выше векторам $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_7$ достаточно дописать слева необходимое число нулей.

Все известные сегодня несистематические коды длины $n = 15$ принадлежат свитчинговому классу кода Хемминга и их число ровно 12 (см. [20]). Общее число несистематических совершенных кодов длины $n = 15$ остаётся неизвестным. В работах [1, 56] неконструктивными методами доказано существование несистематических совершенных двоичных кодов.

7.4. Регулярные разбиения

Компоненты совершенного кода могут образовывать разбиение кода или тупиковую упаковку. В свою очередь, разбиения могут быть как регулярными так и нерегулярными. Любое допустимое семейство компонент кода может быть дополнено до разбиения или тупиковой упаковки.

Разбиение совершенного кода на компоненты называется *регулярным*, если в нём компоненты с одинаковыми координатами встречаются равное число раз. Регулярное разбиение имеет параметры $[k, l]$, если в нём участвуют k различных координат и каждая координата представлена l компонентами. Возможны следующие регулярные разбиения на компоненты кода Хемминга длины $n = 15$: $[1, 16], [2, 8], [4, 4], [8, 2]$ и тупиковая упаковка с параметрами $[5, 2]$. Из конструкции Васильева следует, что существует регулярное разбиение на компоненты двоичного кода Хемминга длины $n = 2t + 1 = 2^s - 1$ с параметрами $[1, 2^{t-(s-1)}]$.

Теперь приведём конструкцию совершенных двоичных кодов, предложенную в [24], из которой следует существование регулярного разбиения на компоненты двоичного кода Хемминга длины $n = 2t + 1 = 2^s - 1$ с параметрами $[2, 2^{t-s}]$ при $s \geqslant 4$.

Пусть носитель $[\mathbf{w}]$ вектора $\mathbf{w} \in \mathbb{H}_s$ является $(s-2)$-мерной плоскостью конечной проективной геометрии $PG_{s-1}(2)$ и R_i, R_j являются соответственно i- и j-компонентами кода Хемминга $\mathbb{H}_s$ $(i, j \notin [\mathbf{w}],\ i \neq j)$, λ, λ' — булевы функции, зависящие от n переменных, $k = i + j$ и

$$A_k = \{\mathbf{v} \mid \mathbf{v} \in \mathbb{H}_{s-1}(\mathbf{w}),\ p(\psi_k(\mathbf{v})) = 0\},$$

$$B_k = \{\mathbf{v} \mid \mathbf{v} \in \mathbb{H}_{s-1}(\mathbf{w}),\ p(\psi_k(\mathbf{v})) = 1\}.$$

Теорема 13 [24]. *При $s \geqslant 4$ множество*

$$\mathbb{C} = \left(\bigcup_{\mathbf{v} \in A_k} (R_i + \lambda(\mathbf{v})\mathbf{e}_i)\right) \bigcup \left(\bigcup_{\mathbf{v} \in B_k} (R_j + \lambda'(\mathbf{v})\mathbf{e}_j)\right)$$

является совершенным двоичным кодом длины $n = 2^s - 1$.

В [23] построены регулярные разбиения с новыми параметрами.

Теорема 14 [23]. *При любом $n = 2^s - 1$ $(s \geqslant 4)$ и любом k таком, что $1 \leqslant k < s$, существует регулярное разбиение кода Хемминга $\mathbb{H}_s$ на i-компоненты с параметрами $[2^k, 2^{t-(s-1)-k}]$, где $t = 2^{s-1} - 1$.*

7.5. Неконструктивные методы

Неконструктивность методов заключается в том, что эти методы не позволяют находить векторы $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$, которые задают сдвиги главной компоненты и определяют допустимое семейство компонент, а позволяют только доказать их существование. Используя неконструктивные методы, можно охарактеризовать некоторые свойства кода $\mathbb{C}$, который получается сдвигами компонент из кода $\mathbb{H}_s$, но нельзя ответить на вопрос: какие векторы из $\mathbb{F}_2^n$ принадлежат $\mathbb{C}$?

