УДК 519.725

Э. М. Габидулин, Н. И. Пилипчук

Московский физико-технический институт (государственный университет)

Эффективность подпространственных сетевых кодов

Рассмотрены конструкции подпространственных сетевых кодов Силвы–Кётера–Кшишанга (SKK-коды)и многокомпонентных кодов с нулевым префиксом (МНП-коды) Габидулина–Боссерта. Определены оптимальные параметры МНП кодов и приведена верхняя граница мощности подпространственных сетевых кодов. Проведён анализ мощности этих кодов и сравнение с верхней границей мощности. Показано, что мощность МНП-кодов больше мощности SKK-кодов при любых параметрах. Оценена эффективность кода в виде отношения мощности конкретного кода к максимальной мощности, определяемой верхней границей.

Ключевые слова: ранговые коды, подпространственные коды, мощность кода, кодовое расстояние, размерность, многокомпонентные коды

1. Введение

Прежде всего введём обозначения и определения. Пусть $W = GF(q)^n$ — основное n-мерное пространство над конечным полем $GF(q)$. $W(n,m)$ — множество всех m-мерных подпространств основного пространства W, называемое грассманианом.

$$|W(n,m)| = \begin{bmatrix} n \\ m \end{bmatrix} = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{m-1})}{(q^m-1)(q^m-q)\dots(q^m-q^{m-1})}.$$

Грассманово расстояние между двумя подпространствами $U, V \in W(n,m)$ определено следующим образом:

$$\begin{aligned} d_{sub}(U,V) &= \dim(U \uplus V) - \dim(U \cap V) = \\ &= \dim(U) + \dim(V) - 2\dim(U \cap V) = \\ &= 2m - 2\dim(U \cap V) = 2\delta. \end{aligned}$$

Обозначим $[n, M, d_{sub} = 2\delta, m]$ некоторый код в грассмановой метрике, у которого n — длина кодовых слов, M — число кодовых слов, d_{sub} — минимальное кодовое расстояние, m — размерность.

Верхняя граница мощности грассмановых кодов получена в 2003 году [1]:

$$M_{\max} \leqslant \frac{|W(n, m-\delta+1)|}{|W(m, m-\delta+1)|} = \frac{\begin{bmatrix} n \\ m-\delta+1 \end{bmatrix}}{\begin{bmatrix} m \\ m-\delta+1 \end{bmatrix}}.$$

Асимптотическая форма этой границы имеет вид

$$M_{\max} \leqslant q^{(N-m)(m-\delta+1)} + q^{(N-m)(m-\delta+1)-\delta}(1+O(1)).$$

На рис. 1 показана зависимость мощности кода от его длины для размерностей $m = 3$ и $m = 4$.

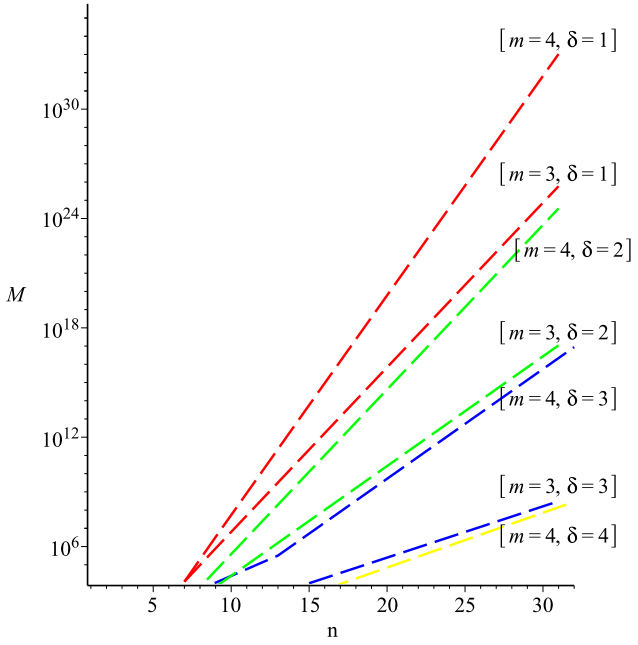

Рис. 1. Зависимость мощности кода от длины

Приведём расчёты верхней границы при заданных параметрах n, δ, m, где $n \geq 2m$.

