УДК 519.725

Э. М. Габидулин, Н. И. Пилипчук

Московский физико-технический институт (государственный университет)

Двойственные многокомпонентные коды максимальной мощности

Расширен класс подпространственных сетевых кодов. Построены двойственные многокомпонентные коды максимальной мощности на основе известных многокомпонентных кодов с нулевым префиксом (МНП), характеризующихся максимальным кодовым расстоянием. Переход к двойственным кодам позволил снять ограничение на соотношение между размерностью кода и кодовым расстоянием.

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

E. M. Gabidulin, N. I. Pilipchuk

Moscow Institute of Physics and Technology (State University)

Dual multicomponent codes of maximal cardinality

The family of subspace network codes is extended. Dual multicomponents codes of maximal cardinality are constructed on the basis of known multicomponent codes with zero prefixes. Using dual codes allows us to remove restrictions on the dimension and subspace distance.

Key words: rank codes, subspace codes, code cardinality, code distance, dimension, multicomponent codes.

1. Введение

Введём основные 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. Мощность грассманиана равна

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

Грассманово расстояние между двумя подпространствами $U, V \in W(n,m)$ определено в виде

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

Обозначим $[n, M, d = 2\delta, m]$ некоторый код в грассмановой метрике, у которого длина равна n, M – число кодовых слов, $d = 2\delta$ – минимальное кодовое расстояние, m – размерность. Важной характеристикой кода является его мощность. Приведём некоторые границы мощности. Верхняя граница мощности для $[n, M, d = 2\delta, m]$ кода получена в 2003 году в работе [1] и имеет вид

$$M \le M_{\text{Wang}} = \left\lfloor \frac{|W(n, m-\delta+1)|}{|W(m, m-\delta+1)|} \right\rfloor = \left\lfloor \frac{\begin{bmatrix} n \\ m-\delta+1 \end{bmatrix}}{\begin{bmatrix} m \\ m-\delta+1 \end{bmatrix}} \right\rfloor. \qquad (1)$$

Далее мы рассмотрим границы для спредов, то есть кодов размерности m с максимальным подпространственным расстоянием $d = 2m$. Верхние границы были получены в ряде работ, некоторые из которых опубликованы намного раньше 2003 года (см., например, [2], [3], [4], [5]).

Запишем длину кода в виде $n = rm + s$, $r \geq 2$, $0 \leq s \leq m - 1$, где r и s – целые числа.

Тогда верхняя граница мощности кода с максимальным кодовым расстоянием $d = 2m$ приобретает вид

$$M = M(n, d = 2m, m) \leq M_{\text{Wang}}(n, d = 2m, m) = \frac{q^n - q^s}{q^m - 1}. \tag{2}$$

Если $s = 0$, то есть длина $n = rm$, то верхняя граница такова:

$$M_{\text{Wang}}(n, d = 2m, m) = \frac{q^n - 1}{q^m - 1}.$$

Для $s = 1$ в работе [3] получена верхняя граница в виде

$$M = M(n, d = 2m, m) \leq \frac{q^n - q}{q^m - 1} - (q - 1). \tag{3}$$

Для $s \geq 2$ в работе [4] приведены результаты, позволяющие модифицировать границу (2) следующим образом:

$$M = M(n, d = 2m, m) \leq \frac{q^n - q^s}{q^m - 1} - \lfloor \theta \rfloor - 1, \tag{4}$$

где

$$2\theta = \sqrt{1 + 4q^m(q^m - q^s)} - (2q^m - 2q^s + 1). \tag{5}$$

Верхняя граница (4) для $s = 2$ имеет вид

$$M = M(n, d = 2m, m) \leq \frac{2^n - 2^2}{2^m - 1} - 2, \tag{6}$$

тогда как нижняя граница (7) равна

$$M = M(n, d = 2m, m) \geq \frac{2^n - 2^2}{2^m - 1} - 3. \tag{7}$$

В работе [6] показано, что для параметров $n = 2m + 2$, $m \geq 4$, $d = 2m$ максимальная мощность равна

$$M_{\max} = 2^{m+2} + 1.$$

Поставим задачу. Используя известные многокомпонентные коды с нулевым префиксом максимальной мощности со следующими параметрами: $n = rm + s$, $r \geq 2$, $0 \leq s \leq m - 1$, $d = 2m$, построим двойственные многокомпонентные коды максимальной мощности новой размерности $m' = n - m$, изменив соотношение между размерностью и кодовым расстоянием. Тем самым мы расширим класс подпространственных сетевых кодов максимальной мощности.

