УДК 519.725

Э. М. Габидулин, Н. И. Пилипчук

Московский физико-технический институт (государственный университет)

Оптимальные и субоптимальные подпространственные коды-спреды

Работа посвящена подпространственным кодам с максимальным кодовым расстоянием, которые называются спредами. Представлены конструкции многокомпонентных кодов с нулевым префиксом (МНП) и оценены их мощности. Показано, что при определённых условиях мощность МНП кодов-спредов достигает верхней границы, в других случаях находится вблизи верхней границы. Соответственно этим данным такие коды названы оптимальными или субоптимальными. Оценена эффективность η в виде отношения мощности кода к верхней границе. Расчёты показали, что для многих параметров субоптимальных кодов эффективность $\eta \geq 0.99$.

Ключевые слова: конечное поле, код, декодирование, пространство, подпространство, мощность кода, ранговая метрика.

E. M. Gabidulin, N. I. Pilipchuk

Moscow Institute of Physics and Technology (State University)

Optimal and suboptimal subspace codes-spreads

This paper is devoted to subspace codes with maximal code distance which are known as spreads. The multicomponent codes with zero prefix (MZP) are presented. Cardinality for different parameters is calculated. The obtained values of cardinality are compared with the upper bound. It is shown that the cardinality of MZP codes-spreads coincides with the upper bound under some conditions and near the upper bound under other conditions. In the first case they are called optimal subspace codes, in the last case they are called suboptimal subspace codes. The efficiency η of suboptimal codes is estimated as a ratio of two values which are the cardinality of the code and the upper bound. This ratio is $\eta \geq 0.99$ for many parameters.

Key words: finite field, code, decding, space, subspace, code cardinality, rank metric.

1. Введение

Введём обозначения и основные определения. Пусть $W = GF(q)^n$ – конечное n-мерное пространство над основным базовым конечным полем $GF(q)$. Пусть $W(n,m)$ – множество всех m-мерных подпространств пространства W, которое называется m-грассманнианом. Размер грассманниана определяется с помощью гауссовых целых чисел:

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

Подпространственное расстояние между двумя подпространствами $U, V \in W$ определено в виде

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

где $U \uplus V$ означает минимальное подпространство, содержащее оба подпространства U и V. Если U и V одной и той же размерности m, то подпространственное расстояние равно

$$d_{\text{sub}}(U,V) = 2(m - \dim(U \cap V)) = 2\delta,$$

где $\delta = m - \dim(U \cap V)$. Это расстояние называется грассманниановой метрикой.

Подпространственный код – это некоторое множество подпространств из пространства W. Если код состоит из подпространств m-грассманниана $W(n, m)$ с числом кодовых подпространств M, минимальным расстоянием d_{sub} и размерностью m, то он называется кодом постоянной размерности и обозначается $[n, M, d_{\text{sub}}, m]$. При максимальном кодовом расстоянии $d_{\text{sub}} = 2m$ подпространственный код называется спредом.

Далее эта статья структурирована следующим образом. В разделе 2 представлены конструкции подпространственных кодов Силвы–Коеттера–Кшишанга [1, 2] основанные на ранговых кодах Габидулина [4]. В разделе 3 описаны конструкции многокомпонентных кодов с нулевым префиксом (МНП), построенные Габидулиным и Боссертом [5, 6] и основанные на SKK кодах Силвы–Коеттера–Кшишанга. В разделе 4 приведены оценки мощности МНП-спредов для многих параметров и произведено сравнение с верхними границами мощности подпространственных кодов, полученными в работах других авторов [7–11]. В разделе 5 кратко подведены итоги этой работы.

2. Коды SKK

В работах [1, 2] Силва, Коеттер и Кшишанг подробно описали конструкцию своего подпространственного случайного кода SKK, предназначенного для работы в сети связи. Этот код состоит из множества матриц вида

$$\mathcal{C}_{\text{skk}} = \left\{ \begin{pmatrix} I_m & M_1 \end{pmatrix} \right\}, \tag{1}$$

где I_m – единичная матрица порядка m, а M_1 – кодовая матрица размера $m \times (n-m)$ из матричного рангового кода $\mathcal{M}_1$ с ранговым расстоянием $d_{\text{rank}} = \delta$ [4]. *Подпространственное расстояние* кода $\mathcal{C}_{\text{skk}}$ равно удвоенному *ранговому расстоянию* матричного кода $\mathcal{M}$: $d_{\text{sub}}(\mathcal{C}_{\text{skk}}) = 2d_{rank}(\mathcal{M}) = 2\delta$. Включение в конструкцию единичной матрицы позволило осуществлять передачу по сети с помощью случайных алгебраических комбинаций элементов конечного поля, что повысило скорость передачи [3].

