О системах четверок Штейнера малого ранга, вложимых в расширенные совершенные коды

Д. И. Ковалевская [1]
Институт математики им. С. Л. Соболева
daryik@rambler.ru

Ф. И. Соловьева [2]
Институт математики им. С. Л. Соболева
Новосибирский Государственный Университет
sol@math.nsc.ru

Аннотация

Известно, что кодовые слова веса 4 расширенного совершенного кода, содержащего нулевой вектор, образуют систему четверок Штейнера. В работе показано, что система четверок Штейнера порядка 2^t, полученная методом свитчингов из Хэмминговой системы четверок Штейнера, вложима в расширенный совершенный код, построенный методом свитчингов $ijkl$-компонент из двоичного расширенного кода Хэмминга.

1 Введение

Пусть F^n – n-мерное метрическое пространство над полем Галуа $GF(2)$ с метрикой Хэмминга. *Двоичным кодом* длины n называется произвольное подмножество метрического пространства F^n. *Параметры* произвольного двоичного кода C из F^n обозначаются через $(n, |C|, d)$, где n – длина кодовых слов (элементов кода), $|C|$ – мощность кода, d – кодовое расстояние (т.е. минимальное хэммингово расстояние между кодовыми словами). Двоичный код C длины n с расстоянием $d = 2d' + 1$ называется *совершенным*, если для любого $x \in F^n$ существует единственный x' из C, такой, что расстояние Хэмминга $d(x, x') = (d-1)/2$. Известно (см [1]), что нетривиальный двоичный совершенный код, исправляющий одну ошибку (упоминаемый далее как совершенный), существует тогда и только тогда, когда $n = 2^t - 1$ для некоторого t.

Если V – множество, состоящее из v элементов, то t-(v, k, λ)-*схемой* называется такое размещение v различных элементов по блокам, что каждый блок содержит точно k различных элементов, любое t-элементное подмножество из V появляется точно в λ блоках. *Системой троек Штейнера порядка* v (обозначим ее $STS(v)$) и *системой четверок Штейнера порядка* v (обозначаемой как $SQS(v)$) называются 2-$(v, 3, 1)$ и 3-$(v, 4, 1)$ схемы соответственно. Известно (см. [2]), что система четверок $SQS(m)$ существует тогда и только тогда, когда $m \equiv 2, 4 (mod\ 6)$.

Пусть $\bar{C}$ – *расширенный совершенный код* длины $n = 2^t$, полученный из совершенного кода C длины $2^t - 1$ добавлением общей проверки на четность. Далее

[1]Работа выполнена при поддержке гранта Президента РФ для молодых российских ученых (грант МК-1700.2011.1)

[2]Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (проект 10-01-00424-а).

будем рассматривать только расширенные совершенные коды, содержащие нулевой вектор. Известно (см [1]), что кодовые слова веса 3 в коде C образуют систему троек Штейнера $STS(2^t-1)$, а кодовые слова веса 4 в коде $\bar{C}$ образуют систему четверок Штейнера $SQS(2^t)$.

Говорят (см. [3]), что код $C' = (C \backslash M) \cup M'$ получен *свитчингом* множества M на множество M' в двоичном коде C, если код C' имеет те же параметры, что и C. Такое множество M называется *i-компонентой* кода C, если $M' = M \oplus e_i$ для некоторого $i \in \{1, 2, \ldots, n\}$, где e_i – вектор веса 1 с единицей в i-ой координатной позиции. *Рангом* кода C называется размерность линейного подпространства пространства F^n, образованного векторами из C.

Существует множество открытых вопросов, касающихся систем троек и систем четверок Штейнера. В том числе – проблема классификации систем троек и четверок Штейнера, проблема вложимости произвольной системы троек (четверок) Штейнера в совершенный (расширенный совершенный) код. В работе [4] П. Р. Остергардом и О. Поттоненом доказано, что только 33 из 80 неизоморфных систем троек Штейнера порядка 15 являются вложимыми в совершенный код, и только 15590 из 1054163 систем четверок Штейнера порядка 16 вложимы в расширенный совершенный код.

