УДК 004.032.2: 004.932

ОЦЕНКА МИНИМАЛЬНОЙ ДЛИНЫ ЦИКЛОВ КВАЗИЦИКЛИЧЕСКИХ РЕГУЛЯРНЫХ КОДОВ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ

Ф. И. Иванов,
аспирант
В. В. Зяблов,
доктор техн. наук, профессор
В. Г. Потапов,
канд. техн. наук, старший научный сотрудник
Институт проблем передачи информации им. А. А. Харкевича, Москва

Доказывается условие отсутствия циклов длины 4 в проверочных матрицах регулярных квазициклических МПП-кодов, построенных на матрицах перестановок. В соответствии с доказанными теоремами построен ансамбль двоичных МПП-кодов, минимальная длина циклов которых равна 6. Представлены результаты моделирования полученных кодовых конструкций для итеративного алгоритма декодирования «распространения доверия» (Sum-Product) при передаче кодового слова по двоичному каналу с аддитивным белым гауссовым шумом.

Ключевые слова *— МПП-код, циклы, матрица перестановок, циклический сдвиг.*

Введение

Двоичные коды с малой плотностью проверок на четность (МПП-коды) были предложены Галлагером [1]. Данные коды являются линейными блоковыми кодами, задаваемыми с помощью проверочной матрицы **H**, характеризуемой относительно малым числом единиц в строках и столбцах. Часто МПП-коды удобно интерпретировать как графы Таннера, в которых для представления строк и столбцов проверочной матрицы используются определенным образом связанные между собой битовые и проверочные узлы.

В настоящее время построены МПП-коды, способные работать в 0,045 дБ от границы Шеннона [2].

К главным недостаткам МПП-кодов можно отнести квадратичную зависимость сложности кодирования от длины кода, хотя существуют подходы, позволяющие при тщательном предварительном проектировании снизить сложность кодирования до линейной [3].

Важной характеристикой матрицы МПП-кода является отсутствие циклов определенной длины. Под циклом длины 4 понимают образование в проверочной матрице прямоугольника, в углах которого стоят единицы. Отсутствие цикла длины 4 можно также определить через скалярное произведение столбцов (или строк) матрицы. Если каждое попарное скалярное произведение всех столбцов (или строк) матрицы не более 1, это говорит об отсутствии цикла длины 4. Циклы больших длин определяются минимальной длиной цикла в графе Таннера.

Существует ряд работ, посвященных алгоритмам поиска циклов минимальных длин в проверочных матрицах МПП-кодов, особо следует отметить работы [4–7].

В некоторых случаях, например, если МПП-код является квазициклическим, можно сформулировать условия отсутствия циклов определенных длин [8–10].

Следуя работе [8], мы рассмотрим ансамбль двоичных квазициклических МПП-кодов, основанных на матрицах перестановок, и докажем необходимое и достаточное условие отсутствия в них циклов длины 4.

Основные определения и обозначения

Приведем основные определения и обозначения, которые будут использоваться в статье.

Произведением Адамара матриц, $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$, назовем матрицу $\mathbf{C} = \mathbf{A} \Diamond \mathbf{B} = (c_{ij})$, где $c_{ij} = a_{ij} b_{ij}$.

Отметим, что для существования произведения Адамара матриц $\mathbf{A} = (a_{ij})$ и $\mathbf{B} = (b_{ij})$ требуется, чтобы они имели одинаковое число строк и столбцов.

Матрицей h-кратного циклического сдвига $\mathbf{I}_h$ назовем квадратную матрицу, которая соответствует h-кратному правому циклическому сдвигу столбцов единичной матрицы $\mathbf{I}$: $\dim \mathbf{I} = \dim \mathbf{I}_h = m$.

