Верхняя оценка минимального расстояния квазициклических низкоплотностных кодов

М. Э. Тожибаева

В данной работе изучаются квазициклические низкоплотностные коды. Приводится верхняя оценка на минимальное расстояние, которая зависит от минимального и максимального количества единиц в столбцах проверочной матрицы данного кода.

Ключевые слова: минимальное расстояние, квазициклический низкоплотностный код.

Введение и постановка задачи

Коды, исправляющие ошибки, используются для передачи информации в каналах связи с шумом. Одним из наиболее часто используемых в настоящее время классов кодов является класс низкоплотностных кодов (LDPC-коды от англ. low-density parity-check). Впервые они были предложены Р. Галлагером [1] и переоткрыты более чем через 30 лет [2, 3]. Другим важным классом кодов является, предложенный Таунсендом и Уэлдоном, класс квазициклических кодов [4]. Было показано, что квазициклические коды являются асимптотически хорошими [5].

Наиболее перспективным классом низкоплотностных кодов являются квазициклические низкоплотностные коды [6]. С одной стороны их квазициклическая структура делает их удобными для практической реализации, а с другой для их декодирования можно использовать декодеры с мягкими решениями. Они уже стали частью многих современных стандартов передачи данных, таких как DVB-S2, 10 Gigabit Ethernet, WiMAX, Wi-Fi, LTE. Несмотря на то, что эти коды

обладают плохим минимальным расстоянием, которое сверху ограничено хоть большой, но константой [7], квазициклические низкоплотностные коды обеспечивают высокую степень исправления ошибок.

Важнейшей характеристикой кода является его минимальное расстояние. Для произвольного линейного кода было доказано, что нахождение минимального расстояния является NP-трудной задачей [8]. Поэтому представляют интерес верхние и нижние оценки минимального расстояния линейного кода в зависимости от его параметров.

В данной статье приводится верхняя оценка минимального расстояния для квазициклического низкоплотностного кода с фиксированным максимальным и минимальным количеством единиц в столбце порождающей матрицы, которая обобщает известную оценку [9].

Основные понятия и определения

Обозначим через $\mathbb{F}_2$ поле Галуа из двух элементов. Тогда под $\mathbb{F}_2^{m\times n}$ и $\mathbb{F}_2^n$ будем подразумевать соответственно множество матриц размерности $m \times n$ и векторов размерности n над полем $\mathbb{F}_2$. Функцией кодирования будем называть отображение $\varphi\colon \mathbb{F}_2^k \to \mathbb{F}_2^n$, где $k \leqslant n$, которое сопоставляет каждому *информационному слову* $u \in \mathbb{F}_2^k$ некоторое *кодовое слово* $x = \varphi(u) \in \mathbb{F}_2^n$.

Обычно в теории кодирования изучают не саму функцию кодирования, а множество кодовых слов. Назовем (n, k)-кодом множество векторов $\mathcal{C} \subseteq \mathbb{F}_2^n$, мощность которого равна 2^k. *Линейный* (n, k)-код — это (n, k)-код, который является линейным пространством над полем $\mathbb{F}_2$. Последнее требование эквивалентно тому, что сумма двух кодовых слов тоже будет кодовым словом. Любой линейный (n, k)-код можно задать как множество решений уравнения $Hx^T = 0$, где $H \in \mathbb{F}_2^{(n-k)\times n}$ — *проверочная матрица*. *Весом* вектора $v \in \mathbb{F}_2^n$ будем называть величину, равную количеству его ненулевых компонент и обозначать ее $\mathrm{wt}(v)$.

Расстояние по Хеммингу $d(u, v)$ между двумя векторами $u, v \in \mathbb{F}_2^n$ — это количество позиций, в которых они отличаются. Легко видеть, что:

$$d(u, v) = \mathrm{wt}(u + v),$$

где $u + v$ — покомпонентная сумма по модулю два векторов u и v.

Наименьшее расстояние между различными кодовыми словами кода $\mathcal{C}$ называется *минимальным расстоянием*:

$$d_{min}(\mathcal{C}) = \min_{\substack{u,v\in\mathcal{C}\\ u\neq v}} d(u,v).$$

Минимальное расстояние линейного кода $\mathcal{C}$ равно минимальному весу ненулевого кодового слова, так как сумма любых двух кодовых слов тоже будет кодовым словом:

$$d_{min}(\mathcal{C}) = \min_{\substack{u,v\in\mathcal{C}\\ u\neq v}} \mathrm{wt}(u+v) = \min_{\substack{w\in\mathcal{C}\\ w\neq 0}} \mathrm{wt}(w).$$

Циркулянтной матрицей будем называть квадратную матрицу, каждая строка которой, начиная со второй, получается из предыдущей циклическим сдвигом вправо на один элемент. *Циркулянтная перестановочная матрица* это циркулянтная матрица, в каждой строке которой ровно одна единица.