Известно, что ранг системы троек Штейнера $STS(2^t-1)$ больше либо равен 2^t-t-1, ранга кода Хэмминга, см. [5]. Ранг системы четверок Штейнера $SQS(2^t)$ также не меньше, чем 2^t-t-1 (см. [6]). В статье [7] В. Д. Тончевым найдена нижняя оценка числа различных систем троек Штейнера порядка 2^t-1 ранга 2^t-t, что на 1 превышает минимально возможный ранг. Тем же автором в работе см. [8] приведена аналогичная формула для числа различных систем четверок Штейнера порядка 2^t ранга 2^t-t. В работе [9] В. А. Зиновьевым и Д. В. Зиновьевым приведен метод построения систем четверок Штейнера порядка $N=2^t$ произвольного ранга, а также найдена нижняя оценка числа всех различных систем четверок Штейнера $SQS(2^t)$ ранга не более 2^t-t+1, построенных с помощью этого метода из системы четверок Штейнера порядка $N/4$ ранга 2^t-t-1:

$$6^{N(N-4)/2^5} \cdot (3^3 \cdot 2^{11})^{N(N-4)(N-8)/(3 \cdot 2^9)}. \qquad (1)$$

В [10] показано, что известный класс систем троек Штейнера порядка 2^t-1, полученный свитчингами Пэш-конфигураций, вложим в класс совершенных кодов, построенных методом ijk-компонент, и приведена нижняя оценка числа систем троек Штейнера порядка 2^t-1 ранга не более 2^t-t+1.

В данной работе для полноты изложения приводится конструкция системы четверок Штейнера $SQS(N)$ (модификация конструкции Ханани), построенная из произвольной системы четверок Штейнера $SQS(m)$, $m=2^t$, $N=4m$. Разбиение такой $SQS(N)$ на определенного вида компоненты соответствует некоторому разбиению на $ijkl$-компоненты расширенного совершенного кода, и такая система четверок Штейнера вложима в расширенный совершенный код, построенный известным методом $ijkl$-компонент. Приведена нижняя оценка числа различных систем четверок Штейнера $SQS(N)$ ранга не более $N-log(N)+1$, вложимых в расширенный совершенный код.

2 Системы четверок Штейнера SQS(4m), вложимые в расширенный совершенный код

В данном разделе рассмотрим конструкцию системы четверок Штейнера $SQS(4m)$ порядка $4m$, которая строится из системы четверок Штейнера $SQS(m)$ порядка m с помощью конструкции Ханани (см. [11]). Из конструкции будет следовать, что некоторые такие $SQS(4m)$ вложимы в расширенный совершенный код.

Пусть $M = \{1, 2, 3, \dots, m\}$ – множество мощности m, на котором задана произвольная система четверок Штейнера $SQS(m)$, $m \equiv 2, 4(mod\ 6)$. Для построения системы четверок Штейнера порядка $4m$ на множестве элементов $M \bigcup \{i_1, \dots, i_m, j_1, \dots, j_m, k_1, \dots, k_m\}$, в дальнейшем упоминаемой как Q_N, где $N = 4m$, рассмотрим следующую таблицу:

$$T_M = \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & \dots & \mathrm{m} \\ \hline i_1 & i_2 & i_3 & \dots & i_m \\ \hline j_1 & j_2 & j_3 & \dots & j_m \\ \hline k_1 & k_2 & k_3 & \dots & k_m \\ \hline \end{array}$$

Сначала рассмотрим, как строится $SQS(4m)$ в самом частном случае, когда $m = 4$. Пусть, например, $SQS(4) = \{(a, b, c, d)\}$. В этом случае система четверок Штейнера $SQS(4m)$ имеет порядок 16, и таблица T_M принимает вид

a	b	c	d
i_a	i_b	i_c	i_d
j_a	j_b	j_c	j_d
k_a	k_b	k_c	k_d

Обозначим полученную таблицу через T_{abcd}. Для построения $SQS(16)$ воспользуемся конструкцией Ханани. Включим в нее все строки и столбцы таблицы T_{abcd}, четверки конструкции Ханани вида

(2)

примененные к каждой паре строк и столбцов, и все миноры второго порядка, т.е. элементы вида

$$(h_1, h_2, t_{h_1}, t_{h_2}), (t1_{h_1}, t1_{h_2}, t2_{h_1}, t2_{h_2}), t, t_1, t_2 \in \{i, j, k\}, h, h_1, h_2 \in \{a, b, c\}. \qquad (3)$$

