Многокомпонентные коды максимальной мощности

Э.М. Габидулин[1], Н.И.Пилипчук[1]
[1] Московский физико-технический институт (государственный университет)

Аннотация

Многокомпонентные коды (МНП) относятся к случайным сетевым подпространственным кодам. Они предложены Габидулиным и Боссертом в 2008 году [1]. С тех пор эта тема активно развивается, что отражено в публикациях [2]-[5]. Как следует из названия, многокомпонентные коды состоят из нескольких компонент. Первой компонентой является известный подпространственный код Силвы—Кёттера—Кшишанга (SKK) [6]-[7] в так называемой лифтинговой конструкции, который построен на основе рангового кода Габидулина[8]. Мощность кодов является основной характеристикой. В этой работе поставлена задача найти условия, в которых многокомпонентные коды имеют максимальную мощность.

1. Введение

Рассматриваем сеть связи как направленный граф без циклов, где вершины – это источник, получатель или промежуточные узлы, а рёбра – каналы связи. В сетевом кодировании на промежуточных узлах сообщения рассматривают в виде элементов конечного поля и образуют линейные комбинации со случайными коэффициентами. Источник вырабатывает n пакетов $X_1, \dots, X_n$ и строит матрицу $\mathbf{X}$, используя пакеты в качестве строк. Получатель принимает n_r искаженных пакетов $Y_1, \dots, Y_{n_r}$ и строит из них матрицу $\mathbf{Y}$. Задача состоит в том, чтобы извлечь информационные пакеты $X_1, \dots, X_n$ из принятой матрицы $\mathbf{Y}$.

Матрица $\mathbf{X}$ SKK кода имеет вид

$$\mathbf{X} = \begin{bmatrix} \mathbf{I}_n & \mathbf{M} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 & M_{11} & M_{12} & \dots & M_{1m} \\ 0 & 1 & \dots & 0 & M_{21} & M22 & \dots & M_{2m} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 1 & M_{n1} & M_{n2} & \dots & M_{nm} \end{bmatrix}$$

где M - матрица рангового кода размера $n \times m$ с ранговым расстоянием δ.

Принята модель канала связи, в которой матрицы $\mathbf{Y}$ и $\mathbf{X}$ связаны соотношением

$$\mathbf{Y} = \mathbf{A}\mathbf{X} + \mathbf{E}_{\text{out}},$$

где $\mathbf{Y}$ – $n_r \times (n+m)$ матрица полного ранга n_r; $(n_r > n; n_r < n;\ n_r = n)$, $\mathbf{Y} = \begin{bmatrix}\mathbf{Y}_1 & \mathbf{Y}_2\end{bmatrix}$, $\rho(\mathbf{Y}_1) = r$. $\mathbf{A}$ – $n_r \times n$ матрица, соответствующая всем линейным преобразованиям на промежуточных узлах.

$\mathbf{E}_{\text{out}} = [E_1\, E_2]$ – *внешняя* $n_r \times (n+m)$ матрица ошибок с неизвестным рангом p.

2. Многокомпонентные сетевые коды с нулевым префиксом

Многокомпонентные сетевые коды с нулевым префиксом (МНП) Габидулина – Боссерта предложены в 2008 г.

C_i, $i = \overline{1,r}$ – кодовая матрица i-й компоненты.

$$\begin{array}{l} C_1 = [I_m\ M_1] \\ C_2 = [O_m^{\delta}\ I_m\ M_2] \\ \dots \\ C_{r-1} = [O_m^{\delta}\ O_m^{\delta}\ \dots\ O_m^{\delta}\ I_m\ M_{r-1}] \\ C_r = [O_m^{\delta}\ O_m^{\delta}\ \dots\ O_m^{\delta}\ I_m] \end{array}$$

Первая компонента C_1 – это SKK-код, последняя компонента C_r – единичная матрица с нулевым префиксом. Общая мощность равна сумме мощностей всех r кодовых компонент C_i, $i = \overline{1,r}$. Другая конструкция предложена в 2009 г. в работе [12].