К. Фелпс и М. Ли Ван [55] обратили внимание на то, что подмножество $A(\mathbf{z})$, которое рассматривали Т. Этцион и А. Варди, является подпространством и порождается всеми векторами кода Хемминга веса 3 с единичной i-й координатой, где $i = \varphi(\mathbf{z})$. Таким образом, совокупность i-компонент кода Хемминга представляет собой совокупность смежных классов, образованных подпространством $A(\mathbf{z})$. Используя линейность i-компонент кода Хемминга, К. Фелпс и М. Ли Ван доказали существование в коде Хемминга непересекающихся i-компонент и j-компонент при $i \neq j$. Пусть R_i — i-компонента кода кода Хемминга $\mathbb{H}_s$ длины $n = 2t+1 = 2^s-1$. Используя линейные свойства i-компоненты R_i, несложно доказать существование вектора $\mathbf{c}' \in \mathbb{H}_s$ такого, что $R_i \cap (R_j + \mathbf{c}') = \varnothing$. Число смежных классов $R_j+\mathbf{c}$, где $\mathbf{c} \in \mathbb{H}_\mathbf{s}$, равно $2^{t-(s-1)}$. Мощность произвольной компоненты кода $\mathbb{H}_s$ равна 2^t. Поскольку пересечение $R_i \cap R_j$ является подпространством и $|R_i \cap R_j| = 2^{\frac{t+1}{2}}$ (см. [55]), то число смежных классов $R_j + \mathbf{c}$, имеющих непустое пересечение с подпространством R_i, равно $2^{\frac{t-1}{2}}$, что значительно меньше их общего числа. Следовательно, при достаточно большом s существует вектор $\mathbf{c}' \in \mathbb{H}_s$ такой, что $R_i \cap (R_j + \mathbf{c}') = \varnothing$.

Пусть подпространство $L \subseteq \mathbb{H}_s$ и компонента $R_i \subseteq L$. Тогда справедлива следующая

Теорема 15. *Множество $\mathbb{C} = (\mathbb{H}_s \setminus L) \cup (L + \mathbf{e}_i)$ является совершенным кодом длины n.*

Эта теорема позволяет доказать существование допустимых семейств компонент кода Хемминга.

В [2] рассмотрено разбиение кода Хемминга $\mathbb{H}_s$, образованное смежными классами подпространства $R_i + R_j$. Такое разбиение порождает разбиение кода $\mathbb{H}_s$ на компоненты и позволяет оценить снизу мощность свитчингового класса кода Хемминга. Полученная оценка близка к оценке Васильева.

В [16] установлено соответствие между свитчингами в квазигруппах и в кодах Хемминга и получена нижняя оценка мощности свитчингового класса кода Хемминга, которая близка к оценке Васильева.

Свитчинговый класс кода Хемминга, по-видимому, является наиболее мощным. Вопрос о мощности этого класса остаётся открытым: близка ли эта мощность к оценке Васильева или существенно от неё отличается?

8. Замощения

Пара подмножеств (V, A) из $\mathbb{F}_2^n$ образует *мозаичное замощение* пространства $\mathbb{F}_2^n$, если каждый вектор $\mathbf{x}$ из $\mathbb{F}_2^n$ единственным образом представим в виде $\mathbf{x} = \mathbf{v} + \mathbf{a}$, где $\mathbf{v} \in V$ и $\mathbf{a} \in A$.

Очевидно, что шар Хемминга радиуса 1 и совершенный код с минимальным расстоянием 3 образуют мозаичные замощения пространства $\mathbb{F}_2^n$. Очевидно также, что множества V и A можно поменять местами (см. [43, 44, 35]).

Теорема 16 [44]. *Пусть (V, A) — мозаичное замощение пространства $\mathbb{F}_2^n$ и $t = |V| - 1$. Кроме того, пусть $H(V)$ — матрица размера $n \times t$, столбцами которой являются ненулевые элементы из V. Тогда множество $\mathbb{C} = \{\mathbf{x} \in \mathbb{F}_2^t \mid H(V)\mathbf{x}^T \in A\}$ является совершенным двоичным кодом длины t.*

Построенный согласно теореме 16 совершенный код $\mathbb{C}$ называется кодом, *соответствующим* мозаичному замощению (V, A).

Т. Этцион и А. Варди [44] построили мозаичные замощения $\mathbb{F}_2^n$ и показали, что при $n \geqslant 1023$ соответствующие им совершенные двоичные коды являются кодами полного ранга с большими размерностями ядер. Они также поставили вопрос о соотношении ранга и размерности ядра совершенного кода, т. е. предлагалось выяснить: какие пары (k, r) являются реализуемыми в качестве ранга r и размерности ядра k какого-либо совершенного кода? Полный ответ на этот вопрос был получен в [60], за исключением некоторого конечного числа случаев, которые исчерпаны в работах [3, 4, 50, 41].