Кроме того, в $SQS(16)$ добавим всевозможные сочетания элементов, находящихся в разных строках и столбцах таблицы T_{abcd}, т.е. множество вида

$$\begin{aligned} \{&(a, i_b, j_c, k_d), (a, i_b, j_d, k_c), (a, i_c, j_b, k_d), (a, i_d, j_b, k_c), (a, i_c, j_d, k_b), (a, i_d, j_c, k_b), \\ &(b, i_a, j_c, k_d), (b, i_a, j_d, k_c), (b, i_c, j_a, k_d), (b, i_d, j_a, k_c), (b, i_c, j_d, k_a), (b, i_d, j_c, k_a), \\ &(c, i_a, j_b, k_d), (c, i_a, j_d, k_b), (c, i_b, j_a, k_d), (c, i_d, j_a, k_b), (c, i_b, j_d, k_a), (c, i_d, j_b, k_a), \\ &(d, i_a, j_b, k_c), (d, i_a, j_c, k_b), (d, i_b, j_a, k_c), (d, i_c, j_a, k_b), (d, i_b, j_c, k_a), (d, i_c, j_b, k_a)\} \end{aligned} \qquad (4)$$

Общее количество получившихся четверок равно $4+4+2\cdot 6\cdot C_4^2+6\cdot C_4^2+4\cdot 6 = = 140$, что совпадает с количеством четверок в $SQS(16)$. Из построения $SQS(16)$ видно, что каждая неупорядоченная тройка элементов содержится в единственном блоке. Таким образом, построена $SQS(16)$ из $SQS(4)$.

Пусть m – произвольное, такое что существует $SQS(m), m \equiv 2,4(mod\ 6)$. Тогда в Q_N включим все столбцы, а также для любой пары столбцов – все миноры вида (3) и блоки конструкции Ханани (2). Таким образом, получим $m+6\cdot C_m^2+6\cdot C_m^2 = m+6m(m-1)$ четверок. Далее, для любой четверки (a,b,c,d) из $SQS(m)$ рассмотрим подматрицу T_{abcd}. Для этой матрицы в Q_N включим (a,b,c,d), оставшиеся строки, блоки конструкции Ханани вида (2), примененные к каждой паре строк, а также четверки вида (4).

Нетрудно видеть, что каждой матрице вида T_{abcd} соответствуют $1+3+6\cdot C_4^2+4\cdot 6 = 64$ четверок в Q_N. Количество таблиц совпадает с количеством четверок в $SQS(m)$ и равно $m(m-1)(m-2)/24$. Следовательно, общее количество четверок в конструкции равно $m+6m(m-1)+64\cdot m(m-1)\cdot(m-2)/24 = 4m(4m-1)\cdot \cdot(4m-2)/24 = |Q_N|$.

Из построения множества четверок легко видеть, что каждая неупорядоченная тройка элементов встречается ровно в одной четверке. Таким образом, построена система четверок Штейнера Q_N порядка $N=4m$ из системы четверок Штейнера $SQS(m)$ порядка m.

Теорема 1. *Из произвольной системы четверок Штейнера порядка m можно построить систему четверок Штейнера порядка $4m$.*

Если M – i-компонента совершенного кода C длины n, содержащего нулевой вектор, то $\bar{M}$ будем называть *il-компонентой расширенного совершенного кода* $\bar{C}$ длины $N=n+1$. Если же $\bar{M}$ является il, jl и kl-компонентой расширенного совершенного кода $\bar{C}$, то $\bar{M}$ называется *$ijkl$-компонентой расширенного совершенного кода $\bar{C}$.*

Известно, что справедлива следующая теорема.

Теорема 2. *(См. [12]) Всякий расширенный совершенный двоичный код Хэмминга длины N можно представить в виде объединения непересекающихся $ijkl$-компонент R^t_{ijkl}, каждая из которых, в свою очередь, может быть представлена как объединение непересекающихся il-компонент R^{pt}_{il}:*
$\mathcal{H}^N = \bigcup_{t=1}^{N_2} R^t_{ijkl} = \bigcup_{t=1}^{N_2}\bigcup_{p=1}^{N_1} R^{pt}_{il}$, *где* $N_1 = 2^{(N-4)/4}$, $N_2 = 2^{(N+4)/4-logN}$.

Эти разбиения позволяют делать свитчинги расширенного кода Хэмминга и в результате получить широкий класс расширенных совершенных кодов.