Мощность кода (общее число кодовых слов) $|\mathcal{C}_{\text{skk}}|$ кода SKK равно числу кодовых слов рангового кода с ранговым расстоянием $d_{\text{rank}} = \delta$ и длиной кодовых слов $(n - m)$:

$$|\mathcal{C}_{\text{skk}}| = q^{(n-m)k}, \tag{2}$$

где $k = m - \delta + 1$, $\delta \leq m$.

Пример 1. Зададим параметры: $q = 2$, $n = 5m = 20$,$m = 4$,$n - m = 16$, $\delta = 3$, $k = m - \delta + 1 = 2$. Мощность равна

$$|\mathcal{C}_{\text{skk}}| = q^{(n-m)(m-\delta+1)} = 2^{32} = 4294967296. \tag{3}$$

Если $\delta = m$ принимает максимальное значение (в данном случае $4 = m$), то показатель степени принимает минимальное значение $k = m - m + 1 = 1$. Мощность равна $|\mathcal{C}_{\text{skk}}| = q^{(n-m)} = 2^{16} = 65536 = M_1$. Увеличение рангового расстояния на 1 (подпространственного расстояния на 2) при той же длине кода $n = 20$ привело к уменьшению показателя степени на 1, и в результате мощность стала равна двоичному корню от предыдущего значения. Увеличим длину кодовых слов вдвое ($n = 40$) при той же максимальной размерности $m = 4$. В этом случае мощность кода SKK возрастёт до $|\mathcal{C}_{\text{skk}}| = q^{(n-m)} = 2^{36} = 68719476736$. В данном случае удвоение длины привело к увеличению мощности более чем в 10^6 раз.

3. Коды МНП

В 2008 году в работе [5] Габидулин и Боссерт представили конструкции новых подпространственных кодов, названных впоследствии многокомпонентными кодами с нулевым

префиксом (МНП). С тех пор и до настоящего времени исследования на эту тему продолжаются (см., например работы [6–22]). Имеются также работы других авторов, посвящённых близким темам [23–31].

В первом описании кодов МНП были приняты следующие параметры: $n = rm$, $\delta = m$, то есть подпространственное расстояние $d_{sub} = 2m$ максимально. В последующих работах при $\delta \leq m$ набор параметров расширился.

Рассмотрим конструкцию кода при следующих параметрах: $n = m + r\delta + s$ – длина кодовых слов, где m – размерность, r – целое число, $r \geqslant 1$ и $0 \leqslant s \leqslant \delta - 1$. Первая компонента кода МНП – код SKK. Матрица этой компоненты состоит из конкатенации двух матриц – единичной матрицы и матрицы рангового кода.

Другие компоненты при $i \geq 2$ состоят из матриц вида

$$\mathcal{C}_{mzp\,i} = \left\{ \left(\begin{array}{ccccc} 0_m^\delta & \dots & 0_m^\delta & I_m & M_i \end{array} \right) \right\}.$$

Начиная со второй компоненты, в качестве префикса стоит матрица из одних нулей размера $m \times \delta$, в каждой последующей компоненте число таких матриц увеличивается на одну, за нулевым префиксом следует единичная матрица порядка m и матрица рангового кода. Нулевые матрицы обеспечивают подпространственное расстояние между компонентами, равное 2δ. В ранговом коде задано ранговое расстояние δ.

Мощность i-й компоненты равна

$$|M_i| = q^{kn_i}, \tag{4}$$

где длина кодовых слов рангового кода i-й компоненты равна $n_i = (r - (i-1)\delta) + s$ При $m < n_i < m + \delta$ строим последнюю компоненту в виде

$$\mathcal{C}_{mzp\,l} = \left(\begin{array}{cccccc} 0_m^\delta & 0_m^\delta & \dots & 0_m^\delta & I_m \end{array} \right).$$

Последняя компонента содержит одну кодовую матрицу-конкатенацию нулевой матрицы размера $m \times (n-m)$ и единичной матрицы порядка m. Так как компоненты не пересекаются, то мощность $|M_{mzp}|$ многокомпонентного кода равна сумме мощностей всех компонент:

$$|M_{mzp}| = \sum_{i=1}^{l-1} q^{((r-i+1)\delta+s)(m-\delta+1)} + 1, \tag{5}$$

где l – общее число компонент.

