Информационные процессы, Том 18, № 2, 2018, стр. 125–134

ПЕРЕДАЧА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Метод построения проверочных матриц квазициклических кодов с малой плотностью проверок над полем GF(q) [1]

С.А. Круглик[*,**], **В.С. Потапова**[*,**], **А.А. Фролов**[*,**]

[*] *Сколковский институт науки и технологий, Москва, Россия*

[**] *Институт проблем передачи информации, Российская академия наук, Москва, Россия*

Поступила в редколлегию 8.06.2018

Аннотация—Предложен алгоритм построения проверочных матриц квазициклических кодов с малой плотностью проверок (КЦ МПП-коды) над полем GF(q). Алгоритм состоит из двух шагов. На первом шаге на основе анализа порога итеративого декодирования выбирается базовая матрица (протограф). На втором шаге алгоритм находит короткие циклы в базовой матрице и пытается их разрушить путем выбора циркулянтов и элементов поля GF(q). В первую очередь алгоритм старается разрушить циклы с наименьшим числом ребер, выходящих наружу цикла. Эффективность алгоритма продемонстрирована с помощью имитационного моделирования. С целью объяснения полученных результатов нами была выведена верхняя граница на кодовое расстояние КЦ МПП-кодов над над полем GF(q).

КЛЮЧЕВЫЕ СЛОВА: МПП-код, проверочная матрица, порог итеративного декодирования, граф Таннера, цикл, поле Галуа.

1. ВВЕДЕНИЕ

В данной работе мы рассматриваем проблему построения проверочных матриц квазициклических МПП-кодов над полем GF(q). КЦ МПП-коды предложены в [1, 2]. Эти коды являются важным классом МПП-кодов [3, 4]. Также КЦ МПП-коды являются подклассом МПП-кодов на протографах [5]. Такие коды просты в описании, для них есть эффективные алгоритмы кодирования [6] и декодирования, основанные на алгоритме распространения доверия [7]. Все это делает эти коды популярными для применения в практических приложениях.

МПП-коды над полем GF(q) впервые рассмотрены в работе [8]. Такие коды значительно превосходят двоичные аналоги по помехоустойчивости особенно в случае пакетов ошибок и модуляций высокой кратности [8, 9]. Однако, необходимо отметить, что сложность декодирования таких кодов больше сложности декодирования двоичных МПП-кодов [10–12].

Существует большое количество методов построения проверочных матриц двоичных КЦ МПП-кодов [13–17]. В данной работе мы обобщим эти методы на недвоичный случай. В качестве дополнительного результата мы получим новую верхнюю границу на кодовое расстояние КЦ МПП-кодов над полем GF(q) и воспользуемся ею для объяснения поведения полученных кодов

Основные результаты работы заключаются в следующем. Предложен алгоритм построения проверочных матриц квазициклических кодов с малой плотностью проверок (КЦ МПП-коды) над полем GF(q). Алгоритм состоит из двух шагов. На первом шаге на основе анализа порога итеративого декодирования выбирается базовая матрица (протограф). На втором шаге алгоритм находит короткие циклы в базовой матрице и пытается их разрушить путем выбора

[1] Работа выполнена за счет гранта Российского научного фонда (проект No 18-19-00673).

циркулянтов и элементов поля $\mathrm{GF}(q)$. В первую очередь алгоритм старается разрушить циклы с наименьшим числом ребер, выходящих наружу цикла. Эффективность алгоритма продемонстрирована с помощью имитационного моделирования. С цель объяснения экспериментальных результатов была получена новая верхняя граница на кодовое расстояние КЦ МПП-кодов над полем $\mathrm{GF}(q)$

2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Рассмотрим следующую двоичную матрицу размера $m \times n$

$$\mathbf{H}_{\text{base}} = [h_{i,j}] \in \{0,1\}^{m \times n}.$$

Эту матрицу мы будем называть базовой матрицей. Данная матрица является матрицей смежности протографа.

Построим проверочную матрицу $\mathbf{H}$ НД КЦ МПП-кода $\mathcal{C}$. Для этого расширим матрицу $\mathbf{H}_{\text{base}}$ циклическими матрицами (циркулянтами), умноженными на ненулевые элементы поля $\mathrm{GF}(q)$, т.е.

$$\mathbf{H} = \begin{bmatrix} \alpha_{1,1}\mathbf{P}_{1,1} & \alpha_{1,2}\mathbf{P}_{1,2} & \cdots & \alpha_{1,n}\mathbf{P}_{1,n} \\ \alpha_{2,1}\mathbf{P}_{2,1} & \alpha_{2,2}\mathbf{P}_{2,2} & \cdots & \alpha_{2,n}\mathbf{P}_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m,1}\mathbf{P}_{m,1} & \alpha_{m,2}\mathbf{P}_{m,2} & \cdots & \alpha_{m,n}\mathbf{P}_{m,n} \end{bmatrix} \in \mathrm{GF}(q)^{ms \times ns},$$

где $\mathbf{P}_{i,j}$ – двоичный циркулянт размера $s \times s$ веса[1] $h_{i,j}$, $i = 1, \ldots, m$; $j = 1, \ldots, n$. $\alpha_{i,j} \in \mathrm{GF}(q) \backslash \{0\}$, $i = 1, \ldots, m$; $j = 1, \ldots, n$.