9. Заключение

Поскольку разброс между нижней и верхней оценками числа неэквивалентных совершенных двоичных кодов длины n является существенным, трудно сказать насколько хороши известные сегодня методы построения совершенных кодов. Умеем ли мы строить большинство совершенных кодов или лишь незначительную их часть? Сближение нижней и верхней оценок числа неэквивалентных совершенных кодов является важной проблемой теории совершенных кодов.

Все известные сегодня нижние оценки числа неэквивалентных совершенных кодов длины n являются оценками мощности свитчингового класса некоторого совершенного кода. Не исключено, что число свитчинговых классов значительно превосходит мощность самого большого свитчингового класса.

По всей видимости подавляющее большинство совершенных кодов — это коды предполного или полного ранга и весьма вероятно, что большинство совершенных кодов образуют свитчинговые классы небольшой мощности, возможно, состоящие из одного или двух кодов.

Все известные сегодня совершенные коды полного ранга длины $n = 15$ принадлежат свитчинговому классу кода Хемминга [22]. Вероятно существуют и другие совершенные коды полного ранга длины $n = 15$, принадлежащие другим свитчинговым классам. Но пока не известны методы, которые позволяли бы построить такие коды.

Недавнее перечисление при помощи компьютера всех систем четверок Штейнера порядка 16 (см. [45]) позволило ответить на многие вопросы в теории дизайнов (работы [69] и [45] разделяет почти столетний период времени). Перечисление всех совершенных кодов длины $n = 15$ также является важной задачей. В частности, это позволило бы ответить на вопрос о числе свитчинговых классов, на которые разбиваются совершенные коды длины $n = 15$.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьёва Ф. И.** О несистематических совершенных двоичных кодах // Проблемы передачи информации. 1996. Т. 32, вып. 3. С. 47–50.
2. **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.
3. **Августинович С. В., Соловьёва Ф. И., Хеден У.** Совершенные коды полного ранга с ядрами больших размерностей // Дискрет. анализ. и исслед. операций. Сер. 1. 2001. Т. 8, № 4. С. 3–8.
4. **Августинович С. В., Соловьёва Ф. И., Хеден У.** О проблеме рангов и ядер совершенных кодов // Проблемы передачи информации. 2003. Т. 39, вып. 4. С. 30–34.
5. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. Вып. 8. М.: Физматгиз, 1962. С. 337–339.
6. **Васильев Ю. Л.** О сравнении сложности тупиковых и минимальных дизъюнктивных нормальных форм // Проблемы кибернетики. Вып. 10. М.: Физматгиз, 1963. С. 5–61.
7. **Васильев Ю. Л., Соловьёва Ф. И.** Кодообразующие факторизации n-мерного единичного куба и совершенных двоичных кодов // Проблемы передачи информации. 1997. Т. 33, вып. 1. С. 64–74.
8. **Зиновьев В. А.** Коды для корреляционной многоадресной селекции. Дис. ... канд. техн. наук. М., 1970.

9. **Зиновьев В. А.** Обобщённые каскадные коды // Проблемы передачи информации. 1976. Т. 12, вып. 1. С. 5–15.
10. **Зиновьев В. А.** Комбинаторные методы построения и анализа нелинейных корректирующих кодов. Дис. ... д-ра физ.-мат. наук. М., 1988.
11. **Зиновьев В. А., Зиновьев Д. В.** Двоичные расширенные совершенные коды длины 16, построенные обобщённой каскадной конструкцией // Проблемы передачи информации. 2002. Т. 38, вып. 4. С. 56–84.
12. **Зиновьев В. А., Зиновьев Д. В.** Двоичные совершенные коды длины 15, построенные обобщённой каскадной конструкцией // Проблемы передачи информации. 2004. Т. 40, вып. 1. С. 27–39.
13. **Зиновьев В. А., Зиновьев Д. В.** Двоичные расширенные совершенные коды длины 16 ранга 14 // Проблемы передачи информации. 2006. Т. 42, вып. 2. С. 63–80.
14. **Зиновьев В. А., Леонтьев В. К.** Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. 1973. Т. 2, № 2. С. 123–132.
15. **Зиновьев В. А., Лобстейн А. С.** Об обобщённых каскадных конструкциях совершенных двоичных нелинейных кодов // Проблемы передачи информации. 2000. Т. 36, вып. 4. С. 59–73.
16. **Кротов Д. С.** Нижние оценки числа m-квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискрет. анализ. и исслед. операций. Сер. 1. 2000. Т. 7, № 2. С. 47–53.
17. **Кротов Д. С.** Комбинированная конструкция совершенных двоичных кодов // Проблемы передачи информации. 2000. Т. 36, вып. 4. С. 74–79.
18. **Лось А. В.** Построение совершенных q-ичных кодов свитчингами простых компонент // Проблемы передачи информации. 2006. Т. 42, вып. 1. С. 34–42.
19. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
20. **Малюгин С. А.** Несистематические совершенные двоичные коды // Дискрет. анализ. и исслед. операций. Сер. 1. 2001. Т. 8, № 1. С. 55–76.
21. **Малюгин С. А.** О классах эквивалентности совершенных двоичных кодов длины 15 // Новосибирск, 2004. 34 с. (Препринт / РАН, Сиб. отд-ние. Институт математики; № 138).
22. **Малюгин С. А.** О перечислении неэквивалентных совершенных двоичных кодов длины 15 и ранга 15 // Дискрет. анализ. и исслед. операций. Сер. 1. 2006. Т. 13, № 1. С. 77–98.
23. **Малюгин С. А., Романов А. М.** О разбиениях кодов Хемминга на непересекающиеся компоненты // Дискрет. анализ. и исслед. операций. Сер. 1. 2002. Т. 9, № 1. С. 42–48.