Пример 2. Зададим $n = m + r\delta + s = 20$, $q = 2$, $m = 4$, $r = 5$,$\delta = 3$,$s = 1$. Вычислим мощность каждой компоненты:

$$\begin{array}{ll} |M_1| = & 2^{k(n-m)} = 2^{32}, \\ |M_2| = & 2^{k(n-m-\delta)} = 2^{26}, \\ |M_3| = & 2^{k(n-m-2\delta)} = 2^{20}, \\ |M_4| = & 2^{k(n-m-3\delta)} = 2^{14}, \\ |M_5| = & 2^{k(n-m-4\delta)} = 2^{8}, \\ |M_6| = 1, & \end{array}$$

где $k = m - \delta + 1 = 2$, $l = r + 1 = 6$. Просуммируем мощности всех компонент:

$$|M_{mzp}| = \sum_{i=1}^{5} M_i + 1 = 4363141377. \tag{6}$$

Основной вклад внесла первая компонента, полученное значение общей мощности всего лишь на 1.6 процента больше мощности первой компоненты.

Перейдём к спреду. Пусть $\delta = m = 4$, $n = 5m = 20$, $s = 0$, $q = 2$, $k = m - m + 1 = 1$.

$$\begin{array}{ll} |M_1| = & 2^{k(n-m)} = 2^{16}, \\ |M_2| = & 2^{k(n-2m)} = 2^{12}, \\ |M_3| = & 2^{k(n-3m)} = 2^{8}, \\ |M_4| = & 2^{k(n-4m)} = 2^{4}, \\ |M_5| = 1. & \end{array}$$

В этом случае общее число компонент $l = 5$.

$$|M_{mzp}| = \sum_{i=1}^{5} |M_i| + 1 = 2^{16} + 2^{12} + 2^8 + 2^4 + 1 = \frac{2^n - 1}{2^m - 1} = 69905. \tag{7}$$

Увеличение размерности на 1 и уменьшение длин кодовых слов рангового кода привело к уменьшению мощности в $\sim 6.2 \times 10^4$ раз.

4. Верхние границы и реальные мощности МНП спредов

Зададим следующие параметры МНП кодов-спредов: $n = mr+s$, $\delta = m$, $0 < s \leq (m-1)$. Вычислим мощность для различных параметров и сравним полученные значения с верхней границей подпространственных кодов для тех же параметров. В уравнении (5) положим $\delta = m$ и получим мощность кода для выбранных параметров:

$$M_{mzp} = |\mathcal{C}_{mzp}| = \sum_{i=1}^{r-1} q^{(mr+s-im)} + 1 = \frac{q^n - q^{m+s}}{q^m - 1} + 1. \tag{8}$$

При $s = 0$ и, следовательно, $n = rm$ мощность МНП спреда в уравнении (8) совпадает с *верхней границей мощности*, полученной в работе [9]:

$$M_{wang} = \frac{q^n - 1}{q^m - 1}. \tag{9}$$

При $n = rm + s$ и $s = 1$ получим из уравнения (8)

$$M_{mzp} = |\mathcal{C}_{mzp}| = \frac{q^n - q^{m+1}}{q^m - 1} + 1. \tag{10}$$

В этом случае полученное выражение для мощности совпадает с *верхней границей мощности*, полученной в работе [7] $M_{beut} = \frac{q^n-1}{q^m-1} - (q-1)$

При $n = rm + 2$ и, следовательно, $s = 2$ получим из (8)

$$M_{mzp} = |\mathcal{C}_{mzp}| = \frac{q^n - q^{m+2}}{q^m - 1} + 1. \tag{11}$$

В работе [8] это выражение совпадает с верхней границей для мощности спредов при $s \geq 2$. В работе [22] с использованием этой оценки максимально возможное значение мощности представлено в виде суммы двух слагаемых. Первое слагаемое – это мощность МНП спреда, а второе слагаемое – это некоторая величина γ_1:

$$M_{dr-fr} \leq \frac{q^n - q^{m+s}}{q^m - 1} + 1 + \gamma_1, \tag{12}$$

где $\gamma_1 = (q^s - \lfloor\theta\rfloor) - 2$, параметр θ зависит от m и s таким образом:

$$\lfloor\theta\rfloor = \begin{cases} 2^{s-1} - 1, & \text{если } 2s < m+2; \\ 2^{s-1} - 2, & \text{если } 2s = m+2; \\ 2^{s-1} - 2^{2s-m-3} - 1, & \text{если } 2s > m+2. \end{cases}$$

Возьмём $q = 2$, $m = 3$ и $s = 2$, тогда $\gamma_1 = 1$. Для этих параметров мощность МНП спреда равна $M = 33$, то есть на $\gamma_1 = 1$ меньше. Используя результаты работы пяти авторов [32], удалось довести мощность до верхней границы при $n = 3r+2$, r – любое, $q = 2$ в работе [22]. Путём полного перебора в работе [32] был построен подпространственный код для параметров $r = 2$, $m = 3$, $s = 2$, $n = 8$, который мы использовали в качестве последней компоненты в МНП спреде.