Таблица 1

Верхняя граница мощности кода, $m = 3$

n	7	9	15	30
$M_{\max},\ \delta = 1$	11811	788035	$2.09 \cdot 10^{11}$	$7.4 \cdot 10^{24}$
$M_{\max},\ \delta = 2$	381	6205	$2.60 \cdot 10^{7}$	$2.7 \cdot 10^{16}$
$M_{\max},\ \delta = 3$	18	73	4681	$1.5 \cdot 10^{8}$

Таблица 2

Верхняя граница мощности кода, $m = 4$

n	7	8	9	15	16	30
$M_{\max},\ \delta = 1$	11811	200787	$3.3 \cdot 10^{7}$	$5.7 \cdot 10^{13}$	$9 \cdot 10^{14}$	$6.6 \cdot 10^{31}$
$M_{\max},\ \delta = 2$	787	6477	52535	$1.3 \cdot 10^{10}$	$1.1 \cdot 10^{11}$	$4.9 \cdot 10^{23}$
$M_{\max},\ \delta = 3$	76	308	1241	$5.1 \cdot 10^{6}$	$2.0 \cdot 10^{7}$	$5.5 \cdot 10^{15}$
$M_{\max},\ \delta = 4$	$- - -$	17	34	2184	4369	$7.2 \cdot 10^{7}$

Как видно из рисунка и расчётов, $M_{\max}$ растёт с ростом длин n. Кроме того, чем больше размерность m, тем больше мощность $M_{\max}$ при том же кодовом расстоянии δ. Чем больше δ, тем меньше $M_{\max}$ при том же m и фиксированном n.

В настоящее время известны подпространственные коды большой мощности. К ним относится случайный сетевой код (SKK-код), разработанный тремя авторами – Силвой, Кёттером, Кшишангом [2–3], многокомпонентный код с нулевым префиксом ($МНП$-код), предложенный Габидулиным и Боссертом 2008 году [4–5] и дополненный оптимизацией параметров в 2012 году [6]. Кроме того, разработан Шишкиным многокомпонентный код [7], основанный на лексикографическом принципе и оптимизации с отбраковкой. Имеются

также отдельные примеры подпространственных сетевых кодов, использующих в качестве основы ранговый код Габидулина [8] и так называемые диаграммы Феррера [9–10]. Однако отдельные примеры не дают возможности определить мощность кодов при всех возможных значениях параметров, поэтому здесь ограничимся анализом характеристик SKK- и $МНП$-кодов.

2. Случайный сетевой код SKK

Кодовая матрица SKK-кода имеет вид

$$\mathcal{C} = \{[I_m \quad M]\},$$

где I_m – единичная матрица, M – матрица рангового кода над базовым полем $GF(q)$.

Мощность этого кода такова:

$$M_{skk} = q^{k(n-m)}, \text{ где } k = m - \delta + 1.$$

Зависимость от длины кода показана на рис. 2.

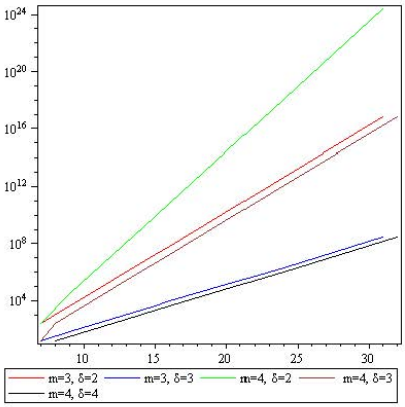

Рис. 2. Мощность кодов SKK в зависимости от длины кода

3. Многокомпонентный сетевой код *МНП*

3.1. Структура кода

В 2008 году Габидулиным и Боссертом предложен многокомпонентный сетевой код: это код с нулевым префиксом (*МНП*-код) [4–5].

Пусть M_i, $i = 1, \ldots, r$ – кодовая матрица i-й компоненты. Компоненты имеют следующую структуру:

$$\begin{aligned} M_1 &= I_m M_1, \\ M_2 &= O_m^\delta I_m M_2, \\ &\ldots \\ M_r &= O_m^\delta O_m^\delta \ldots O_m^\delta I_m M_r, \end{aligned}$$

где первая компонента M_1 – это SKK-код. Как видно из этой структуры, перед каждой следующей компонентой появляется матрица из m-строк и δ-столбцов, состоящая из одних нулевых элементов. В результате число столбцов матрицы рангового кода уменьшается на δ.