24. **Романов А. М.** О построении совершенных нелинейных двоичных кодов инверсией символов // Дискрет. анализ. и исслед. операций. Сер. 1. 1997. Т. 4, № 1. С. 46–52.

25. **Романов А. М.** О несистематических совершенных кодах длины 15 // Дискрет. анализ. и исслед. операций. Сер. 1. 1997. Т. 4, № 4. С. 75–78.

26. **Романов А. М.** Совершенные двоичные коды с тривиальным ядром // Дискрет. анализ. и исслед. операций. Сер. 1. 2000. Т. 7, № 2. С. 71–74.

27. **Романов А. М.** О разбиениях q-ичных кодов Хемминга на непересекающинся компоненты // Дискрет. анализ. и исслед. операций. Сер. 1. 2004. Т. 11, № 3. С. 80–87.

28. **Соловьёва Ф. И.** О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. Сб. науч. тр. Вып. 37. Новосибирск: Ин-т математики, 1981. С. 65–76.

29. **Соловьёва Ф. И.** Точные границы связности кодообразующих д.н.ф. // Новосибирск, 1990. 15 с. (Препринт / АН СССР, Сиб. отд-ние. Институт математики; № 10).

30. **Форни Д.** Каскадные коды. М.: Мир, 1970.

31. **Avgustinovich S. V., Heden O., Solov'eva F. I.** The classification of some perfect codes // Designs, Codes and Cryptog. 2004. V. 31, N 3. P. 313–318.

32. **Avgustinovich S. V., Lobstein A., Solov'eva F. I.** Intersection matrices for partitions by binary perfect codes // IEEE Trans. on Inform. Theory. 2001. V. 47, N 4. P. 1621–1624.

33. **Bauer H., Ganter B., Hergert F.** Algebraic techniques for nonlinear codes // Combinatorica. 1983. V. 3, N 1. P. 21–33.

34. **Cohen G., Honkala I., Litsyn S., Lobstein A.** Covering codes. North Holland: Elsevier, 1998.

35. **Cohen G., Litsyn S., Vardy A., Zemor G.** Tilings of binary spaces // SIAM J. Discrete Math. 1996. V. 9, N 3. P. 393–412.

36. **Delsarte P., Goethals J. M.** Unrestricted codes with the Golay parameters are unique // Discrete Math. 1975. V. 12, N 3. P. 211–224.

37. **Gibbons P. B.** Computing techniques for the construction and analysis of block designs. Ph.D. Thesis, Department of Computer Science, University of Toronto, 1976.

38. **Hamming R. W.** Error detecting and error correcting codes // Bell System Tech. J. 1950. V. 29, N 2. P. 147–160.

39. **Heden O.** A new construction of group and nongroup perfect codes // Inform. and Control. 1977. V. 34, N 4. P. 314–323.

40. **Heden O.** A binary perfect code of length 15 and codimension 0 // Designs, Codes and Cryptog. 1994. V. 4, N 3. P. 213–220.

41. Heden O. A full rank perfect code on length 31 // Designs, Codes and Cryptog. 2006. V. 38, N 1. P. 125–129.

42. Hergert F. The equivalence classes of the Vasil'ev codes of length 15 // Combinatorial Theory. Berlin: Springer, 1982. P. 176–186. (Lectures Notes in Math. V. 969).

43. Etzion T., Vardy A. Perfect binary codes: constructions, properties, and enumeration // IEEE Trans. on Inform. Theory. 1994. V. 40, N 3. P. 754–763.