Подсчитаем мощность МНП кода для заданных параметров. Пусть длина $n = rm + s, 1 \le s \le m-1$, расстояние $d_{sub} = 2m$, размерность m. Число кодовых матриц равно

$$M_{\text{мнп}} = q^{(r-1)m+s} + q^{(r-2)m+s} + \dots + q^{m+s} + 1 = \frac{q^n - q^s}{q^m - 1} - q^s + 1.$$

Сравним полученное число с известной границей Ванга [11], которая имеет вид

$$M_{Wang} = q^{(r-1)m+s} + q^{(r-2)m+s} + \dots + q^{m+s} + q^s = \frac{q^n - q^s}{q^m - 1}.$$

При $s = 0$ мощности $M_{\text{мнп}}$ и M_{Wang} совпадают. При $s = 1$ $M_{\text{мнп}} < M_{Wang}$.

Изменим параметры. Пусть $s = 1$, $n = rm + 1$. Тогда

$$M_{\max} = q^{(r-1)m+1} + q^{(r-2)m+1} + \cdots + q^{m+1} + 1 = M_{\text{мнп}}.$$

В соответствии с результатами работы [9] полученная мощность является максимальной для подпространственных кодов с этими параметрами. Однако, при $s > 1$ МНП код не является оптимальным.

3. ZJSSS код

Приведём теорему о максимальной мощности, доказанную в работе [10]. Пусть $q = 2$, длина кода равна $n = rm + s$, $0 \le s \le m - 1$, r – целое число, размерность кодовых подпространств $m = 3$, $s = 2$, подпространственное расстояние $d = 2m = 6$. Тогда максимальная мощность подпространственного кода равна

$$M_{max} = \begin{cases} 1, & \text{если } 3 \le n \le 5; \\ \frac{2^n - 2^s}{2^3 - 1} - s, & \text{если } n \ge 6. \end{cases}$$

В качестве примера в этой работе представлен подпространственный код максимальной мощности со следующими параметрами

$$n = rm + 2 = 8, \quad m = 3, \quad r = 2, \quad q = 2,$$

построенный путём исчерпывающего перебора. Код обозначим по первым буквам авторов ZJSSS код. Его мощность равна

$$M_{max} = q^{(r-1)m+2} + q^{(r-2)m+2} + \cdots + q^{m+2} + q = 34 > M_{\text{мнп}} = 33.$$

Кодовые матрицы представлены в виде трёх независимых строк в десятичной форме:

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)	$A_{34} = (137, 91, 44)$		

Мультииндексы таковы:

$A_1(1,2,6)$	$A_2(1,3,6)$	$A_3(2,4,7)$	$A_4(1,2,4)$
$A_5(1,2,3)$	$A_6(2,3,7)$	$A_7(2,4,6)$	$A_8(1,2,8)$
$A_9(3,4,5)$	$A_{10}(1,2,6)$	$A_{11}(1,2,3)$	$A_{12}(2,3,4)$
$A_{13}(1,2,5)$	$A_{14}(1,2,3)$	$A_{15}(1,2,3)$	$A_{16}(1,3,5)$
$A_{17}(1,2,5)$	$A_{18}(1,2,3)$	$A_{19}(1,2,3)$	$A_{20}(1,2,3)$
$A_{21}(1,3,5)$	$A_{22}(1,2,3)$	$A_{23}(1,4,5)$	$A_{24}(1,2,4)$
$A_{25}(1,2,3)$	$A_{26}(1,2,4)$	$A_{27}(1,2,3)$	$A_{28}(1,2,4)$
$A_{29}(1,2,3)$	$A_{30}(1,2,3)$	$A_{31}(1,4,5)$	$A_{32}(1,2,3)$
$A_{33}(1,3,4)$	$A_{34}(1,2,3)$		

Индекс (123) встречается 14 раз.