Увеличим размерность на 1, то есть $m = 4$, а остальные параметры $q = 2$, $r \geq 2$, $n = 4r+2$ и $s = 2$. В качестве верхней границы используем верхнюю оценку из работы [10]:

$$M_{Kurz} = \frac{2^{4r+2} - 49}{15}. \tag{13}$$

Теперь возьмём формулу для МНП спреда (8) для тех же параметров и увидим, что мощность МНП спреда совпадает с верхней границей (13).

Перейдём к новым оценкам верхних границ подпространственных кодов, полученным в работе [11]. В этой работе имеется две важные для нас теоремы. Здесь мы приведём их в нашей интерпретации и наших обозначениях.

Теорема 1. *При* $0 < s < m$ *и* $m > q^s$ *верхняя граница мощности подпространственного кода равна* $M_{HKK1} = \frac{q^{mr+s} - q^{m+s} + q^m - 1}{q^m - 1}$.

Выполним условия этой теоремы $0 < s < m$ и $m > q^s$ и сравним мощность M_{mzp} (8) с границей M_{HKK1} (1). Увидим,что они совпадают. Коды, у которых мощность совпадает с верхней границей, называем оптимальными кодами.

В этой же работе [11] доказана другая теорема, где дана верхняя оценка максимальной мощности подпространственного кода в противоположных ограничениях.

Теорема 2. *При* $m < q^s$ *и по-прежнему* $0 < s \leq (m-1)$ *мощность подпространственного кода* $M_{HKK2} = \frac{q^n - q^{m+s} + q^m - 1}{q^m - 1} + \gamma_2$,

где γ_2 вычисляется с помощью дополнительных параметров. Сравнение мощности МНП спреда при параметрах $0 < s \leq (m-1)$ и $m < q^s$ с оценкой M_{HKK2} показало, что при этих условиях МНП спред верхней оценки мощности подпространственного кода не достигает. Это впервые для рассмотренных случаев.

В теореме 2 предлагается вычислять два значения параметра γ_2: $\gamma_{21} > 1$ и $\gamma_{22} > 1$. Далее, при оценке мощности выбирать наименьшее значение:

$$\gamma_{21} = \lceil 2^m - \frac{1}{2}(1 + 2^{m+2}(2^m - 2^s))^{\frac{1}{2}} \rceil - 1, \tag{14}$$

$$\gamma_{22} = \lceil 2^s - \frac{1}{2}(1 + 2^{s+2}(m - s))^{\frac{1}{2}} \rceil - 1. \tag{15}$$

Мы считаем, что в этих условиях можем также использовать оценку Дрейка–Фримана [8], в которой добавка к мощности МНП спреда представлена параметром $\gamma_1 = (q^s - \lfloor \theta \rfloor) - 2$ (12).

Как мы видим, в обеих теоремах не указаны оценки мощности при выполнении равенства $m = 2^s$. Проверим, в какую из теорем можно включить это соотношение. Зададим, например, значения $m = 4$, $s = 2$, $m = 8$, $s = 3$ и $m = 16$, $s = 4$, и вычислим γ_{21}, γ_{22} и γ_1 по формулам (14), (15) и (12) соответственно. Вычислим мощность M_{mzp} МНП спреда при этих параметрах, добавим наименьшее из значений γ и получим верхнюю оценку M_{up}. Отношение $\eta = \frac{M_{mzp}}{M_{up}}$ оценивает эффективность МНП спреда.

Таблица 1

Эффективность $\eta = \frac{M_{mzp}}{M_{up}}$ **при** $m = 2^s$ **и** $n = 2m + s$

η	1.000	1.000	0.9999...	0.9999...	0.99999...
M_{mzp}	65	4049	1048579	137438953473	118059162071741130342 5
M_{up}	65	4049	1048578	137438953473	118059162071741130342 8
$n = 2m + s$	10	19	36	69	134
m	4	8	16	32	64
s	2	3	4	5	6
γ_{21}	5	3	7	15	31
γ_{22}	0	0	1	1	3
γ_1	1	3	7	15	31

Как видно из приведённых в табл. 1 значений дополнительного слагаемого $\gamma : \gamma_{21}, \gamma_{22}, \gamma_1$, наименьшее значение имеет γ_{22}, но оно равно нулю только для параметров $m = 4$, $s = 2$ и $m = 8$, $s = 4$, в остальных случаях $\gamma_{22} \geq 1$. Это объясняет условие в приведённых выше теоремах из работы [25], выраженное знаком неравенства больше: $m > 2^s$ (первая теорема), меньше: $m < 2^s$ (вторая теорема), а не знаком больше-равно: $m \geq 2^s$ или меньше-равно: $m \leq 2^s$ соответственно приведённым здесь теоремам. В этих численных примерах мощности МНП спредов настолько велики по сравнению со вторым слагаемым – минимальным из значений $\gamma_{21}, \gamma_{22}, \gamma_1$, что эффективность выражена большим количеством цифр 9 после нуля и точки. Поэтому можно считать, что практически эффективность равна $\eta = 1.000$ при условии $m = 2^s$.