Легко видеть, что любая циркулянтная перестановочная матрица представляет собой матрицу циклического сдвига $I(p) \in \mathbb{F}_2^{r\times r}$, в i-й строке которой есть равно одна единица на позиции $i+p$ по модулю r, где $p \in \{0,1,\ldots,r-1\}$.

Определение 1. *Квазициклический низкоплотностный код* — это линейный код, проверочная матрица которого выглядит следующим образом:

$$H = \begin{bmatrix} H_{0,0} & H_{0,1} & \ldots & H_{0,I-1} \\ H_{1,0} & H_{1,1} & \ldots & H_{1,I-1} \\ \vdots & \vdots & \ddots & \vdots \\ H_{J-1,0} & H_{J-1,1} & \ldots & H_{J-1,I-1} \end{bmatrix},$$

где $H \in \mathbb{F}_2^{Jr\times Ir}$, и каждая подматрица $H_{i,j} \in \mathbb{F}_2^{r\times r}$ может быть либо циркулянтной перестановочной матрицей, либо нулевой матрицей.

Обозначим через $\mathfrak{C}_{t,s}$ класс квазициклических низкоплотностных кодов, в каждом столбце проверочной матрицы которых количество единиц не меньше чем t, и не больше, чем s. Будем называть $(0,1)$-*матрицей* целочисленную матрицу, состоящую из нулей и единиц.

Определение 2. *Весовой матрицей* для $H \in \mathbb{F}_2^{Jr\times Ir}$ называется $(0,1)$-матрица $\mathrm{wt}(H) = (b_{i,j})_{J\times I}$, где $b_{i,j}$ равно единице в случае, когда $H_{i,j}$ — это циркулянтная перестановочная матрица, и нулю иначе.

Рассмотрим свойства проверочной матрицы квазициклического низкоплотностного кода. Для проверочной матрицы $H \in \mathbb{F}_2^{Jr\times Ir}$ кода $\mathfrak{C}_{t,s}$ можно определить некоторые ее характеристики, общие с соответствующей ей весовой матрицей $B = (b_{i,j})_{J\times I}$. Рассмотрим i-й столбец матрицы H. Каждая единица данного столбца входит ровно в одну циркулянтную перестановочную матрицу, которая в свою очередь дает одну единицу в матрице B, если же $H_{i,j}$ — нулевая матрица, то $b_{i,j}$ равно нулю. В таком случае справедливо следующее утверждение:

Лемма 1. *Для квазициклического низкоплотностного кода, заданного проверочной матрицей $H \in \mathbb{F}_2^{Jr\times Ir}$, количество единиц в ее столбце равно количеству единиц в соответствующем столбце матрицы $B = \mathrm{wt}(H)$.*

Заметим также, что аналогичное утверждение справедливо и для строк.

Определение 3. *Перманентом* целочисленной матрицы $A = (a_{i,j})_{n\times n}$ будем называть величину

$$\mathrm{perm}(A) = \sum_{\sigma} \prod_{j\in[n]} a_{j,\sigma(j)},$$

где сумма берется по всем $n!$ перестановкам σ множества $[n] = \{1,\dots,n\}$.

Пусть задана целочисленная матрица $A = (a_{i,j})_{n\times n}$. Тогда для перманента этой матрицы справедливо следующее свойство [10]:

$$\mathrm{perm}(A) = \mathrm{perm}(A^T).$$

Пусть S произвольное подмножество множества $[I]$ мощности $J+1$, а $B = (b_{i,j})_{J\times I}$ некоторая целочисленная матрица. Через $B_{S\setminus i}$ обозначим ее подматрицу, составленную из столбцов с индексами из множества $S \setminus \{i\}$.

Пусть $\mathcal{C}$ квазициклический низкоплотностный код, заданный проверочной матрицей $H \in \mathbb{F}_2^{Jr\times Ir}$ и $B = \mathrm{wt}(H)$. В работе [7] приведена следующая оценка на минимальное расстояния данного кода:

$$d_{min}(\mathcal{C}) \leqslant \min_{\substack{S\subseteq[I]\\ |S|=J+1}}{}^{*} \sum_{i\in S} \mathrm{perm}(B_{S\setminus i}), \tag{1}$$

где под $\min^*$ понимается минимум по всем ненулевым значениям.

Поскольку $J \times J$ матрица $B_{S\setminus i}$ является $(0,1)$-матрицей, то из определения перманента непосредственно следует, что

$$\operatorname{perm}(B_{S\setminus i}) \leqslant J!.$$

Таким образом, из оценки 1 можно получить следующую оценку [7]:

$$d_{min}(\mathcal{C}) \leqslant (J+1)!. \tag{2}$$

Рассмотрим квазициклический низкоплотностный код $\mathcal{C} \in \mathfrak{C}_{t,s}$, заданный проверочной матрицей $H \in \mathbb{F}_2^{Jr\times Ir}$. Пусть количество единиц в строках матрицы H намного меньше, чем J. В этом случае оценка 2 будет сильно завышенной. Приведенная ниже теорема является обобщением оценки 2 и восполняет этот пробел.