3.2. Мощность кода

Благодаря тому, что все эти компоненты в подпространственном смысле ортогональны, общая мощность многокомпонентного кода равна сумме мощностей всех r кодовых компонент M_i, $i = \overline{1,r}$.

Зафиксируем параметры n, m, δ и подсчитаем мощность.

Мощность *МНП*-кода состоит из трёх частей:

$$M_{МНП} = M_{skk} + S_1 + S_2 + 1,$$

где

$$S_1 = \sum_{i=1}^{s_1} 2^{k(n-m-i\delta)},$$

$$S_2 = \sum_{i=1}^{s_2} 2^{k_i m}.$$

Здесь M_{skk} – мощность первой компоненты, S_1 – суммарная мощность компонент, начиная со второй до s_1-й, S_2 – суммарная мощность компонент, начиная с $((s_1)+1)$-й до последней компоненты. Параметры s_1, s_2, k_i выбираем в соответствии с алгоритмом построения кода: s_1-й сдвиг длин кодовых слов происходит при выполнении условия $n-m-s_1\delta = m+\gamma$, где $0 \le \gamma \le \delta - 1$. Так что $s_1 = \frac{n-2m-\gamma}{\delta}$. Далее происходит уменьшение длины на δ $(m+\gamma-\delta < m)$ и транспонирование кодовой матрицы.

Теперь сторона длины $m+\gamma-\delta$ – размерность, которая уменьшается на δ на каждом шаге. Множитель в показатели степени $k_i = (m+\gamma-i\delta)-\delta+1$.

Параметр s_2 определим из условий

$$\delta \le m+\gamma-s_2\delta \text{ и } m+\gamma-(s_2+1)\delta < \delta:$$

$$\frac{m+\gamma-2\delta}{\delta} < s_2 \le \frac{m+\gamma-\delta}{\delta}.$$

Пример 1. Пусть $n = 70$, $m = 15$, $\delta = 3$. Здесь $\gamma = 1$. $s_1 = \frac{n-2m-\gamma}{\delta} = \frac{70-30-1}{3} = 13$ $\frac{15+1-6}{3} < s_2 \le \frac{15+1-3}{3}$

С учётом целочисленности получаем $s_2 = 4$. Мощность этого МНП-кода равна

$$M_{МНП} = 2^{13\cdot 55} + \sum_{i=1}^{13} 2^{13(55-3i)} + \sum_{i=1}^{4} 2^{15(14-3i)} + 1.$$

Функция разности мощностей $\Delta M = M_{МНП} - M_{skk}$ в зависимости от n при фиксированных параметрах m и δ представлена на рис. 3. Из рисунка видно, что функция ΔM растет при увеличении n и зависит от m и δ.

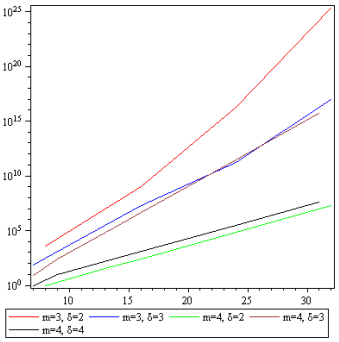

Рис. 3. Функция ΔM в зависимости от длины кода

3.3. Оптимальность кода *МНП*

Доказано [6], что *МНП*-код имеет максимальную мощность при следующих параметрах: $\delta = m$ и $n = lm$.

$$M_{\max} = \frac{q^n - 1}{q^m - 1} = \frac{q^{lm} - 1}{q^m - 1}, \tag{1}$$

где l – целое число. Если $n = lm + s$, $1 \leqslant s < m$, то мощность этого кода выражается формулой

$$M = q^{(l-1)m+s} + q^{(l-2)m+s} + \cdots + q^{m+s} + 1. \tag{2}$$

Пример 2. Рассмотрим два случая. Пусть $\delta = m = 4$ и $n = 15$, $s = 3$. Используем формулу (2) и получаем

$$M = 2^{(3-1)4+3} + 2^{(3-2)4+3} + 1 = 2177. \tag{3}$$

Верхняя граница в этом случае даёт значение $M_{\max}$=2184, то есть относительная разность равна $\frac{M_{\max}-M}{M_{\max}}$=0.0032. Пусть $\delta = m = 4$ и $n = 17$, $s = 1$. Используем формулу (2) и получаем

$$M = 2^{(4-1)4+1} + 2^{(4-2)4+1} + 2^{(4-3)4+1} + 1 = 8737. \tag{4}$$

Верхняя граница в этом случае даёт значение $M_{\max}$=8738, то есть $\frac{M_{\max}-M}{M_{\max}}$=0.0000114. В обоих случаях оценка по формуле (2) близка к верхней границе (1).