Теперь при выполнении условий $m < q^s$ и $0 < s \leq (m-1)$ задаём параметры m, s, длину в виде $n = 2m + s$ и вычислим значения трёх величин γ_1, γ_{21} γ_{22}. Выбрав наименьшее из этих значений, просуммируем с мощностью МНП спреда. Полученное значение используем в качестве верхней оценки и обозначим M_{up}. Эффективность МНП спреда оценим в виде отношения $\eta = \frac{|M_{mzp}|}{|M_{up}|}$. В табл. 2 приведены значения эффективности, мощности для заданных параметров и значения вспомогательных параметров γ.

Таблица 2

Эффективность $\eta = \frac{M_{mzp}}{M_{up}}$ **при** $m < 2^s$ **и** $n = 2m + s$

η	0.971	0.970	0.992	0.985	0.996	0.993	0.992	0.997
M_{mzp}	33	129	257	513	513	1025	2049	1025
M_{up}	34	133	259	521	515	1032	2066	1028
$n = 2m + s$	8	11	13	14	15	16	17	17
m	3	4	5	5	6	6	6	7
s	2	3	3	4	3	4	5	3
γ_{21}	1	4	3	8	2	9	18	3
γ_{22}	1	5	2	11	3	7	25	1
γ_1	1	4	3	10	3	8	17	3
M_{mzp}	2049	4097	4097	8193	16385	8193	32769	524289
M_{up}	2055	4112	4103	8207	16414	8208	32824	524296
$n = 2m + s$	18	19	20	21	22	20	23	34
m	7	7		8	8	7	8	15
s	4	5	4	5	6	6	7	4
γ_{21}	6	15	6	15	144	15	73	7
γ_{22}	7	22	6	20	51	54	106	2
γ_1	7	19	7	14	29	35	55	9

В табл. 2 представлены значения эффективности для случаев, когда выполняется условие $m < 2^s$ и длина определена в виде $n = 2m + s$. Заметим, что при такой длине мы имеем всего две компоненты МНП-кода, причём первая из них – это SKK-код, а вторая

компонента имеет одно кодовое слово в виде конкатенации нулевой и единичной матриц. Добавление такой компоненты незначительно меняет общую мощность. Так что вычисленное отношение мощности МНП-кода к верхней границе фактически в этом случае оценивает эффективность SKK-кода.

Анализируя данные, представленные в табл. 2, отмечаем следующее. При размерностях от $m = 3$ до $m = 5$ эффективность $\eta = \frac{|M_{mzp}|}{|M_{up}|}$ меняется от 0.970 до 0.985, при $m \geq 6$ эффективность $\eta > 0.99$. Дополнительное слагаемое γ тем больше, чем больше s. В то же время увеличение s при той же размерности увеличивает длину кодового слова, задаваемого по формуле $n = 2m + s$. Поэтому при одной и той же размерности $m = 7$ мощность МНП спреда равна $|M_{mzp}| = 4097$ при $s = 5$ и почти вдвое больше – $|M_{mzp}| = 8193$ при $s = 6$. Эффективность η равна соответственно 0.996 и 0.998, то есть отличается в третьем знаке десятичной дроби.

Перейдём к случаю использования трёхкомпонентного МНП-кода, когда $n = 3m + s$. Составим аналогичную таблицу для этого случая.

Т а б л и ц а 3

Эффективность $\eta = \frac{M_{mzp}}{M_{up}}$ при $m < 2^s$ и $n = 3m + s$

η	0.9966	0.9982	0.9998	0.9995	0.99994	0.99988	0.99988	0.999999
M_{mzp}	289	2177	8449	16897	33281	66561	133121	132097
M_{up}	290	2181	8451	16905	33283	66569	133138	132098
$n = 3m + s$	11	15	18	19	21	22	23	24
m	3	4	5	5	6	6	6	7
s	2	3	3	4	3	4	5	3
γ_{21}	1	4	3	8	2	9	18	3
γ_{22}	1	5	2	11	3	7	25	1
γ_1	1	4	3	10	3	8	17	3

Приведённые расчёты показали, что при условии $m < 2^s$ мощность МНП спредов хотя и не достигает внешней границы, но находится близи её: отношение мощности к максимальному значению тем больше, чем больше длина. Например, при $n = 11$ эффективность $\eta = 0.996552$, а при $n = 21$ эффективность $\eta = 0.999940$.