Систему четверок Штейнера порядка N, соответствующую двоичному расширенному коду Хэмминга $\mathcal{H}^N$, будем называть *Хэмминговой системой четверок Штейнера $SQS(\mathcal{H}^N)$.*

Множество Q называется *il-компонентой Хэмминговой системы четверок Штейнера $SQS(\mathcal{H}^N)$*, если Q – подмножество векторов веса 4 из il-компоненты расширенного кода Хэмминга $\mathcal{H}^N$ длины N. Если же il-компонента системы четверок Штейнера Q является также jl-компонентой и kl-компонентой, то Q называется *$ijkl$-компонентой Хэмминговой системы четверок Штейнера $SQS(\mathcal{H}^N)$.*

Утверждение 1. *Хэммингова система четверок Штейнера $SQS(\mathcal{H}^N)$ представима в виде объединения подмножеств $1 + N(N-4)(N-8)/(3 \cdot 2^9)$ непересекающихся $ijkl$-компонент, каждая из которых, в свою очередь, является объединением подмножеств $N/4 + (N-4)(N-8)/2^5$ либо 8 непересекающихся il-компонент.*

Рассмотрим систему четверок Штейнера $SQS(m)$ и построенную из нее по Теореме 1 систему четверок Штейнера Q_N. Заметим, что если $SQS(m)$ является Хэмминговой системой четверок Штейнера $SQS(\mathcal{H}^m)$, то система Q_N является Хэмминговой системой четверок Штейнера $SQS(\mathcal{H}^N)$. Справедлива

Теорема 3. *Система четверок Штейнера, полученная методом свитчингов $ijkl$-компонент из системы $SQS(\mathcal{H}^N)$, является вложимой в совершенный код, полученный из кода Хэмминга $\mathcal{H}^N$ методом свитчингов $ijkl$-компонент.*

Приведем нижнюю оценку числа различных систем четверок Штейнера порядка N ранга не более $N - logN + 1$, вложимых в расширенный совершенный код, построенный методом свитчингов $ijkl$-компонент. Число таких систем четверок Штейнера обозначим через $R(N)$. Справедлива

Теорема 4. *Число $R(N)$ различных систем четверок Штейнера $SQS(N)$ порядка N ранга не более $N - logN + 1$, вложимых в расширенный совершенный код, не меньше, чем*

$$(3^2 \cdot 2^8 - 8)^{N(N-4)(N-8)/(3 \cdot 2^9)} \cdot 2^{N(N-4)/2^5} \cdot \frac{N(N-1)(N-2)}{2^3} \cdot D(N/4),$$

где $D(N/4)$ – число различных Хэмминговых систем четверок Штейнера порядка $N/4$.

Полученная оценка меньше (1), и вопрос о том, все ли такие системы четверок Штейнера из [9] являются вложимыми в расширенные совершенные коды, остается открытым.

Список литературы

[1] *Ф. Дж. Мак-Вильямс, Н. Дж. Слоэн.* "Теория кодов, исправляющих ошибки": Пер. с англ. М.: Связь. 1979. 744 с.

[2] *М. Холл.* "Комбинаторика": Пер. с англ. М.: Мир. 1970. 424 с.

[3] *Ф. И. Соловьева.* "Введение в теорию кодирования": Учеб. пособие // Новосиб. гос. ун-т. Новосибирск, 2006. 124 с.

[4] *P. R. Östergård, O. Pottonen* The Perfect Binary One-Error-Correcting Codes of Length 15: Part 1 – Classification. // IEEE Trans. Inform. Theory. 2009. № 55. P. 4657–4660.

[5] *J. Doyen, X. Hubaut, M. Vandensavel* Ranks of incidence matrices of Steiner triple systems. // Math. 1978. S. Z. № 163. P. 251–259.

[6] *L. Teirlinck* On projective and affine hyperplanes. // J Combin. Theory. 1980. S. A. № 28. P. 290–306.

[7] *V. D. Tonchev.* A mass formula for Steiner triple systems $STS(2^n - 1)$ of 2-rank $2^n - n$. // Journal of Combin. Theory. 2001. Series A **95**, P. 197–208.

[8] *V. D. Tonchev.* A formula for the number of Steiner quadruple systems on 2^n points of 2-rank $2^n - n$. // Journal of Combin. Designs. 2003. № 11. P. 260–274.

[9] *В. А. Зиновьев, Д. В. Зиновьев.* О разрешимости систем Штейнера $S(v = 2^m, 4, 3)$ ранга $r \leq v - m + 1$ над F^2. // Пробл. передачи информ. 2007. Т. 43. Вып. 1. С. 39–55.

[10] *Е. С. Глухих.* Вложимость систем троек Штейнера в совершенные коды. // Магистерская диссертация. Новосибирск. 2005.

[11] *H. Hanani.* The Existence and Construction of Balanced Incomplete Block Designs. // Ann. Math. Statist. 1961. V. 32, № 2 P. 361–386.

[12] *С. В. Августинович, Ф. И. Соловьева.* Построение совершенных двоичных кодов последовательными сдвигами $\tilde{\alpha}$-компонент. // Пробл. передачи информ. 1997. Т. 33. Вып. 3. С. 15–21.