В n-мерном пространстве над $GF(q)$ для каждого m-мерного подпространства X существует ортогональное ему дуальное $(n - m)$-мерное подпространство $X^{\perp}$. Так как

$$(X \cup Y)^{\perp} = X^{\perp} \cap Y^{\perp},$$

то отсюда следует, что если в коде заменить все подпространства на дуальные, то получим код с той же мощностью и подпространственным расстоянием, но с другой размерностью. Изменение размерности при максимальной мощности принципиально меняет постановку задачи. Ранее предполагалось $d = 2m$.

Если мощность была максимальной для размерности m, то она остаётся максимальной и для дуальной размерности $n - m$.

2. Многокомпонентные коды с нулевым префиксом

В 2008 г. в работе [7] для случая $\delta = m$ впервые был предложен класс многокомпонентных кодов с нулевым префиксом (МНП) при любых значениях основных параметров. В дальнейшем эти исследования дополнялись в работах [8], [9]. Заметим, что в работе 2009 г. [10] также имеется алгоритм построения подпространственных кодов максимальной мощности для кода с определёнными параметрами $n = rm$.

МНП-код состоит из нескольких компонент. (i)-я компонента состоит из $m \times (n - m - (i-1)m)$ матриц вида

$$\mathcal{C}_{\text{мнп},i} = \left\{ \begin{pmatrix} O_m & \ldots & O_m & I_m & M_i \end{pmatrix} \right\},$$

где $i = 1, \ldots, r$, $r \geq 2$. Первая компонента совпадает с кодом SKK [11], [12] (Silva–Koetter–Kschischang), без нулевого префикса: $\mathcal{C}_{\text{мнп},1} = \mathcal{C}_{\text{skk}}$.

Матрица M_i выбирается из матриц $m \times (n-m-(i-1)m)$ кода Габидулина [13] с ранговым расстоянием $\delta = m$.

Рассматриваем код с параметрами: длина кода n, размерность кодовых подпространств m, кодовое расстояние $d = 2m$. Обозначим $a_i = \max\{m, (n - m - (i-1)m)\}$ и $b_i = \min\{m, (n - m - (i-1)m)\}$. Мощность i-й компоненты равна

$$|\mathcal{C}_{\text{мнп}\, i}| = q^{a_i(b_i - m + 1)}. \tag{8}$$

Общая мощность равна сумме мощностей всех компонент:

$$\mathcal{C}_{\text{мнп}} = \sum_{i=1}^{r} q^{a_i(b_i - m + 1)}.$$

3. Двойственные мнокомпонентные коды (ДМК)

Пусть подпространство X размерности m задаётся матрицей L размера $m \times n$ ранга m. Тогда ортогональное подпространство $X^{\perp}$ размерности $n - m$ задаётся матрицей $L^{\perp}$ размера $(n - m) \times n$ такой, что

$$(L^{\perp})(L^{\top}) = 0,$$

где $L^{\top}$ означает транспонирование. Построим двойственный многокомпонентный код (ДМК). Для $j = 1, \ldots, r$ компоненты МНП-кода размерности m и длины $n = rm + s$ задаются матрицами ранга m вида

$$L_j = \begin{bmatrix} \mathbf{0}_m & \ldots & \mathbf{0}_m & \mathbf{I}_m & \mathbf{M}_j \end{bmatrix},$$

которые состоят из нулевого матричного префикса размера $m \times (j-1)m$, единичной подматрицы $\mathbf{I}_m$ порядка m и подматрицы $\mathbf{M}_j$ размера $m \times (n - j)m$.