Такие коды являются высоко эффективными кодами, так как показатель эффективности $\eta > 0.99$ при всех рассмотренных параметрах. Мощность близка к верхней границе, хотя незначительно от неё отличается. Мы называем эти коды субоптимальными подпространственными кодами.

5. Заключение

Здесь были представлены подпространственные коды с максимальным кодовым расстоянием – МНП спреды. Мощность этих кодов при больших размерностях ($m > 2^s$) совпадает с верхней границей. Для случаев противоположного неравенства $m < 2^s$ были проведены расчёты для ряда параметров: найдено отношение мощности кода к верхней границе $\eta = \frac{|M_{mzp}|}{|M_{up}|}$, которое определено как эффективность. Для всех рассмотренных случаев двухкомпонентного МНП-кода эффективность $\eta > 0.9$, а для трёхкомпонентного МНП-кода $\eta > 0.99$. При условии равенства $m = 2^s$ есть случаи совпадения мощности с верхней границей и есть также случаи небольшого отличия.

Таким образом, показано, что при $m > 2^s$ МНП-коды являются оптимальными подпространственными кодами-спредами, а при $m < 2^s$ эти коды названы субоптимальными подпространственными кодами-спредами.

При оценке эффективности были использованы верхние границы мощности подпространственных кодов-спредов, полученные в работах [7, 11].

Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (Проект 15-07-08480-2017).

Литература

1. *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.
2. *Silva D., Koetter R., Kschischang F.* A Rank-Metric Approach to Error Control in Random Network Coding // IEEE Trans. Inform. Theory. 2008. V. 54. N 9. P. 3951–3967.
3. *Ahlswede R., Cai N., Li S.-Y.R., Yeung R.W.*Network information flow // IEEE Trans. Inform. Theory. 2000. V. IT-46, N 6. P.1204–1216.
4. *Габидулин Э.М.* Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. 1985. Т. 21, вып. 1. С. 3–16.
5. *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.
6. *Габидулин Э.М., Боссерт М.* Алгебраические коды для сетевого кодирования // Проблемы передачи информации. 2009. Т. 45, вып. 4. С. 54–68.
7. *Beutelspacher A.* Partial Spreads in Finite Projective Spaces and Partial Designs//Math. Z. 1975. V. 145, N 3. P. 211–229.
8. *Drake D.A., Freeman J.W.*Partial t-Spreads and Group Constructible (s, r, μ)-Nets // J. Geom. 1979. V. 13, N 2. P. 210–216.
9. *Wang H., Xing C. , Safavi-Naini R.* Linear Autentication Codes: Bounds and Constructions // IEEE Trans. Inform. Theory. 2003. V. 49, N 4. P. 866–873.
10. *Kurz S.* Improved upper bounds for partial spreads // arXiv preprint 1606.08581(2016), Designs, Codes and Cryptography (to be appeared).
11. *Honold T., Kiermaier M., Kurz S.* Partial spreads and vector space partitions // arXiv:1611.06328v1[math.CO] 19 Nov. 2016.
12. *Габидулин Э.М., Пилипчук Н.И., Боссерт М.* Декодирование случайных сетевых кодов // Проблемы передачи информации. 2010. Т. 46, вып. 4. С. 33–55.
13. *Габидулин Э.М., Пилипчук Н.И.* Multicomponent Network Coding // WCC 2011 – Workshop on coding and cryptography. Apr 2011. Paris, France. P. 443–452.
14. *Pilipchuk N.I., Gabidulin E.M., Afanasiev V.B.* Decoding Multicomponent Codes Based on Rank Subcodes // Proc. 13 Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2012). Pomorie, Bulgaria. June. 2012.
15. *Габидулин Э.М., Пилипчук Н.И.* Ранговые подкоды в многокомпонентном сетевом кодировании // Проблемы передачи информации. 2013. Т. 49, вып. 1. С. 46–60.
16. *Gabidulin E., Pilipchuk N.* Bounds of Cardinality on Subspace Network Codes // Proc. Intern. Conf. on Engineering and Telecommunication. Moscow, Russia. 26–28 November. 2014.
17. *Габидулин Э.М., Пилипчук Н.И.* Эффективность подпространственных сетевых кодов // Труды МФТИ. 2015. Т. 7, № 1. С. 104–111.
18. *Габидулин Э.М., Григорьев А.А., Пилипчук Н.И., Сысоев И.Ю., Уривский А.В., Шишкин А.Л.* Подпространственные коды, основанные на ранговой метрике – новое направление в теории кодирования // Труды МФТИ. 2015. Т. 7, № 1. С. 85–103.
19. *Габидулин Э.М., Пилипчук Н.И.* Двойственные многокомпонентные коды максимальной мощности / /Труды МФТИ. 2016. Т. 8, № 1. С. 32–40.