Далее мы сформулируем элементарные утверждения о матрицах циклических сдвигов, которые понадобятся нам для дальнейшего анализа:

1) $\mathbf{I}_t = \mathbf{I}_s \leftrightarrow t = s$;

2) если $\mathbf{I}_s$ и $\mathbf{I}_t$ — матрицы s-кратного и t-кратного циклического сдвига соответственно, то

$$\mathbf{I}_t \Diamond \mathbf{I}_s = \begin{cases} \mathbf{0}, t \neq s \\ \mathbf{I}_t, t = s \end{cases};$$

3) если $\dim \mathbf{I}_h = m$, то $(\mathbf{I}_h)^{-1} = \mathbf{I}_{m-h}$;

4) если $\dim \mathbf{I}_t = \dim \mathbf{I}_s = m$, то

$$\mathbf{I}_t \mathbf{I}_s = \mathbf{I}_s \mathbf{I}_t = \mathbf{I}_{(t+s) \bmod m}.$$

Теперь введем определение квазициклического регулярного (l, n_0) МПП-кода.

Пусть $\mathbf{I}_{p_{ij}}$ — $m \times m$ матрица p_{ij}-кратного циклического сдвига, $1 \le i \le l$, $1 \le j \le n_0$. Построим $l \times n_0$ матрицу $\mathbf{H}$ следующего вида:

$$\mathbf{H} = \begin{pmatrix} \mathbf{I}_{p_{11}} & \dots & \mathbf{I}_{p_{1n_0}} \\ \dots & \dots & \dots \\ \mathbf{I}_{p_{l1}} & \dots & \mathbf{I}_{p_{ln_0}} \end{pmatrix}.$$

Размерность $\mathbf{I}_{p_{ij}}$ — $m \times m$, поэтому размерность $\mathbf{H}$ — $ml \times mn_0$. $\mathbf{H}$ определяет *ансамбль регулярных квазициклических МПП-кодов* длины $n = mn_0$. Обозначим этот ансамбль $\varepsilon_Q(l, n_0, m)$. Элементы ансамбля получаются путем равновероятного выбора (возможно, с возвращениями) матриц p_{ij}-кратных циклических сдвигов.

Формулировка и доказательство основного результата

В работе [8] доказано, что блочная матрица вида $\begin{pmatrix} \mathbf{R} & \mathbf{S} \\ \mathbf{P} & \mathbf{Q} \end{pmatrix}$ не содержит циклов длины 4 тогда и только тогда, когда $(\mathbf{PR}^{\mathrm{T}}) \Diamond (\mathbf{QS}^{\mathrm{T}}) \neq \mathbf{0}$. Пусть

$$\mathbf{P} = \mathbf{I}_{p_1},\ \mathbf{R} = \mathbf{I}_{p_2},\ \mathbf{Q} = \mathbf{I}_{p_3},\ \mathbf{S} = \mathbf{I}_{p_4}.$$

Тогда $(\mathbf{PR}^{\mathrm{T}}) \Diamond (\mathbf{QS}^{\mathrm{T}}) \neq \mathbf{0}$ эквивалентно следующему условию:

$$\left(\mathbf{I}_{p_1} \mathbf{I}_{p_2}^{\mathrm{T}}\right) \Diamond \left(\mathbf{I}_{p_3} \mathbf{I}_{p_4}^{\mathrm{T}}\right) \neq \mathbf{0}. \qquad (1)$$

Воспользуемся тем, что $\mathbf{I}_{p_j}$ — ортогональная матрица, т. е. $\mathbf{I}_{p_j}^{\mathrm{T}} = \mathbf{I}_{p_j}^{-1}$. С другой стороны, $\mathbf{I}_{p_j}^{-1} = \mathbf{I}_{m-p_j}$, тогда условие (1) примет вид

$$(\mathbf{I}_{p_1} \mathbf{I}_{m-p_2}) \Diamond (\mathbf{I}_{p_3} \mathbf{I}_{m-p_4}) \neq \mathbf{0}.$$

Воспользовавшись утверждением 4, получим

$$(\mathbf{I}_{p_1+m-p_2 \bmod m}) \Diamond (\mathbf{I}_{p_3+m-p_4 \bmod m}) \neq \mathbf{0}.$$

По утверждению 2 это означает, что

$$(p_1 + m - p_2) \bmod m \neq (p_3 + m - p_4) \bmod m.$$

Всегда можно считать, что $p_2 > p_1$ и $p_4 > p_3$, тогда окончательно получим

$$p_2 - p_1 \neq p_4 - p_3. \qquad (2)$$

Соотношение (2) назовем *уравнением неравномерности*, а блочную матрицу, для которой выполняется уравнение неравномерности, — *неравномерной матрицей*.

