Верхние оценки минимального кодового расстояния для квазициклических МПП-кодов*

А.А. Фролов
Институт Проблем Передачи Информации
Российская академия наук
Москва, Россия
alexey.frolov@iitp.ru

Аннотация

Получены две верхние оценки минимального кодового расстояния для квазициклических кодов с малой плотностью проверок (КЦ МПП-кодов) 1-го типа. Сформулировано необходимое условие для того, чтобы минимальное кодовое расстояние таких кодов росло линейно с длиной кода. Описана процедура оценки минимального кодового расстояния для конкретного КЦ МПП-кода.

1. Введение

В этой работе исследуется минимальное кодовое расстояние КЦ МПП-кодов [1, 2, 3]. Эти коды являются важным классом МПП-кодов [4, 5]. Также КЦ МПП-коды являются подклассом МПП-кодов на протографах [6]. Такие коды просты в описании, для них есть эффективные алгоритмы кодирования [7] и декодирования, основанные на алгоритме распространения доверия [8]. Все это делает эти коды популярными для применения в практических приложениях.

В работе [2] получена верхняя оценка минимального кодового расстояния КЦ МПП-кодов в случае, когда базовая матрица состоит только из единиц. В этом случае минимальное кодовое расстояние ограничено сверху величиной $(m+1)!$, где m – это высота базовой матрицы, а также ввиду ее структуры и число единиц в столбце базовой матрицы. В этой работе мы обобщим результат работы [2] на случай базовых матриц с нулями и единицами (такие КЦ МПП-коды называют КЦ МПП-кодами 1-го типа).

Основные результаты работы заключаются в следующем. Получены две верхние оценки минимального кодового расстояния КЦ МПП-кодов 1-го типа. Сформулировано необходимое условие для того, чтобы минимальное кодовое расстояние таких кодов росло линейно с длиной кода. Описана процедура оценки минимального кодового расстояния для конкретного КЦ МПП-кода.

Структура работы такова. В разделе 2 приведены необходимые сведения о КЦ МПП-кодах. В разделе 3 выводятся верхние оценки минимального кодового расстояния таких кодов. В разделе 4 описана процедура оценки минимального кодового расстояния для конкретного КЦ МПП-кода.

2. Предварительные сведения

В этой работе мы рассматриваем только двоичные линейные коды. Пусть w – некоторое целое положительное число. Рассмотрим следующую матрицу размера $m \times n$

$$\mathbf{H}^{(W)} = [h_{i,j}] \in \{0, 1, \ldots, w\}^{m \times n}.$$

Эту матрицу мы будем называть матрицей весов[1].

Построим проверочную матрицу $\mathbf{H}$ КЦ МПП-кода $\mathscr{C}$. Для этого расширим матрицу $\mathbf{H}^{(W)}$ циклическими матрицами(циркулянтами) следующим образом:

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}_{1,1} & \mathbf{P}_{1,2} & \cdots & \mathbf{P}_{2,n} \\ \mathbf{P}_{2,1} & \mathbf{P}_{2,1} & \cdots & \mathbf{P}_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{P}_{m,1} & \mathbf{P}_{m,1} & \cdots & \mathbf{P}_{m,n} \end{bmatrix} \in \mathbb{F}_2^{ms \times ns},$$

где $\mathbf{P}_{i,j}$ – циркулянт над полем $\mathbb{F}_2$ размера $s \times s$ ($s \geqslant w$) веса[2] $h_{i,j}$, $i = 1, \ldots, m$; $j = 1, \ldots, n$.

Обозначим длину кода $\mathscr{C}$ через $N = ns$, для скорости полученного кода справедливо следующее неравенство

$$R(\mathscr{C}) \geqslant 1 - \frac{m}{n}.$$

*Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 12-07-31035 "мол_а").

[1] также в литературе используется термин "протоматрица".

[2] весом циркулянта называется вес его первой строки.