4. Эффективность SKK- и МНП-кодов

Определим эффективность кодов в виде отношения мощности данного кода к максимальной мощности, определяемой верхней границей, при фиксированных параметрах n, m, δ:

$\eta_{skk} = \frac{M_{skk}}{M_{\max}}$ – эффективность SKK-кода;

$\eta_0 = \frac{M_{МНП}}{M_{\max}}$ – эффективность *МНП*-кода.

Приведём расчёт эффективности этих кодов при фиксированном $n = 16$ и различных значениях параметров m, δ.

Таблица 3

Длина кода $n = 16$, расстояние $\delta = 2$

m	2	3	4	5	6	7	8
η_{skk}	0.750	0.656	0.615	0.596	0.587	0.583	0.581
η_0	1.000	0.700	0.625	0.598	0.587	0.583	0.581

Таблица 4

Длина кода $n = 16$, расстояние $\delta = 3$

m	2	3	4	5	6	7	8
η_{skk}	-	0.875	0.820	0.794	0.782	0.777	0.774
η_0	–	1.000	0.823	0.796	0.782	0.777	0.774

Таблица 5

Длина кода $n = 16$, расстояние $\delta = 4$

m	2	3	4	5	6	7	8
η_{skk}	–	–	0.938	0.908	0.894	0.887	0.887
η_0	–	–	1.000	0.912	0.908	0.887	0.887

Таблица 6

Длина кода $n = 16$, расстояние $\delta = 5$

m	2	3	4	5	6	7	8
η_{skk}	–	–	–	0.969	0.954	0.946	0.942
η_0	–	–	–	0.999	0.954	0.946	0.942

Таблица 7

Длина кода $n = 16$, расстояние $\delta = 6$

m	2	3	4	5	6	7	8
η_{skk}	–	–	–	–	0.984	0.977	0.973
η_0	–	–	–	–	0.985	0.977	0.973

Таблица 8

Длина кода $n = 16$, расстояние $\delta = 7$

m	2	3	4	5	6	7	8
η_{skk}	–	–	–	–	–	0.992	0.988
η_0	–	–	–	–	–	0.994	0.988

Таблица 9

Длина кода $n = 16$, расстояние $\delta = 8$

m	2	3	4	5	6	7	8
η_{skk}	–	–	–	–	–	–	0.996
η_0	–	–	–	–	–	–	1.000

Приведённые расчёты показали,что эффективность *МНП*-кода всегда больше или в некоторых случаях (при заданной точности 3 знака после запятой) равна эффективности SKK-кода. При условии $m = \delta$ и $\frac{n}{m}$ – целом эффективность *МНП*-кода равна 1, то есть совпадает с верхней границей.

5. Заключение

- Проанализирована верхняя граница мощности подпространственных кодов в зависимости от основных параметров. Показано, что мощность увеличивается при увеличении длины, а также размерности кода и уменьшается при увеличении кодовых расстояний.

- В качестве нижней границы предложено использовать мощность многокомпонентного кода с нулевым префиксом (*МНП*-кода) Габидулина – Боссерта. Мощность *МНП*-кода больше мощности случайного сетевого кода Силвы–Кёттера–Кшишанга (SKK-кода)при всех значениях основных параметров. В случаях равенства кодовых расстояний и размерностей мощность *МНП*-кода практически (в некоторых случаях точно) совпадает с верхней границей мощности.

- Оценена эффективность кодов SKK и *МНП* и приведены расчёты эффективности (с точностью до третьего знака после запятой) для следующих параметров: $n = 16$, $m = 2, 3, 4, 5, 6, 7, 8$, $\delta = 2, 3, 4, 5, 6, 7, 8$, где $n \geq 2m$. Показано, что при такой точности и больших размерностях эффективность SKK-кода и *МНП*-кода практически одинакова. Так что в этих случаях можно использовать мощность любого из рассматриваемых кодов в качестве нижней границы мощности подпространственных сетевых кодов.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект № 15-07-08480 А.