Ортогональная матрица $L_j^{\perp}$ ранга $n - m$ имеет вид

$$L_j^{\perp} = \begin{bmatrix} \mathbf{I}_{(j-1)m} & \mathbf{0}_{(j-1)m}^{m} & \mathbf{0}_{(j-1)m}^{n-jm} \\ \mathbf{0}_{n-jm}^{(j-1)m} & -\mathbf{M}^{\top} & \mathbf{I}_{n-jm} \end{bmatrix}.$$

Здесь $\mathbf{0}_l^v$ означает нулевую матрицу размера $l \times v$.

ДМК-код $L_j^{\perp}$ имеет размерность $n - m$ и подпространственное расстояние $d = 2m$. Для $n = mr + s, m = 2, 3, s = 0, 1$, эти коды имеют максимальную мощность.

4. Максимальная мощность кодов МНП и ДМК

Сначала рассмотрим случаи, при которых мощность МНП-кода максимальна, а затем перейдём к ДМК. Пусть заданы параметры $\delta = m$ и $n = rm + s$, $s = 0$. Тогда

$$M_{\text{мнп}} = \sum_{i=1}^{r-1} q^{(r-i+1)m(m-m+1)} + 1 = \frac{q^n - 1}{q^m - 1}.$$

Это совпадает с *верхней* границей (1).

Теперь пусть $n = rm + 1$, $s = 1$, тогда

$$M_{\text{мнп}} = |\mathcal{C}_{\text{мнп}}| = q\frac{q^{(r+1)m} - 1}{q^m - 1} - (q - 1).$$

Это значение совпадает с уточнённой *верхней* границей (3)

$$M = q\frac{q^{(r+1)m} - 1}{q^m - 1} - (q - 1).$$

Это означает, что при размерности $m = 2$ коды МНП всегда имеют максимальную мощность при любых значениях параметров n, d, а при $m = 3$ коды МНП имеют максимальную мощность при $\delta = 3$ и $n = rm + s$, $s = 0$, 1. Соответствующие двойственные коды также имеют максимальную мощность при другой (в общем случае) размерности $m' = n - m$.

Пример. Построим МНП-код с параметрами $n = (2 \times 3) + 1 = 7$, $d = 6$ и соответствующий двойственный код размерности $n - 3 = 4$. В данном случае МНП-код состоит из двух компонент. Первая компонента является конкатенацией двух матриц – единичной матрицы I_3 порядка 3 и матрицы рангового кода M размера 3×4. Вторая компонента также является конкатенацией двух матриц – матрицы из нулевых элементов 0_3^4 размера 3×4 и единичной матрицы I_3 порядка 3. Мощность первой компоненты $M_1 = 2^4$, мощность второй компоненты $M_2 = 1$. Суммарная мощность $M_{\max} = 17$ соответствует верхней границе (3) для этих параметров.

Соответствующий двойственный код также состоит из двух компонент. Первая компонента является конкатенацией двух матриц – транспонированной матрицы рангового кода $-M^T$ размера 4×3 и единичной матрицы порядка 4. Вторая компонента также является конкатенацией двух матриц – единичной матрицы I_4 порядка 4 и матрицы из нулевых элементов 0_4^3 размера 4×3. Построенный двойственный код имеет размерность 4, в то время как исходный МНП-код имел размерность 3. В данном случае условие равенства удвоенной размерности ($2 \times m' = 8$) и расстояния $d = 6$ не соблюдено. Тем не менее код имеет максимальную мощность. На этом небольшом примере видно, что построение двойственных кодов на основе МНП-кодов максимальной мощности увеличивает число подпространственных кодов максимальной мощности.

5. ZJSSS-код максимальной мощности

Изменим параметры: пусть $n = (rm + 2) = 8$, $m = 3$. В этом случае МНП-код имеет мощность $M = 33$, в то время как верхняя граница даёт значение $M_{\max} = 34$.