Замечание 1. *Легко заметить, что полученный код является квазициклическим. Пусть дано кодовое слово* $\mathbf{c} \in \mathscr{C}$. *Разделим это кодовое слово на* n *подблоков в соответствии со структурой проверочной матрицы* $\mathbf{H}$*:*

$$\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n),$$

тогда легко видеть, что если мы применим одинаковые циклические сдвиги в каждом из подблоков, то мы снова получим кодовое слово $\mathscr{C}$.

Замечание 2. *Построенный код является КЦ МПП-кодом типа* w. *Далее в этой работе мы рассматриваем только КЦ МПП-коды* 1*-го типа, т.е.* $w = 1$. *В этом случае матрицу* $\mathbf{H}^{(W)}$ *можно рассматривать как матрицу над* $\mathbb{F}_2$.

Пусть $\mathbb{F}$ – некоторое поле, $\mathbb{F}[x]$ – кольцо всех многочленов с коэффициентами из поля $\mathbb{F}$. Известен изоморфизм между кольцом циклических матриц размера $s \times s$ над полем $\mathbb{F}$ и фактор-кольцом $\mathbb{F}^{(s)}[x] = \mathbb{F}[x]/(x^s - 1)$. Поэтому проверочную матрицу $\mathbf{H}$ можно представить в полиномиальной форме в виде матрицы $\mathbf{H}(x) \in \left(\mathbb{F}_2^{(s)}[x]\right)^{m \times n}$:

$$\mathbf{H}(x) = \begin{bmatrix} p_{1,1}(x) & p_{1,2}(x) & \cdots & p_{1,n}(x) \\ p_{2,1}(x) & p_{2,1}(x) & \cdots & p_{2,n}(x) \\ \vdots & \vdots & \ddots & \vdots \\ p_{m,1}(x) & p_{m,1}(x) & \cdots & p_{m,n}(x) \end{bmatrix},$$

где $p_{i,j}(x) = \sum_{t=1}^{s} P_{i,j}(t,1) x^{t-1}$, под $P_{i,j}(t,1)$ мы понимаем элемент, стоящий пересечении строки с номером t и столбца с номером 1 в матрице $P_{i,j}$.

Пример 1. *Проверочной матрице*

$$\mathbf{H} = \left[\begin{array}{ccc|ccc|ccc} 0&0&0&0&1&0&0&0&1 \\ 0&0&0&0&0&1&1&0&0 \\ 0&0&0&1&0&0&0&1&0 \\ \hline 1&0&0&0&0&0&0&1&0 \\ 0&1&0&0&0&0&0&0&1 \\ 0&0&1&0&0&0&1&0&0 \end{array}\right]$$

соответствуют матрицы

$$\mathbf{H}^{(W)} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

и

$$\mathbf{H}(x) = \begin{bmatrix} 0 & x^2 & x \\ 1 & 0 & x^2 \end{bmatrix}.$$

Замечание 3 (О связи с МПП-кодами на протографах)**.** *КЦ МПП-коды являются являются подклассом МПП-кодов на протографах. В этом случае* $\mathbf{H}^{(W)}$ *– это матрица смежности протографа, а матрицы перестановок разрешается выбирать только из циркулянтов.*

Поставим в соответствие вектору

$$\mathbf{c} = (\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n),$$

где

$$\mathbf{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,s}), \quad i = 1, 2, \ldots, n,$$

вектор полиномов

$$\mathbf{c}(x) = (c_1(x), c_2(x), \ldots, c_n(x)),$$

где $c_i(x) = \sum_{t=1}^{s} c_{i,t} x^{t-1}$.