4. Объединение двух кодов

Пусть коды C_1 и C_2 имеют одинаковое подпространственное расстояние $2m$, где C_1– SKK код, C_2-ZJSSS код с добавленным нулевым префиксом. Заданы параметры $m = 3$, $d_{sub} = 6$, $n = 3 \times 3 + 2 = 11$, $s = 2$.

$$\mathcal{C}_1 = \begin{bmatrix} I_m & L_1 \end{bmatrix}, \quad \mathcal{C}_2 = \begin{bmatrix} 0_m & L_2 \end{bmatrix}$$

Тогда их объединение C является оптимальным кодом:

$$\mathcal{C} = \mathcal{C}_1 \bigcup \mathcal{C}_2$$

Приведем примеры. Пусть $n = m \times r + s = 14$, $m = 3$, $r = 4$, $s = 2$, $d_{sub} = 2m$. МНП–ZJSSS код состоит из первых двух компонент МНП кода и третьей компоненты в виде ZJSSS кода с префиксом из двух нулевых матриц. Мощность этого кода

$$M_{\text{мнп-zjsss}} = 2^{11} + 2^8 + 34 = 2338.$$

По теореме о максимальной мощности для этого случая имеем

$$M_{max} = \frac{2^{14} - 2^2}{2^3 - 1} - 2 = 2338.$$

Мощности совпадают. Построенный МНП–ZJSSS код для параметров $n = m \times r + s$, $m = 3$, $r > 2$, $s = 2$, $d_{sub} = 2m$ имеет максимальную мощность то есть является оптимальным.

5. Подпространственный и двойственный подпространственный коды

Пусть задан подпространственный код

$$[n, M, d_{sub} = 2\delta, m]$$

размерности m. Тогда можно построить двойственный код

$$[n, M, d_{sub} = 2\delta, n - m]$$

размерности $n - m$. Если один из кодов оптимален (имеет максимальную мощность), то и другой код оптимален. Для подпространства $X \in W(n, m)$ размерности m существует ортогональное дополнительное подпространство $X^\perp \in W(n, n - m)$ размерности $n - m$. Для двух подпространств X, Y одинаковой размерности m можно записать соотношение

$$(X \cup Y)^\perp = X^\perp \cap Y^\perp.$$

Кодовое расстояние подпространственного и двойственного подпространственного кодов совпадают:

$$\begin{aligned} d_{\text{sub}}(X^\perp, Y^\perp) &= \dim(X^\perp) + \dim(Y^\perp) - 2\dim(X^\perp \cap Y^\perp) \\ &= n - \dim(X) + n - \dim(Y) - 2(n - \dim(X \cup Y)) \\ &= 2\dim(X \cup Y) - \dim(X) - \dim(Y) \\ &= 2\dim(X) + 2\dim(Y) - 2\dim(X \cap Y) - \dim(X) - \dim(Y) \\ &= \dim(X) + \dim(Y) - 2\dim(X \cap Y) = d_{\text{sub}}(X, Y). \end{aligned}$$

$$d_{\text{sub}}(X^\perp, Y^\perp) = d_{\text{sub}}(X, Y).$$

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

$$L(L^\perp)^\top = 0.$$

Пусть подпространство задано такой матрицей, как в SKK коде:

$$L = [I_m \; M].$$

Тогда $L^{\perp} = [-M^{\top}\ I_{n-m}]$. Пусть подпространство задано матрицей с нулевым префиксом:

$$X = [0_m^k\ L],$$

где L – это $m \times n$ матрица ранга m. Тогда двойственное пространство задаётся матрицей

$$X^{\perp} = \begin{bmatrix} I_k & 0_k^n \\ 0_{n-m}^k & L^{\perp} \end{bmatrix},$$

где $L^{\perp}$ матрица размера $(n-m)\times n$ и ранга $n-m$, ортогональная по отношению к матрице L.

6. Оптимальные коды с расстоянием $d_{\text{sub}} = 4$, $d_{\text{sub}} = 6$

Пусть длина кода $n = 2r + s, \quad r \geq 2, \quad s = 0, 1$. Размерность кодовых подпространств $m = 2$ для всех n. Для двойственных кодов размерность меняется на $m = n - 2$. Мощность кода

$$M_{n,\text{opt}} = \frac{q^n - q^s}{q^2 - 1} - s$$

совпадает с мощностью МНП кода.