20. *Gabidulin E., Pilipchuk N.* New constructions of multicomponentcodes//Proceedings of the Fifteenth Intern. Workshop on Algebraic and Combinatorial Coding Theory. June 18–24. 2016. Albena, Bulgaria. P. 162–167.

21. *Gabidulin E., Pilipchuk N., Sysoev I.* Decoding New multicomponent codes / /XV Intern. Symp. on Problems of Redundancy in Information and Control Systems. September. Saint-Peterburg. Russia. P. 53–57.

22. *Габидулин Э.М., Пилипчук Н.И.* Многокомпонентные коды с максимальным кодовым расстоянием // Проблемы передачи информации. 2016. Т. 52, вып. 3. С. 85–92.

23. *Шишкин А.Л.* Комбинированный метод построения многокомпонентных сетевых кодов // Труды МФТИ. 2014. Т.6, № 2. С. 188–194.

24. *Cruz J., Willems W.* On network codes and partial spreads//Seventh International Workshop on Optimal Codes and Related Topics. September 6–12. 2013. Albena, Bulgaria. P. 77–78.

25. *Honold T., Kiermaier M., Kurz S.* Optimal Binary Subspace Codes of Length 6, Constant Dimension 3 and Subspace Distance 4 // arXiv:1311.0464v2[math. CO] 26 Nov. 2014.

26. *Haiteng L. Honold T.* A New Approach to the Main Problem of Subspace Coding // arXiv:1408.1181v1[math. CO] 6 Aug. 2014.

27. *Braun M., Etzion T., Ostergard P.R.J., Vardy A., Wasserman A.* Existence of q-analogs of Steiner systems // Apr. 2013, preprint arXiv:1304.1462 [math.CO]

28. *Xia T., Fu F.W.* Jonson type bounds on constant dimension codes // Designs, Codes and Cryptography 2009. V.50, № 2. P. 163–172.

29. *Etzion T., Silberstein N.* Error-correcting Codes in Projective Space Via Rank-Metric Codes and Ferrers Diagrams // IEEE Trans. Inform. Theory. 2011. V. 55, № 7. P. 2909–2919.

30. *Silberstein N., Etzion T.* Large Constant Dimension Codes and Lexicodes // Advance in Mathematics of Communications. 2011. V. 5, № 2. P. 177–189.

31. *Silberstein N., Etzion T.* Codes and Designs Related to Lifted MRD Codes // Proc. 2011 IEEE Int. Sympos. on Information Theory (ISIT'2011). P. 2288–2292.

32. *El-Zanati S., Jordon H., Seelinger G., Sissokho P., Spence L.* The maximum size of a partial 3-spread in a finite vector space over GF(2) // Des. Codes Cryptogr. 2010. V.54, № 2. P. 101–107.

References

1. *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.

2. *Silva D., Koetter R., Kschischang F.* A Rank-Metric Approach to Error Control in Random Network Coding. IEEE Trans. Inform. Theory. 2008. V. 54, N 9. P. 3951–3967.

3. *Ahlswede R., Cai N., Li S.-Y.R., Yeung R.W.* Network information flow. IEEE Trans. Inform. Theory. 2000. V. IT-46, N. 6. P.1204–1216.

4. *Gabidulin E.M.* Theory of codes with maximal rank distance. Probl. Inform. Transm. 1985. V. 21, N 1. P. 3–16.

5. *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.

6. *Gabidulin E., Bossert M.* Algebraic codes for network coding. Probl. Inform. Transm. 2009. V. 45, N. 4. P. 54–68. (In Russian)

7. *Beutelspacher A.* Partial Spreads in Finite Projective Spaces and Partial Designs. Math. Z. 1975. V. 145, N 3. P. 211–229.

8. *Drake D.A., Freeman J.W.*Partial t-Spreads and Group Constructible (s, r, μ)-Nets. J. Geom. 1979. V. 13, N. 2. P. 210–216.

9. *Wang H., Xing C. , Safavi-Naini R.* Linear Autentication Codes: Bounds and Constructions. IEEE Trans. Inform. Theory. 2003. V. 49, N 4. P. 866–873.