Таким образом, доказана теорема.

Теорема 1. Блочная матрица $\begin{pmatrix} \mathbf{R} & \mathbf{S} \\ \mathbf{P} & \mathbf{Q} \end{pmatrix}$ не содержит циклов длины 4 тогда и только тогда, когда она является неравномерной.

Отметим, что уравнение неравномерности является также условием невырожденности блочной квадратной матрицы, а именно детерминант матрицы $\begin{pmatrix} \mathbf{R} & \mathbf{S} \\ \mathbf{P} & \mathbf{Q} \end{pmatrix}$ (в блочном смысле) равен $\mathbf{RQ} - \mathbf{PS}$. Пусть

$$\mathbf{P} = \mathbf{I}_{p_1},\ \mathbf{R} = \mathbf{I}_{p_2},\ \mathbf{Q} = \mathbf{I}_{p_3},\ \mathbf{S} = \mathbf{I}_{p_4},$$

тогда

$$\mathbf{RQ} - \mathbf{PS} = \mathbf{I}_{p_2} \mathbf{I}_{p_3} - \mathbf{I}_{p_1} \mathbf{I}_{p_4} =$$
$$= \mathbf{I}_{(p_2+p_3) \bmod m} - \mathbf{I}_{(p_1+p_4) \bmod m}.$$

Поэтому условие $\det \begin{pmatrix} \mathbf{R} & \mathbf{S} \\ \mathbf{P} & \mathbf{Q} \end{pmatrix} \neq \mathbf{0}$ можно представить в следующем виде:

$$\mathbf{I}_{(p_2+p_3) \bmod m} \neq \mathbf{I}_{(p_1+p_4) \bmod m},$$

$$(p_2 + p_3) \bmod m \neq (p_1 + p_4) \bmod m,$$

$$p_2 - p_1 \neq p_4 - p_3.$$

Мы вновь получили уравнение (2).

Таким образом, условие неравномерности равносильно условию невырожденности блочного детерминанта.

В работе [8] доказано, что матрица

$$\mathbf{H} = \begin{pmatrix} \mathbf{I}_{p_{11}} & \dots & \mathbf{I}_{p_{1n_0}} \\ \dots & \dots & \dots \\ \mathbf{I}_{p_{l1}} & \dots & \mathbf{I}_{p_{ln_0}} \end{pmatrix}$$

не содержит циклов длины 4 тогда и только тогда, когда не содержит циклов длины 4 любая ее подматрица вида $\begin{pmatrix} \mathbf{I}_{p_{i1j1}} & \mathbf{I}_{p_{i1j2}} \\ \mathbf{I}_{p_{i2j1}} & \mathbf{I}_{p_{i2j2}} \end{pmatrix}$. Таким образом, справедлива следующая теорема.

Теорема 2. Проверочная матрица

$$\mathbf{H}=\begin{pmatrix}\mathbf{I}_{p_{11}} & \dots & \mathbf{I}_{p_{1n_0}}\\ \dots & \dots & \dots\\ \mathbf{I}_{p_{l1}} & \dots & \mathbf{I}_{p_{ln_0}}\end{pmatrix}$$

квазициклического МПП-кода не содержит циклов длины 4 тогда и только тогда, когда любая ее подматрица вида $\begin{pmatrix}\mathbf{I}_{p_{i1j1}} & \mathbf{I}_{p_{i1j2}}\\ \mathbf{I}_{p_{i2j1}} & \mathbf{I}_{p_{i2j2}}\end{pmatrix}$ является неравномерной (имеет невырожденный блочный детерминант).