Теорема 1. *Пусть задан некоторый квазициклический низкоплотностный код $\mathcal{C} \in \mathfrak{C}_{t,s}$ с проверочной матрицей $H \in \mathbb{F}_2^{Jr\times Ir}$. Тогда для его минимального расстояния справедлива оценка:*

$$d_{min}(\mathcal{C}) \leqslant (J+1)s!^{J/t}.$$

Доказательство. Пусть $(0,1)$-матрица $B = (b_{i,j})_{J\times I}$ является весовой матрицей для H. Воспользуемся оценкой 1:

$$d_{min}(\mathcal{C}) \leqslant \min_{\substack{S\subseteq[I]\\|S|=J+1}}{}^{*} \sum_{i\in S} \operatorname{perm}(B_{S\setminus i}). \tag{3}$$

Согласно свойству перманента $\operatorname{perm}(A^T) = \operatorname{perm}(A)$. Используя неравенство 3 получим:

$$d_{min}(\mathcal{C}) \leqslant \min_{\substack{S\subseteq[I]\\|S|=J+1}}{}^{*} \sum_{i\in S} \operatorname{perm}(B^T_{S\setminus i}). \tag{4}$$

Как доказано в [10], для $(0,1)$-матрицы $A = (a_{i,j})_{n\times n}$ с количеством единиц в i-й строке, равным r_i, справедливо следующее неравенство:

$$\operatorname{perm}(A) \leqslant \prod_{i=1}^{n} r_i!^{1/r_i}. \tag{5}$$

Из леммы 1 следует, что для рассматриваемого кода $\mathcal{C} \in \mathfrak{C}_{t,s}$ количество единиц в весовой матрице B не менее, чем t, и не более, чем s. Воспользовавшись этим фактом и оценкой 5 получим неравенство:

$$\operatorname{perm}(B^T_{S\setminus i}) \leqslant \prod_{i=1}^{J} s!^{1/t}. \tag{6}$$

Воспользовавшись неравенством 4 и неравенством 6, получим:

$$d_{min}(\mathcal{C}) \leqslant \min_{\substack{S\subseteq[I]\\|S|=J+1}}{}^{*} \sum_{i\in S} s!^{J/t} \leqslant (J+1)s!^{J/t},$$

что доказывает данную теорему.

Заключение

Основным результатом данной работы является оценка, полученная в теореме 1, на минимальное расстояние квазициклического низкоплотностного кода, заданного проверочной матрицей $H \in \mathbb{F}_2^{Jr\times Ir}$, число единиц в каждом столбце которой не меньше чем t, и не больше чем s. Она улучшает известную оценку (2) на случай проверочных матриц, в которых верхняя граница s на количество единиц в столбцах значительно меньше, чем количество циркулянтных строк J. При этом оценка (2) является частным случаем полученной в работе оценки, если положить $s = t = J$.

Автор выражает признательность своему научному руководителю сотруднику кафедры математической теории интеллектуальных систем механико-математического факультета МГУ к.ф.-м.н. П. А. Пантелееву за помощь во время работы над статьей.

Список литературы

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

[2] MacKay D. J. C., Neal R. M. Good codes based on very sparse matrices // Cryptography and Coding. Ser. Lecture Notes in Computer Science / C. Boyd, Ed. — Berlin, Heidelberg: Springer, 1995. — Vol. 1025. — P. 100–111.

[3] Wiberg N. Codes and decoding on general graphs: Ph.D. dissertation. — Department of Electrical Engineering, Linköping University, Sweden, 1996.

[4] Townsend R., Weldon E. Self-orthogonal quasi-cyclic codes // Information Theory, IEEE Transactions on. — 1982. Vol. 13, no. 2. — P. 183–195.

[5] Kasami T. A gilbert-varshamov bound for quasi-cycle codes of rate 1/2 // Information Theory, IEEE Transactions on. — 1974. Vol. 20, no. 5. — P. 679.

[6] Fossorier M. P. C. Quasicyclic low-density parity-check codes from circulant permutation matrices // Information Theory, IEEE Transactions on. — 2004. Vol. 50, no. 8. — P. 1788–1793.

[7] Smarandache R., Vontobel P. Quasi Cyclic LDPC Codes: Influence of Proto-and Tanner-Graph Structure on Minimum Hamming Distance Upper Bounds // IEEE Trans. Inf. Theory. — Jan. 26, 2009. — P. 585–607.

[8] Vardy A. The intractability of computing the minimum distance of a code // IEEE Trans. Inf. Theory. — 1997. Vol. 43, Iss. 6. — P. 1757–1766.

[9] MacKay D. J. C., Davey M. C. Evaluation of Gallager codes for short block length and high rate applications // Codes, Systems and Graphical Models. — 2001. Vol. 123. — P. 113–130.

[10] Минк Х. Перманенты. М.: Мир, 1982. С. 110–116.