Ясно, что условие

$$\mathbf{H}\mathbf{c}^T = \mathbf{0} \quad (\text{в поле } \mathbb{F}_2)$$

эквивалентно условию

$$\mathbf{H}(x)\mathbf{c}^T(x) = \mathbf{0} \quad (\text{в кольце } \mathbb{F}_2^{(s)}[x]).$$

Весом полинома $f(x)$ назовем число ненулевых коэффициентов, будем обозначать вес через $||f(x)||$. Вес вектора многочленов $\mathbf{c}(x) = (c_1(x), c_2(x), \ldots, c_n(x))$ определим так

$$||\mathbf{c}(x)|| = \sum_{i=1}^{n} ||c_i(x)||.$$

3. Минимальное кодовое расстояние

Обозначим минимальное кодовое расстояние кода $\mathscr{C}$ через $D(\mathscr{C})$. Начнем с очевидного результата.

Теорема 1. *Пусть* $\mathscr{C}$ *– это КЦ МПП-код* 1*-го типа с матрицей весов* $\mathbf{H}^{(W)}$ *и пусть* d *– это минимальное кодовое расстояние двоичного кода, соответствующего проверочной матрице* $\mathbf{H}^{(W)}$*, тогда*

$$D(\mathscr{C}) \leqslant ds. \tag{1}$$

Доказательство. Пусть c_W – это кодовое слово веса d кода с проверочной матрицей $\mathbf{H}^{(W)}$, $S = \operatorname{supp}(c_W)$ и пусть $f(x) = \sum_{j=0}^{s-1} x^j$. Построим кодовое слово $\mathbf{c}(x) \in \mathscr{C}$. Для $i = 1, \ldots, n$

$$c_i(x) = \begin{cases} f(x), & i \in S, \\ 0, & \text{иначе.} \end{cases}$$

Осталось заметить, что $x^j f(x) = f(x) \, \forall j = 0, \ldots, s-1$, поэтому

$$\mathbf{H}(x)\mathbf{c}^T(x) = f(x)\mathbf{H}^{(W)} c_W^T = \mathbf{0}.$$

□

Введем обозначение для подматрицы. Пусть $\mathbf{A}$ – некоторая матрица размера $M \times N$. Пусть $I \subseteq \{1, 2, \ldots, M\}$ – подмножество строк, а $J \subseteq \{1, 2, \ldots, N\}$ – подмножество столбцов, через $\mathbf{A}_{I,J}(x)$ обозначим подматрицу $\mathbf{A}$, состоящую из строк с номерами из I и столбцов с номерами из J. Если $I = \{1, 2, \ldots, M\}$, то будем использовать обозначение $\mathbf{A}_J(x)$.

Лемма 1 (Маккей и Дэви, [2]). *Пусть $\mathscr{C}$ – это КЦ МПП-код 1-го типа с матрицей $\mathbf{H}(x)$. Пусть $J \subset \{1,2,\ldots,n\}$, $|J| = m+1$ и пусть $\Delta_j(x) = \det\left(\mathbf{H}_{\mathbf{J}\setminus\{\mathbf{j}\}}(x)\right)$, тогда слово $\mathbf{c}(x) = (c_1(x), c_2(x), \ldots, c_n(x))$, где*

$$c_j(x) = \begin{cases} \Delta_j(x), & j \in J, \\ 0, & \textit{иначе.} \end{cases}$$

является кодовым словом кода $\mathscr{C}$.

Доказательство. Покажем, что $\mathbf{s}(x) = \mathbf{H}(x)\mathbf{c}^T(x) = \mathbf{0}$ в кольце $\mathbb{F}_2^{(s)}[x]$. Проведем доказательство только для первой компоненты синдрома:

$$s_1(x) = \sum_{j=1}^{n} p_{1,j}(x)c_j(x) = \sum_{j\in J} p_{1,j}(x)\Delta_j(x).$$