В работе [14] путём исчерпывающего перебора построен код максимальной мощности для этих параметров. Соответственно первым буквам фамилий авторов обозначим его ZJSSS-код.

Кодовые подпространства размерности $m = 3$ ZJSSS-кода заданы порождающими двоичными матрицами размера 3×8. Для краткости каждая 8-битная строка записывается как двоичное разложение десятичного числа. Кодовые матрицы имеют вид

A_1=(169, 75, 5)	A_2 = (195, 43, 6)	A_3 = (108, 29, 3)	A_4=(130, 72, 20)
A_5=(144, 68, 33)	A_6 = (65, 61, 2)	A_7 = (66, 19, 4)	A_8=(140, 87, 1)
A_9=(35, 16, 9)	A_{10} = (147, 99, 7)	A_{11} = (155, 76, 38)	A_{12}=(69, 40, 24)
A_{13}=(132, 103, 12)	A_{14} = (152, 88, 56)	A_{15} = (153, 94, 39)	A_{16}=(196, 34, 11)
A_{17}=(167, 97, 15)	A_{18} = (159, 84, 32)	A_{19} = (154, 71, 55)	A_{20}=(145, 80, 50)
A_{21}=(131, 54, 13)	A_{22} = (134, 74, 53)	A_{23} = (166, 18, 8)	A_{24}=(164, 64, 31)
A_{25}=(138, 90, 60)	A_{26} = (135, 73, 27)	A_{27} = (146, 77, 37)	A_{28}=(171, 105, 17)
A_{29}=(158, 79, 52)	A_{30} = (128, 89, 47)	A_{31} = (129, 22, 10)	A_{32}=(143, 83, 46)
A_{33}=(205, 36, 21)	A_{34} = (137, 91, 44)		

6. Двойственный код (DZJSSS)

Кодовые подпространства размерности $n - m = 8 - 3 = 5$ длины $n = 8$ DZJSSS-кода заданы порождающими двоичными матрицами размера 5×8. Каждая 8-битная строка записывается как двоичное разложение десятичного числа.

$A_1^{\perp}$=(135, 66, 39, 16, 13)	$A_2^{\perp}$ = (137, 73, 40, 16, 7)	$A_3^{\perp}$ = (128, 43, 75, 12, 19)
$A_4^{\perp}$=(130, 72, 32, 20, 1)	$A_5^{\perp}$=(144, 68, 33, 8, 4)	$A_6^{\perp}$ = (128, 69, 36, 20, 12)
$A_7^{\perp}$ = (128, 32, 8, 67, 17)	$A_8^{\perp}$=(134, 66, 32, 18, 14)	$A_9^{\perp}$=(128, 64, 34, 11, 4)
$A_{10}^{\perp}$ = (144, 85, 53, 8, 3)	$A_{11}^{\perp}$ = (129, 71, 35, 17, 14)	$A_{12}^{\perp}$=(128, 65, 56, 5, 2)
$A_{13}^{\perp}$=(141, 65, 33, 16, 3)	A_{14} = (232, 24, 4, 2, 1)	$A_{15}^{\perp}$ = (161, 98, 19, 11, 6)
$A_{16}^{\perp}$=(132, 68, 42, 16, 9)	$A_{17}^{\perp}$=(138, 67, 41, 16, 6)	$A_{18}^{\perp}$ = (129, 69, 20, 9, 3)
$A_{19}^{\perp}$ = (131, 98, 51, 11, 5)	$A_{20}^{\perp}$=(129, 83, 34, 8, 4)	$A_{21}^{\perp}$=(137, 64, 43, 27, 7)
$A_{22}^{\perp}$ = (129, 71, 33, 17, 15)	$A_{23}^{\perp}$ = (132, 64, 36, 22, 1)	$A_{24}^{\perp}$=(133, 37, 17, 9, 3)
$A_{25}^{\perp}$=(150, 84, 36, 14, 1)	$A_{26}^{\perp}$ = (132, 67, 32, 22, 13)	$A_{27}^{\perp}$ = (130, 72, 41, 18, 5)
$A_{28}^{\perp}$=(130, 74, 40, 25, 4)	$A_{29}^{\perp}$=(131, 65, 38, 21, 10)	$A_{30}^{\perp}$ = (67, 34, 19, 9, 6)
$A_{31}^{\perp}$ = (129, 64, 32, 20, 14)	$A_{32}^{\perp}$=(135, 70, 35, 22, 12)	$A_{33}^{\perp}$=(136, 72, 37, 25, 2)
$A_{34}^{\perp}$ = (131, 66, 36, 18, 13)		