44. Etzion T., Vardy A. On perfect codes and tilings: problems and solution // SIAM J. Discrete Math. 1998. V. 11, N 2. P. 205–253.

45. Kaski P., Östergård P. R. J., Pottonen O. The Steiner quadruple systems of order 16 // J. Combin. Theory. Ser. A. 2006. V. 113, N 8. P. 1764–1770.

46. Limbos M. Projective embeddings of small "Steiner triple systems"// Ann. Discrete Math. 1980. V. 7. P. 151–173.

47. Lobstein A. S., Zinoviev V. A. On new perfect binary nonlinear codes // Applicable Algebra in Engineering, Communication and Computing. 1997. V. 8, N 5. P. 415–420.

48. Mollard M. A generalized parity function and its use in construction of perfect codes // SIAM J. Algebraic Discrete Methods. 1986. V. 7, N 1. P. 113–115.

49. Östergård P. R. J., Pottonen O. The exist Steiner triple systems of order 15 that do not occur in a perfect binary one-error-correcting code // J. of Combinatorial Designs, to appear.

50. Östergård P. R. J., Vardy A. Resolving the existence of full-rank tilings of binary Hamming spases // SIAM J. Discrete Math. 2004. V. 18, N 2. P. 382–387.

51. Phelps. K. T. A combinatorial construction of perfect codes // SIAM J. Algebraic Discrete Methods. 1983. V. 4, N 3. P. 398–403.

52. Phelps K. T. A general product construction for error correcting codes // SIAM J. Algebraic Discrete Methods 1984. V. 5, N 2. P. 224–228.

53. Phelps K. T. An enumeration of 1-perfect binary codes // Australas. J. Combin. 2000. V. 21. P. 287–298.

54. Phelps K. T. Combinatorial designs and perfect codes // Electronic Notes in Discrete Math. 2001. V. 10. 15 p.

55. Phelps K. T., LeVan M. Kernels of nonlinear Hamming codes // Designs Codes and Cryptogr. 1995. V. 6, N 3. P. 247–257.

56. Phelps K. T., LeVan M. Non-systematic perfect codes // SIAM J. Discrete Math. 1999. V. 12, N 1. P. 27–34.

57. Phelps K. T., LeVan M. Switching equivalence classes of perfect codes // Designs Codes and Cryptogr. 1999. V. 16, N 2. P. 179–184.

58. Phelps K. T., Rifà J., Villanueva M. Kernels and p-kernels of p^r-ary 1-perfect codes // Designs Codes and Cryptogr. 2005. V. 37, N 2. P. 243–261.

59. Phelps K. T., Villanueva M. Ranks of q-ary 1-perfect codes // Designs Codes and Cryptogr. 2002. V. 27, N 1–2. P. 139–144.

60. Phelps K. T., Villanueva M. On perfect codes: rank and kernel // Designs Codes and Cryptogr. 2002. V. 27, N 3. P. 183–194.

61. Pless V. On the uniqueness of the Golay codes // J. Combin. Theory. 1968. V. 5, N 3. P. 215–228.

62. Rifà J. Well-ordered Steiner triple systems and 1-perfect partitions of the n-cube // SIAM J. Discrete Math. 1999. V. 12, N 1. P. 35–47.

63. Rifà J., Vardy A. On partitions of space into perfect codes // III French-Israeli Workshop on Coding Theory and Information Integrity. Ein Boqeq, Dead Sea, Israel, October 1997.

64. Schönheim J. On linear and nonlinear single-error-correcting q-nary perfect codes // Inform. and Control. 1968. V. 12, N 1. P. 23–26.

65. Solov'eva F. I. Structure of i-components of perfect binary codes // Discrete Applied Math. 2001. V. 111, N 1–2. P. 189–197.

66. Solov'eva F. I. On perfect codes and related topics. Korea: Pohang, Combinatorial and Computational Mathematics Center. Pohang University of Science and Technology, 2004. 80 p. (Lecture Note Ser. 13).

67. Tietäväinen A. On the nonexistence of perfect codes over finite fields // SIAM J. Applied Math. 1973. V. 24, N 1. P. 88–96.

68. van Lint J. H. Introduction to coding theory. New York–Berlin: Springer-Verlag, 1982.

69. White H. S., Cole F. N. Cummings L. D. Complete classification of triad systems on fifteen elements // Memoirs Nat. Acad. Sci. USA. 1919. V. 14. P. 1–89.

Адрес автора:

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

Статья поступила
9 марта 2006 г.