Пусть $J = \{j_1, j_2, \ldots, j_{m+1}\}$. Заметим, что

$$\begin{aligned} s_1(x) &= \det \left[\begin{array}{cccc} p_{1,j_1}(x) & p_{1,j_2}(x) & \cdots & p_{1,j_{m+1}}(x) \\ \hline p_{1,j_1}(x) & p_{1,j_2}(x) & \cdots & p_{1,j_{m+1}}(x) \\ p_{2,j_1}(x) & p_{2,j_2}(x) & \cdots & p_{2,j_{m+1}}(x) \\ \vdots & \vdots & \ddots & \vdots \\ p_{m,j_1}(x) & p_{m,j_2}(x) & \cdots & p_{m,j_{m+1}}(x) \end{array}\right] \\ &= 0, \end{aligned}$$

так как в матрице две одинаковые строки. Аналогично можно провести доказательство для остальных компонент синдрома. □

Теорема 2. *Пусть $\mathscr{C}$ – это КЦ МПП-код 1-го типа с матрицей весов $\mathbf{H}^{(W)}$ размера $m \times n$. Пусть ℓ – это средний вес столбца в $\mathbf{H}^{(W)}$, тогда*

$$D(\mathscr{C}) \leqslant \lfloor \ell \rfloor ! \ell^{m-\lfloor \ell \rfloor}(m+1). \qquad (2)$$

Доказательство. Расположим столбцы матрицы $\mathbf{H}^{(W)}$ по возрастанию веса, соответствующим образом переставим и столбцы $\mathbf{H}(x)$. Пусть $J = \{1,2,\ldots,m+1\}$. Ясно, что средний вес столбца в подматрице $\mathbf{H}_J^{(W)}$ не превосходит ℓ. Построим кодовое слово $\mathbf{c}(x)$ в соответствии с леммой 1. Последние $n - |J|$ позиций $\mathbf{c}(x)$ равны нулю.

Рассмотрим $\Delta_1(x)$. Заметим, что

$$||\Delta_1(x)|| \leqslant \lfloor \ell \rfloor ! \prod_{j=1}^{m-\lfloor \ell \rfloor} \ell_j,$$

где ℓ_j – это вес столбца с номером j в матрице $\mathbf{H}_J^{(W)}$. Это так, потому что в сумме для $\Delta_1(x)$ не более, чем $\lfloor \ell \rfloor ! \prod_{j=1}^{m-\lfloor \ell \rfloor} \ell_j$ слагаемых, каждое из которых представляет из себя моном. Так как

$$\prod_{j=1}^{m-\lfloor \ell \rfloor} \ell_j \leqslant \ell^{m-\lfloor \ell \rfloor},$$

то

$$||\Delta_1(x)|| \leqslant \lfloor \ell \rfloor ! \ell^{m-\lfloor \ell \rfloor}.$$

Аналогичные неравенства справедливы для всех $\Delta_j(x)$, $j \in J$. Так как ненулевых позиций в слове $\mathbf{c}(x)$ всего $m+1$, то $||\mathbf{c}(x)|| \leqslant \lfloor \ell \rfloor ! \ell^{m-\lfloor \ell \rfloor}(m+1)$.

Отдельно следует рассмотреть случай, когда миноры $\Delta_j(x) = 0 \quad \forall j \in J$. В этом случае лемма 1 дает нулевое слово. Найдем в матрице $\mathbf{H}_J(x)$ ненулевой минор максимального порядка r, $r < m$. Пусть I – это множество номеров строк, а S – множество столбцов, на пересечении которых находится найденный минор. Пусть $S' = S \cup j$, $j \in J \setminus S$. Рассмотрим подматрицу $\mathbf{H}_{I,S'}(x)$. В соответствии с леммой 1 построим кодовое слово для этой подматрицы. По построению в этом слове будет, по крайней мере, одна позиция, отличная от нуля. Если дополнить это слово нулями на позициях $\{1,2\ldots,n\}\setminus S'$, то мы получим кодовое слово для матрицы $\mathbf{H}(x)$, так как все миноры большего порядка равны нулю. В этом случае

$$D(\mathscr{C}) \leqslant \lfloor \ell \rfloor ! \ell^{r-\lfloor \ell \rfloor}(r+1) < \lfloor \ell \rfloor ! \ell^{m-\lfloor \ell \rfloor}(m+1),$$

что и завершает доказательство. □

Замечание 4. *Заметим, что оценка (2) не зависит от параметра s.*

Таким образом, для того, чтобы $D(\mathscr{C})$ росло линейно с длиной кода $N = ns$ необходимо, чтобы оценки (1) и (2) росли линейно с N.