Пусть длина кода $n = 3r + s, \quad r \geq 1, \quad s = 0, 1$. Размерность кодовых подпространств $m = 3$ для всех n. Для двойственных кодов $m = n - 3$.

Мощность кода

$$M_{n,\text{opt}} = \frac{q^n - q^s}{q^3 - 1} - s.$$

совпадает с мощностью МНП кода.

Для двоичных кодов ($q = 2$) с длиной $n = 3r + 2$, $r \geq 2$

$$M_{n,\max} = \frac{2^n - 2^2}{2^3 - 1} - 2.$$

В частности, мощность $M_{8,\text{opt}} = 34$ на 1 больше мощности МНП кода.

Представим открытую проблему. Пусть

$$n = rm + s.$$

Предполагаем, что верна гипотеза

$$M_{\max} = q^{(r-1)m+s} + q^{(r-2)m+s} + \cdots + q^{m+s} + q^{s-1}.$$

7. Выводы

1) МНП код является оптимальным для случая, когда подпространственное кодовое расстояние d_{sub} равно удвоенной размерности m и длина кодового слова равна $n = rm + s$, где $s = 0$, 1 и r – положительное целое число.

2) МНП код является оптимальным для случая, когда подпространственное кодовое расстояние равно удвоенной размерности $m = 2$ при любой длине n. Двойственный код имеет ту же длину n, то же кодовое расстояние d_{sub}, новое значение размерности $n - m$ и тоже характеризуется максимальной мощностью. В этом случае кодовое расстояние может быть не равным удвоенной размерности.

3) ZJSSS код является оптимальным для $m = 3$, $n = 8$, $d_{sub} = 2m$. Построен новый оптимальный код, двойственный по отношению к ZJSSS коду. Размерность кода $n - m = 8 - 3 = 5$. В этом случае расстояние не равно удвоенной размерности.

4) Объединение кодов МНП и ZJSSS образует новый оптимальный МНП-ZJSSS код для размерности $m = 3$, расстояния $d_{sub} = 2m$ и для длин вида $n = rm + s$, где $s = 0$, 1, 2 и r – положительное целое число.

5) Двойственный код (по отношению к МНП-ZJSSS коду), имеющий размерность $n - m$, также является оптимальным.

Благодарности

Работа выполнена при частичной финансовой поддержке РФФИ (грант 15-07-08480).

Список литературы

[1] 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.

[2] Габидулин Э.М., Боссерт М. Алгебраические коды для сетевого кодирования // Пробл. передачи информ.-2009. Т. 45. №4. С. 54-68.

[3] Pilipchuk N., Gabidulin E., Afanasiev V. Decoding multicomponent codes based on rank subcodes // Proc. 2012 ACCT Int. Workshop. on Algebraic and Combinatorial Coding Theory. (ACCT'2012). Pomorie, Bulgaria June 15-21, 2012. P. 275-281.

[4] Габидулин Э.М., Пилипчук Н.И. Ранговые подкоды в многокомпонентном сетевом кодировании // Пробл. передачи информ.-2013. Т. 49. №1. С. 46-60.

[5] Габидулин Э.М., Пилипчук Н.И. Эффективность подпространственных сетевых кодов //Труды МФТИ.-2015.-Т.7. №1. С.104-111.

[6] Koetter R., Kschischang F.R. Coding for Errors and Erasures in Random Network Coding // IEEE Trans. Inform. Theory. 2008. V. 54. No. 8. P. 3579-3591.

[7] 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. No. 9. P. 3951-3967.

[8] Габидулин Э.М. Теория кодов с максимальным ранговым расстоянием// Пробл. передачи информ.1985. Т. 21. №1. С. 3-16.

[9] 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 pp. 77-78.

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

[11] *Wang H.,Xing C., Safavi-Naini R.* Linear Autentication Codes: Bounds and Constructions//IEEE Trans. Inform. Theory. 2003. V. 49.№4. P.866-873.

[12] *Xia T., Fu F.W.* Jonson type bounds on constant dimension codes "Designs, Codes and Cryptography,"vol.50, no 2, pp.163-172, 2009.