10. *Kurz S.* Improved upper bounds for partial spreads. arXiv preprint 1606.08581(2016). Designs, Codes and Cryptography. (to be appeared).

11. *Honold T., Kiermaier M., Kurz S.* Partial spreads and vector space partitions. arXiv:1611.06328v1[math.CO]. 19 Nov. 2016.

12. *Gabidulin E.M., Pilipchuk N.I., Bossert M.* Decoding of random network codes. Probl. Inform. Transm. 2010. V. 46, N 4. P. 33–55. (In Russian).

13. *Gabidulin E. M., Pilipchuk N.I.* Multicomponent network coding. WCC 2011 Workshop on coding and cryptography. Apr 2011. Paris, France. P. 443–452.

14. *Pilipchuk N.I., Gabidulin E. M., Afanasiev V.B.* Decoding Multicomponent Codes Based on Rank Subcodes. Proc. 13 Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2012). Pomorie, Bulgaria. June, 2012.

15. *Gabidulin E. M., Pilipchuk N.I.* Rank subcodes in multicomponent network coding. Probl. Inform. Transm. 2013. V. 49, N 1. P. 46–60. (In Russian)

16. *Gabidulin E., Pilipchuk N.* Bounds of Cardinality on Subspace Network Codes. Proc. Intern. Conf. on Engineering and Telecommunication. Moscow, Russia. 26–28 November. 2014.

17. *Gabidulin E.M., Pilipchuk N.I.* Efficiency of subspace network codes. Proceed. MIPT. 2015. V. 7, N 1. P. 104–111. (In Russian)

18. *Gabidulin E.M., Grigoriev A.A., Pilipchuk N.I., Sysoev I.Yu., Urivskiy A.V., Shishkin A.L.* Subspace codes based on rank metric – the new direction in the coding theory. Proceed. MIPT. 2015. V. 7, N 1. P. 85–103. (In Russian).

19. *Gabidulin E.M., Pilipchuk N.I.* Dual multicomponent codes of maximal cardinality. Proceed. MIPT. 2016. V. 8, N 1. P. 32–40. (In Russian).

20. *Gabidulin E., Pilipchuk N.* New constructions of multicomponentcodes. Proceedings of the Fifteenth Intern. Workshop on Algebraic and Combinatorial Coding Theory. June 18-24, 2016. Albena, Bulgaria. P. 162–167.

21. *Gabidulin E., Pilipchuk N., Sysoev I.* Decoding New multicomponent codes. XV Intern. Symp.on Problems of Redundancy in Information and Control Systems. September, Saint-Peterburg, Russia. P. 53–57.

22. *Gabidulin E.M., Pilipchuk N.I.* Multicomponent codes with maximum code distance. Probl. Inform. Transm. 2016. V. 52, N 3. P. 84–91. (In Russian).

23. *Shishkin A.L.* Combined method for constructing multicomponent network codes. Proceed. of MIPT. 2014. V. 6, N 2. P. 188–194. (In Russian).

24. *Cruz J., Willems W.* On network codes and partial spreads. Seventh International Workshop on Optimal Codes and Related Topics. September 6-12. 2013. Albena, Bulgaria. P. 77–78.

25. *Honold T., Kiermaier M., Kurz S.* Optimal Binary Subspace Codes of Length 6, Constant Dimension 3 and Subspace Distance 4. arXiv:1311.0464v2[math. CO] 26 Nov. 2014.

26. *Haiteng L. Honold T.* A New Approach to the Main Problem of Subspace Coding. arXiv:1408.1181v1[math. CO] 6 Aug. 2014.

27. *Braun M., Etzion T., Ostergard P.R.J., Vardy A., Wasserman A.* Existence of q-analogs of Steiner systems. Apr. 2013, preprint arXiv:1304.1462 [math.CO]

28. *Xia T., Fu F.W.* Jonson type bounds on constant dimension codes. Designs, Codes and Cryptography 2009. V. 50, N. 2. P. 163–172.

29. *Etzion T., Silberstein N.* Error-correcting Codes in Projective Space Via Rank-Metric Codes and Ferrers Diagrams. IEEE Trans. Inform. Theory. 2011. V. 55, N. 7. P. 2909–2919.

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

31. *Silberstein N., Etzion T.* Codes and Designs Related to Lifted MRD Codes. Proc. 2011 IEEE Int. Sympos. on Information Theory (ISIT'2011). P. 2288–2292.

32. *El-Zanati S., Jordon H., Seelinger G., Sissokho P., Spence L.* The maximum size of a partial 3-spread in a finite vector space over GF(2). Des. Codes Cryptogr. 2010. V. 54, N. 2. P. 101–107.

Поступила в редакцию 28.04.2017