Замечание 5. *Если параметры m и n фиксированы, а $s \to \infty$, то в соответствии с оценкой (2) $D(\mathscr{C})$ не растет линейно с N. Отметим, что в работе* [9] *показано, что в случае МПП-кодов на протографах существуют коды, минимальное кодовое расстояние которых растет линейно с длиной кода даже при фиксированных размерах базовой матрицы.*

4. Процедура оценки минимального кодового расстояния для конкретной проверочной матрицы

Оценка (2) является достаточно грубой верхней оценкой. В действительности, при заданной матрице $\mathbf{H}(x)$ можно получить гораздо более точную оценку минимального кодового расстояния кода $\mathscr{C}$, соответствующего этой матрице. Нужно действовать следующим образом:

1. для всех $J \subset \{1,2,\ldots,n\} : |J| = m+1$ построить кодовые слова $\mathbf{c}^{(J)}(x)$ в соответствии с леммой 1. Если для некоторого J $\mathbf{c}^{(J)}(x)$ является нулевым словом, то заменить это слово на ненулевое, как описано во второй части доказательства теоремы 2.
2. $D(\mathscr{C}) \leqslant \min_J(||\mathbf{c}^{(J)}(x)||)$.

5. Заключение

В работе получены две верхние оценки минимального кодового расстояния для КЦ МПП-кодов 1-го типа. Сформулировано необходимое условие для того, чтобы минимальное кодовое расстояние таких кодов росло линейно с длиной кода. Показано, что при фиксированных размерах базовой матрицы минимальное кодовое расстояние КЦ МПП-кодов не растет линейно с длиной кода. Описана процедура оценки минимального кодового расстояния для конкретного КЦ МПП-кода.

Автор выражает искреннюю благодарность В. В. Зяблову за многочисленные советы и рекомендации. Автор также благодарен П. С. Рыбину за обсуждения работы, позволившие существенно ее улучшить.

Список литературы

[1] R. M. Tanner. On quasi-cyclic repeat-accumulate codes. in *Proc. 37th Allerton Conf. Commun., Contr., Comput.*, Monticello, IL, Sep. 22–24, 1999, pp. 249–259, Allerton House.

[2] D. J. C. MacKay and M. C. Davey. Evaluation of Gallager codes for short block length and high rate applications. in *Codes, Systems, and Graphical Models (Minneapolis, MN, 1999), B. Marcus and J. Rosenthal, Eds.* New York: Springer-Verlag, 2001, pp. 113–130.

[3] M. P. C. Fossorier. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.

[4] R. G. Gallager. *Low-Density Parity-Check Codes.* Cambridge, MA: M.I.T. Press, 1963.

[5] R. M. Tanner. A recursive approach to low-complexity codes. *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

[6] J. Thorpe. Low-density parity-check (LDPC) codes constructed from protographs. JPL, IPN Progress Rep., Aug. 2003, vol. 42–154.

[7] Z. Li, L. Chen, L. Zeng, S. Lin, and W. H. Fong. Efficient encoding of quasi-cyclic low-density parity-check codes. *IEEE Trans. Commun.*, vol. 54, no. 1, pp. 71–78, Jan. 2006.

[8] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger. Factor graphs and the sum-product algorithm. *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.

[9] А. Шридхаран, М. Лентмайер, Д. В. Трухачев, Д. Дж. Костелло, К. Ш. Зигангиров. О минимальном расстоянии низкоплотностных кодов с проверочными матрицами, составленными из перестановочных матриц. *Пробл. передачи информ.*, 41:1, С. 39—52, 2005.