7. Семейство МНП и объединённых кодов

Алгоритм построения МНП-кодов позволяет включить ZJSSS-код в качестве конечной компоненты с целью увеличения мощности. Пусть $n = 11$. МНП-код состоит из 3-х компонент. Первая компонента – SKK-код. Заменим две последние компоненты МНП-кода на одну компоненту – код ZJSSS с нулевым матричным префиксом $\mathbf{0}_3$ порядка 3. Мощность этой компоненты равна 34 и является максимально возможной для длины $n = 8$ и расстояния $d = 2m = 6$. Получили двухкомпонентный объединённый МНП–ZJSSS-код $[11, 6, 3]$ максимальной мощности 290. Таким же образом получим семейство подпространственных кодов максимальной мощности с параметрами $n = 3(r-1) + 8 = 3(r+1) + 2$,$m = 3$, $d = 6$.

Сначала построим объединённый МНП–ZJSSS-код длины $n = 3 \times r + 2$, где r – некоторое целое число. Пусть размерность $m = 3$ и подпространственное расстояние максимально, то есть $d = 2m = 6$. Для примера зададим несколько значений r = 2, 3, 4, 5, соответственно n = 8, 11, 14, 17. Подсчитаем мощности кодов МНП и МНП–ZJSSS, оценим относительную разность в процентах. Эти данные приведём в таблице.

r	n	$M_{\max}$	$M_{\text{МНП}}$	$\frac{1}{M_{\max}}\%$
2	8	34	33	3
3	11	290	289	0.35
4	14	2338	2337	0.043
5	17	18722	18721	0.005

Используя структуру объединённого МНП–ZJSSS-кода с параметрами $n = 11$, $m = 3$, $d = 6$, построим объединённый двойственный двухкомпонентный код. Первая компонента задана матрицей

$$\begin{bmatrix} M^T & I_8 \end{bmatrix}.$$

Матрица второй компоненты имеет вид

$$\begin{bmatrix} I_3 & 0_3^8 \\ 0_5^3 & Z^{\perp} \end{bmatrix},$$

где $Z^{\perp}$ – матрица DZJSSS-кода размера 5×8. Матрица размера 8×11 является конкатенацией двух подматриц, из которых первая подматрица M^T является транспонированной матрицей рангового кода размера 3×8, а вторая подматрица I_8 является единичной матрицей порядка 8. Вторая компонента представляет двойственный ZJSSS-код в виде общей матрицы размера 8×11, состоящей из четырёх подматриц: в левом верхнем углу единичная матрица I_3 порядка 3, в правом верхнем углу матрица 0_3^8 из нулевых элементов размера 3×8; в левом нижнем углу матрица 0_5^3 из нулевых элементов размера 5×3, в правом нижнем углу матрица размера 5×8, ортогональная матрице ZJSSS-кода размера 3×8.

Теперь построим объединёный двойственный трёхкомпонентный код длины $n = 14$, размерности $m' = n - m = 14 - 3 = 11$ максимальной мощности. Первая компонента МНП-кода имеет вид

$$\begin{bmatrix} I_3 & M_{11} & M_{12} & M_{13} & M_{14} \end{bmatrix},$$

где матрица рангового кода M_1 записана в виде конкатенации четырёх матриц:

$$M_1 = \begin{bmatrix} M_{11} & M_{12} & M_{13} & M_{14} \end{bmatrix},$$

причём первые три матрицы размера 3×3, четвёртая матрица размера 3×2. Соответствующая первая компонента двойственного кода такова:

$$\begin{bmatrix} M_{11}^T & I_3 & 0^3 & 0^3 & 0^2 \\ M_{12}^T & 0^3 & I_3 & 0^3 & 0^2 \\ M_{13}^T & 0^3 & 0^3 & I_3 & 0^2 \\ M_{14}^T & 0^3 & 0^3 & 0^3 & I_2 \end{bmatrix}.$$