Конструкция квазициклического МПП-кода, не содержащего циклов длины 4

Далее мы приведем пример конструкции проверочной матрицы МПП-кода и докажем, что она не содержит циклов длины 4.

Пусть $b_1 \in N$, $(b_1, m) = 1$, где $(\cdot,\cdot)$ — наибольший общий делитель, $\mathrm{ord}(b_1) = x > l$. Построим столбец $\mathbf{P}_1$, состоящий из матриц циклического сдвига:

$$\mathbf{P}_1=\begin{pmatrix}\mathbf{I}_{b_1}\\ \mathbf{I}_{b_1^2}\\ \mathbf{I}_{b_1^3}\\ \dots\\ \mathbf{I}_{b_1^l}\end{pmatrix}.$$

Выберем $b_2 \in N$, $(b_2, m) = 1$, $b_2 \neq b_1^i \bmod m$, $i = 1 \dots l$. Построим столбец $\mathbf{P}_2$:

$$\mathbf{P}_2=\begin{pmatrix}\mathbf{I}_{b_1b_2}\\ \mathbf{I}_{b_1^2b_2}\\ \mathbf{I}_{b_1^3b_2}\\ \dots\\ \mathbf{I}_{b_1^lb_2}\end{pmatrix}.$$

Для $b_3 \in N$ потребуем выполнения всех условий, приведенных выше, кроме того, $b_3 \neq b_2b_1^i \bmod m$, $i = 1 \dots l$. Вообще для $b_j \in N$ необходимо выполнение $j-1$ системы соотношений:

$$\begin{cases} b_j \neq b_1^i \bmod m\\ b_j \neq b_2b_1^i \bmod m\\ b_j \neq b_3b_1^i \bmod m\\ \vdots\\ b_j \neq b_{j-1}b_1^i \bmod m\end{cases}. \qquad (3)$$

Тогда способом, описанным выше, построим столбцы $\mathbf{P}_3$, $\mathbf{P}_4$, ..., $\mathbf{P}_{n_0}$, где

$$\mathbf{P}_j=\begin{pmatrix}\mathbf{I}_{b_1b_j}\\ \mathbf{I}_{b_1^2b_j}\\ \mathbf{I}_{b_1^3b_j}\\ \dots\\ \mathbf{I}_{b_1^lb_j}\end{pmatrix}.$$

Тогда матрица

$$\mathbf{H}=(\mathbf{P}_1,\mathbf{P}_2,\dots,\mathbf{P}_{n_0})=\begin{pmatrix}\mathbf{I}_{b_1} & \mathbf{I}_{b_1b_2} & \dots & \mathbf{I}_{b_1b_{n_0}}\\ \mathbf{I}_{b_1^2} & \mathbf{I}_{b_1^2b_2} & \dots & \mathbf{I}_{b_1^2b_{n_0}}\\ \dots & \dots & \dots & \dots\\ \mathbf{I}_{b_1^l} & \mathbf{I}_{b_1^lb_2} & \dots & \mathbf{I}_{b_1^lb_{n_0}}\end{pmatrix}$$

определяет ансамбль регулярных квазициклических МПП-кодов длины $n = mn_0$, который мы обозначим $\varepsilon_{QM}(l, n_0, m)$. Очевидно, что $\varepsilon_{QM}(l, n_0, m)$ является подансамблем ансамбля $\varepsilon_Q(l, n_0, m)$. Элементы ансамбля $\varepsilon_{QM}(l, n_0, m)$ получаются путем случайного выбора без возвращений числа $b_1 \in N$, $(b_1, m) = 1$, $\mathrm{ord}(b_1) = x > l$, а также чисел b_j, $j = 1 \dots n_0$, удовлетворяющих системе (3). Указанный выше способ построения проверочной матрицы гарантирует, что все матрицы в каждой строке и каждом столбце будут различны (столбцы являются классами смежности).