Литература

1. *Wang H., Xing C., Safavi-Naini R.* Linear Authentication Codes: Bounds and Constructions // IEEE Trans. Inform. Theory. — 2003. V. 49, N 4. P. 866–873.
2. *Koetter R., Kschischang F.R.* Coding for Errors and Erasures in Random Network Coding // IEEE Trans. Inform. Theory. 2008. — V. 54, N 8. — P. 3579–3591.
3. *Silva D., Kschischang F.R., Koetter R.* A Rank-Metric Approach to Error Control in Random Network Coding // IEEE Trans. Inform. Theory. — 2008. — V. 54, N 9. — P. 3951–3967.
4. *Gabidulin E., Bossert M.* Codes for Network Coding // Proceedings of the Int. Sympos. on Information Theory. (ISIT'2008). — 2008.— P. 867–870.
5. *Габидулин Э.М., Боссерт М.* Алгебраические коды для сетевого кодирования // Проблемы передачи информации. — 2009. Т. 45, вып. 4. — С. 3–18.
6. *Pilipchuk N., Gabidulin E., Afanasiev V.* Decoding multicomponent codes based on rank subcodes // Proceedings of the Int. Workshop. on Algebraic and Combinatorial Coding Theory (ACCT'2012). — 2012. P. 275–281.
7. *Shishkin А.Л., Gabidulin E.M., Pilipchuk N.I.* On cardinality of network subspace codes // Proceeding of the Fourteenth Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XIV). — 2014.— P. 300–306.
8. *Габидулин Э. М.* Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. —1985. — Т. 21, вып. 1. С. 1–12.
9. *Etzion T., Silberstein N.* Error-Correcting Codes in Projective Spaces via Rank-Metric Codes and Ferrers Diagrams // IEEE Transactions on Information Theory. — 2011. — V. 55, N 7. — P. 2909–2919.
10. *Etzion T., Silberstein N.* Large Constant Dimension Codes and Lexicodes // Advances in Mathematics of Communications. — 2011. — V. 5, N 2. — P. 177–189.

References

1. *Wang, H., Xing, C., Safavi-Naini, R.* Linear Authentication Codes: Bounds and Constructions. IEEE Trans. Inform. Theory. 2003. V. 49. N 4. P. 866–873.
2. *Koetter, R., Kschischang, F.R.* Coding for Errors and Erasures in Random Network Coding. IEEE Trans. Inform. Theory. 2008. V. 54. N 8. P. 3579–3591.
3. *Silva, D., Kschischang, F.R., Koetter R.* A Rank-Metric Approach to Error Control in Random Network Coding. IEEE Trans. Inform. Theory. 2008. V. 54. N 9. P. 3951–3967.
4. *Gabidulin, E., Bossert, M.* Codes for Network Coding // Proc. 2008 IEEE Int. Sympos. on Information Theory. (ISIT'2008). Toronto, Canada July 6-11, 2008. P. 867-870.
5. *Gabidulin, E., Bossert, M.* Algebraic codes for network coding. Probl. Inform. Transm. 2009. V 45, N 4. P. 3–18. (in Russian).
6. *Pilipchuk N., Gabidulin E., Afanasiev V.* Decoding multicomponent codes based on rank subcodes. Proceedings of the Int. Workshop. on Algebraic and Combinatorial Coding Theory (ACCT'2012). 2012. P. 275–281.

7. *Shishkin A., Gabidulin E.M., Pilipchuk N. I.* On cardinality of network subspace codes. Proceed. Fourteenth Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XIV). Svetlogorsk(Kaliningrad region), Russia September 7–13, 2014. P. 300–306.

8. *Gabidulin E.M.* Theory of codes with maximum rank distance. Probl. Inform. Transm. 1985. V.21. N 1. P. 1–12. (in Russian).

9. *Etzion T., Silberstein N.* Error-Correcting Codes in Projective Spaces via Rank-Metric Codes and Ferrers Diagrams. IEEE Transactions on Information Theory. 2011. V. 55, N 7. P. 2909–2919.

10. *Etzion T., Silberstein N.* Large Constant Dimension Codes and Lexicodes. Advances in Mathematics of Communications. 2011. V. 5, N 2. P. 177–189.

Поступила в редакцию 04.03.2015.