Вторая компонента МНП-кода имеет вид

$$\begin{bmatrix} 0_3^3 & I_3 & M_{21} & M_{22} & M_{23} \end{bmatrix},$$

где матрица рангового кода M_2 записана в виде конкатенации трёх матриц:

$$M_2 = \begin{bmatrix} M_{21} & M_{22} & M_{23} \end{bmatrix},$$

причём первые две матрицы размера 3×3, третья матрица размера 3×2.

Соответствующая вторая компонента двойственного кода такова:

$$\begin{bmatrix} I_3 & 0^3 & 0^3 & 0^3 & 0^2 \\ 0^3 & M_{21}^T & I_3 & 0^3 & 0^2 \\ 0^3 & M_{22}^T & 0^3 & I_3 & 0^2 \\ 0^3 & M_{23}^T & 0^3 & 0^3 & I_2 \end{bmatrix}.$$

Третья компонента объединённого трёхкомпонентного кода является конкатенацией двух нулевых матриц размера 3×3 и матрицы ZJSSS-кода размера 3×8:

$$\begin{bmatrix} 0_3^3 & 0_3^3 & Z \end{bmatrix},$$

где Z – матрица ZJSSS-кода.

Соответствующая третья компонента двойственного кода такова:

$$\begin{bmatrix} I_3 & 0_3^3 & 0_3^8 \\ 0_3^3 & I_3 & 0_3^8 \\ 0_5^3 & 0_5^3 & Z^T \end{bmatrix},$$

где Z^T – транспонированная матрица ZJSSS-кода размера 5×8.

8. МНП-коды размерности $m \geq 4$ и двойственные коды

В работе [6] показано, что для параметров $n = 2m + 2$, $m \geq 4$, $d = 2m$ максимальная мощность $M_{\max} = 2^{m+2} + 1$. Такую мощность при этих параметрах обеспечивает МНП-код, состоящий из двух компонент.

Пусть $m = 4$, $n = 10$, $d = 8$. Первая компонента – SKK-код:

$$\begin{bmatrix} I_4 & M_{11} & M_{12} \end{bmatrix}$$

мощности $M_1 = 2^{m+2} = 64$. Вторая компонента имеет вид

$$\begin{bmatrix} 0_4^6 & I_4 \end{bmatrix}$$

и дает единственное кодовое слово.

Соответствующий двойственный код имеет две компоненты. Первая компонента

$$\begin{bmatrix} M_{11}^T & I_4 & 0_4^2 \\ M_{12}^T & 0_2^4 & I_2 \end{bmatrix}.$$

Вторая компонента

$$\begin{bmatrix} I_4 & 0_4^4 & 0_4^2 \\ 0_2^4 & 0_2^4 & I_2 \end{bmatrix}.$$

Новая размерность равна $m' = n - m = 10 - 4 = 6$. В этом случае удвоенное значение размерности $2m' = 12$ не совпадает с расстоянием $d = 8$.

Пусть $n = 3m + 2 = 14$, $m = 4$, $d = 8$. Исходный трёхкомпонентный код

$$\begin{bmatrix} I_4 & M_{11} & M_{12} & M_{13} \end{bmatrix},$$
$$\begin{bmatrix} 0_4^4 & I_4 & M_{21} & M_{22} \end{bmatrix},$$
$$\begin{bmatrix} 0_4^4 & 0_4^4 & I_4 & 0_4^2 \end{bmatrix},$$

где каждая строка – соответствующая компонента, матрицы M_{11}, M_{12}, M_{21} имеют размер 4×4, матрицы M_{13} и M_{22} размера 4×2.