Теперь докажем, что матрица $\mathbf{H}$ не содержит циклов длины 4: зафиксировав в матрице $\mathbf{H}$ любые строки с индексами $1 \le j1 \le j2 \le l$ и любые 2 столбца с индексами $1 \le k \le s \le n_0$, рассмотрим подматрицу $\mathbf{H}_1$ вида

$$\mathbf{H}_1=\begin{pmatrix}\mathbf{I}_{b_1^{j1}b_k} & \mathbf{I}_{b_1^{j1}b_s}\\ \mathbf{I}_{b_1^{j2}b_k} & \mathbf{I}_{b_1^{j2}b_s}\end{pmatrix}.$$

По теореме 1 отсутствие циклов в матрице $\mathbf{H}_1$ (а значит и в матрице $\mathbf{H}$) равносильно неравномерности $\mathbf{H}_1$. Для неравномерности $\mathbf{H}_1$ необходимо и достаточно, чтобы выполнялось следующее соотношение на коэффициенты:

$$\left(b_1^{j2}b_k - b_1^{j1}b_k\right)\bmod m \neq \left(b_1^{j2}b_s - b_1^{j1}b_s\right)\bmod m;$$

$$b_k\left(b_1^{j2} - b_1^{j1}\right)\bmod m \neq b_s\left(b_1^{j2} - b_1^{j1}\right)\bmod m;$$

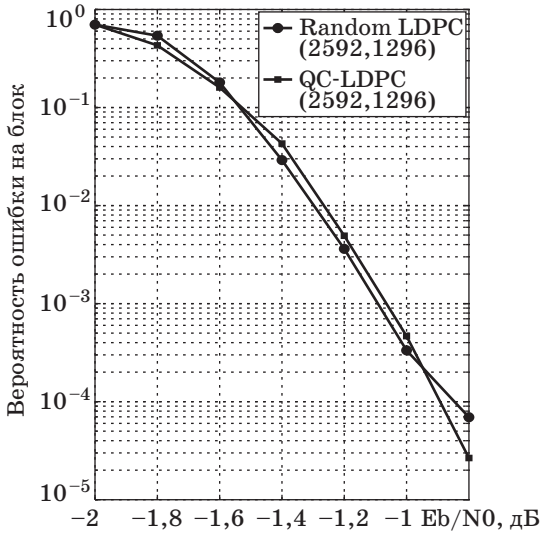
$$b_k \bmod m \neq b_s \bmod m.$$

Последнее условие всегда выполняется, так как все числа b_j, $j = 1 \dots n_0$, различны. Следовательно, матрица $\mathbf{H}_1$, а значит и матрица $\mathbf{H}$, не содержат циклов длины 4, т. е. минимальная длина циклов в них равна 6.

Результаты моделирования

Для генерации проверочных матриц МПП-кодов из ансамбля $\varepsilon_{QM}(l, n_0, m)$ была написана функция для MatLab. Моделирование производилось ме-

Eb/N0, дБ	Random LDPC (2592, 1296)	QM-LDPC (2592, 1296)
–2	$7 \cdot 10^{-1}$	$7 \cdot 10^{-1}$
–1,8	$5{,}4 \cdot 10^{-1}$	$4{,}3 \cdot 10^{-1}$
–1,6	$1{,}8 \cdot 10^{-1}$	$1{,}6 \cdot 10^{-1}$
–1,4	$2{,}9 \cdot 10^{-2}$	$4{,}3 \cdot 10^{-2}$
–1,2	$3{,}6 \cdot 10^{-3}$	$4{,}9 \cdot 10^{-3}$
–1	$3{,}3 \cdot 10^{-4}$	$4{,}7 \cdot 10^{-4}$
–0,8	$6{,}9 \cdot 10^{-5}$	$2{,}7 \cdot 10^{-5}$



■ Зависимость вероятности ошибки на блок от отношения сигнал/шум для случайного кода Галлагера и кода из ансамбля $\varepsilon_{QM}(l, n_0, m)$

тодами имитационного моделирования с использованием среды MatLab. В качестве канала был выбран двоичный канал с аддитивным белым гауссовым шумом. В качестве алгоритма декодирования был выбран итеративный алгоритм Sum-Product с «мягким» входом, работающий с представлением кода в виде двудольного графа Таннера [11]. Максимальное число итераций ограничивалось 50.

Результат моделирования (таблица и рисунок) показывает, что код из ансамбля $\varepsilon_{QM}(l, n_0, m)$ не уступает по корректирующим способностям коду из ансамбля Галлагера [1], в то же время код из ансамбля $\varepsilon_{QM}(l, n_0, m)$ имеет более простую реализацию, а также требует хранения только шести чисел $b_1, b_2, ..., b_6$. Следует также отметить, что код из ансамбля $\varepsilon_{QM}(l, n_0, m)$ при отношении сигнал/шум –0,8 дБ превосходит по корректирующим способностям случайный код более чем на треть порядка, что говорит о возможности его практического применения.

Заключение

В данной работе предложен простой способ исследования проверочной матрицы **H** квазициклического МПП-кода на наличие в ней циклов длины 4. Предложен способ построения ансамбля квазициклических МПП-кодов, минимальная длина циклов в котором равна 6. Результаты компьютерного моделирования позволяют сделать вывод о том, что полученные кодовые конструкции не уступают кодам из ансамбля Галлагера [1].

Литература

1. **Галлагер Р. Дж.** Коды с малой плотностью проверок на четность. — М.: Мир, 1966. — 90 с.
2. **MacKay D. J. C., Neal R. M.** Near Shannon limit performance of low density parity check codes // IEEE Electronics Letters. 1996. Vol. 32. N 18. P. 1645–1646.
3. **Richardson T., Urbanke R.** Efficient encoding of low density parity check codes // IEEE Trans. Inform. Theory. 2001. Vol. 47. P. 638–656.
4. **Kim S., No J.-S., Chung H., Shin D.-J.** Girth analysis of Tanner's (3,5) QC LDPC codes // Proc. of IEEE Intern. Symp. on Information Theory (ISIT'05). 2005. P. 1632–1636.
5. **Djidjev Hristo N.** A faster algorithm for computing the girth of planar and bounded genus graphs // ACM Transactions on Algorithms (TALG). 2010. Vol. 7. N 1. P. 1–16.
6. **Xiaofu Wu, Xiaohu You, Chunming Zhao.** An Efficient Girth-Locating Algorithm for Quasi-Cyclic LDPC Codes // Proc. of IEEE Intern. Symp. on Information Theory (ISIT'06). 2006. P. 817–820.
7. **Lu J., Moura M. F., Niesen U.** Grouping-and-shifting designs for structured LDPC codes with large girth // Proc. of IEEE Intern. Symp. on Information Theory (ISIT'04). 2004. P. 236.
8. **Gabidulin E., Moinian A., Honary B.** Generalized construction of quasi-cyclic regular LDPC codes based on permutation matrices // Proc. of IEEE Intern. Symp. on Information Theory (ISIT'06). 2006. P. 679–683.
9. **Vasic B., Pedagani K., Ivkovic M.** High-rate girth-eight low-density parity-check codes on rectangular integer lattices // IEEE Transactions on Communications. 2004. Vol. 52. N 8. P. 1248–1252.
10. **Zhang H., Moura M. F.** The design of structured regular LDPC codes with large girth // Proc. of IEEE Global Telecommunications Conf. (GLOBECOM'03). 2003. Vol. 7. P. 4022–4027.
11. **Kschischang F. R., Frey B. J., Loeliger H. A.** Factor graphs and the sum-product algorithm // IEEE Trans. Inform. Theory. 2001. Vol. 47. N 2. P. 498–519.