Первая компонента двойственного кода

$$\begin{bmatrix} M_{11}^T & I_4 & 0_4^4 & 0_4^2 \\ M_{12}^T & 0_4^4 & I_4 & 0_4^2 \\ M_{13}^T & 0_2^4 & 0_2^4 & I_2 \end{bmatrix},$$

вторая компонента двойственного кода

$$\begin{bmatrix} I_4 & 0_4^4 & 0_4^4 & 0_4^2 \\ 0_4^4 & M_{21}^T & I_4 & 0_4^2 \\ 0_2^4 & M_{22}^T & 0_2^4 & I_2 \end{bmatrix},$$

третья компонента двойственного кода

$$\begin{bmatrix} I_4 & 0_4^4 & 0_4^4 & 0_4^2 \\ 0_4^4 & I_4 & 0_4^4 & 0_4^2 \\ 0_2^4 & 0_2^4 & 0_2^4 & I_2 \end{bmatrix}.$$

Заключение

Расширен класс кодов с максимальной мощностью за счёт перехода к двойственным кодам, у которых меняется размерность, но сохраняется мощность и кодовое расстояние. Теперь условие равенства кодового расстояния и удвоенной размерности, вообще говоря, не соблюдается. Это значит, что расширены условия для построения подпространственных кодов максимальной мощности.

Для всех значений параметров $m \geq 2$, $n = (r+1)m+s$, где $s = 0,\ 1,\ 2$, $d = 2m$, построены подпространственные многокомпонентные коды максимальной мощности. На основе этих кодов построены двойственные коды максимальной мощности размерности $m' = n - m$, в общем случае не равной половине подпространственного кодового расстояния.

Работа выполнена при частичной финансовой поддержке гранта РФФИ, проект № 15-07-08480/16.

Литература

1. *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.

2. *Dembowski P.* Finite geometries // Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968.

3. *Beutelspacher A.* Partial spreads in finite projective spaces and partial designs // Math. Z. 1975. 145(3). P. 211–229.

4. *Drake D.A., Freeman J.W.* Partial t-spreads and group constructible s, r, μ-nets // J. Geom. 1979. 13(2). P. 210–216.

5. *Beutelspacher A.* Blocking sets and partial spreads in finite projective spaces // Geom. Dedicata. 1980. 9(4). P. 425–449.

6. *Kurz S.* Improved upper bounds for partial spreads // arXiv:1512.04297[math.CO]

7. *Gabidulin E., Bossert M.* Codes for Network Coding // Proc. IEEE Int. Sympos. on Information Theory (ISIT'2008). Toronto, Canada. July 6–11. 2008. P. 867–870.

8. *Габидулин Э.М., Боссерт М.* Алгебраические коды для сетевого кодирования // Пробл. передачи информ. 2009. Т. 45, № 4. С. 54–68.

9. *Габидулин Э.М., Пилипчук Н.И.* Эффективность подпространственных сетевых кодов // Труды МФТИ. 2015. Т. 7, № 1. С. 104–111.

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

11. *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.

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

13. *Габидулин Э.М.* Теория кодов с максимальным ранговым расстоянием // Пробл. передачи информ. 1985. Т. 21. № 1. С. 3–16.

14. *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. P. 101–107.

References

1. *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.

2. *Dembowski P.* Finite geometries. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968.

3. *Beutelspacher A.* Partial spreads in finite projective spaces and partial designs. Math. Z. 1975. 145(3). P. 211–229.

4. *Drake D.A., Freeman J.W.* Partial t-spreads and group constructible s, r, μ-nets. J. Geom. 1979. 13(2). P. 210–216.

5. *Beutelspacher A.* Blocking sets and partial spreads in finite projective spaces. Geom. Dedicata. 1980. 9(4). P. 425–449.

6. *Kurz S.* Improved upper bounds for partial spreads. arXiv:1512.04297[math.CO]

7. *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.

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

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

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

11. *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.

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

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

14. *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. P. 101–107.

Поступила в редакцию 26.02.2016