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

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

Пусть $\mathrm{GF}(q)$ некоторое поле, а $\mathrm{GF}(q)[\mathrm{x}]$ кольцо полиномов с коэффициентами из $\mathrm{GF}(q)$. Т.к. кольцо циркулянтов размера $s \times s$ над $\mathrm{GF}(q)$ изоморфно факто-кольцу

$$GF(q)^{(s)}[x] = GF(q)[x] / \left(x^s - 1\right),$$

то сопоставим проверочной матрице $\mathbf{H}$ полиномиальную проверочную матрицу $\mathbf{H}(x)$ размера $m \times n$:

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

где $p_{i,j}(x) = \sum_{t=1}^{s} \mathbf{P}_{i,j}(t,1)x^{t-1}$, а $\mathbf{P}_{i,j}(t,1)$ – элемент на перечечении t-го строки и первого столбца матрицы $\mathbf{P}_{i,j}$.

Пример 1. Рассмотрим следующую базовую матрицу

$$\mathbf{H}_{\text{base}} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

[1] Весом циркулянта называется вес его первой строки.

При расширении каждая единица заменяется на пару (z, β), где z – это номер циркулянта (величина сдвига), а β – это ненулевой элемент поля $\mathrm{GF}(q)$. Например, мы можем получить такую матрицу

$$\mathbf{H}_{\exp} = \begin{bmatrix} -- & (2,1) & (1,2) \\ (0,1) & -- & (2,3) \end{bmatrix}.$$

Отметим, что $\mathbf{H}_{\exp}$ соответствует такой проверочной матрице

$$\mathbf{H} = \left[\begin{array}{ccc|ccc|ccc} 0&0&0&0&1&0&0&0&2 \\ 0&0&0&0&0&1&2&0&0 \\ 0&0&0&1&0&0&0&2&0 \\ \hline 1&0&0&0&0&0&0&3&0 \\ 0&1&0&0&0&0&0&0&3 \\ 0&0&1&0&0&0&3&0&0 \end{array}\right].$$

Замечание 1. Отметим, что элементы циркулянта умножаются на один и тот же элемент поля $\mathrm{GF}(q)$. Это очень важно для практической реализации этих кодов, так как проверочные матрицы занимают малый объем памяти и могут эффективно храниться. Также предложенная конструкция проверочных матриц допускает параллельную реализацию алгоритмов кодирования и декодирования.

Сопоставим вектор

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

где

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

с вектором 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

$$\mathbf{H}\mathbf{c}^T = \mathbf{0} \quad (\text{в кольце } \ GF(q))$$

эквивалентно

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

Под весом полинома $f(x)$ мы понимаем число его ненулевых коэффициентов и обозначаем как $||f(x)||$. Определим вес вектора полиномов $\mathbf{c}(x) = (c_1(x), c_2(x), \ldots, c_n(x))$ как

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

3. МИНИМАЛЬНОЕ КОДОВОЕ РАССТОЯНИЕ

Обозначим минимальное расстояние кода $\mathcal{C}$ как $D(\mathcal{C})$. Пусть

$$\mathbf{H}_{\text{base}}^{(q)} = [\alpha_{i,j} h_{i,j}].$$

Обозначим через d^* минимальное расстояние кода над $\mathrm{GF}(q)$ с проверочной матрицей $\mathbf{H}_{\text{base}}^{(q)}$, максимизированное над всеми возможными комбинациями $\alpha_{i,j}$, $i = 1, \ldots, m$, $j = 1, \ldots, n$).

Теорема 1. *Пусть $\mathcal{C}$ КЦ МПП код над GF(q) с проверочной матрицей $\mathbf{H}_{base}$, тогда*

$$D(\mathcal{C}) \leq d^* s. \tag{1}$$

Доказательство. Пусть c^{base} – кодовое слова веса d^* кода с проверочной матрицей $\mathbf{H}^{(q)}_{\text{base}}$, $S = \text{supp}(c^{\text{base}})$ и $f_i(x) = c_i^{\text{base}} \sum_{j=0}^{s-1} x^j$. Построим кодовое слово $\mathbf{c}(x) \in \mathcal{C}$. Для $i = 1, \ldots, n$

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

Остоется заметить что $x^j f_i(x) = f_i(x)\ \forall j = 0, \ldots, s-1, \forall i = 1, \ldots, n$, hence

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

Пусть $\mathbf{A}$ матрица размера $M \times N$, $I \subseteq \{1, 2, \ldots, M\}$ подмножество строк, $J \subseteq \{1, 2, \ldots, N\}$ подмножество столбцов. Обозначим через $\mathbf{A}_{I,J}$ подматрицу матрицы $\mathbf{A}$, содержащую строки и столбцы только из I и J соответственно. В случае если $I = \{1, 2, \ldots, M\}$ обозначим $\mathbf{A}_{I,J}$ через $\mathbf{A}_J$.

Перед выводом границы обобщим лемму, описывающую процесс построения кодовых слов КЦ МПП-кода над GF(q) из [19, 20]

Лемма 1. *Пусть $\mathcal{C}$ КЦ МПП-код над GF(q) с полиномиальной матрицей $\mathbf{H}(x)$. Пусть $J \subset \{1, 2, \ldots, n\}$, $|J| = m + 1$ и $\Delta_j(x) = \det\left(\mathbf{H}_{\mathbf{J}\setminus\{\mathbf{j}\}}(x)\right)$, 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 $\mathcal{C}$.

Доказательство. Покажем что $\mathbf{s}(x) = \mathbf{H}(x)\mathbf{c}^T(x) = \mathbf{0}$ в кольце $GF(q)^{(s)}[x]$. Ниже приведем доказательство только для первого элемента синдрома

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

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

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

как матрица, содержащая две одинаковых строки. Доказательство для остальных элементов синдрома аналогично.

Введем обозначение $\bar{l}(t_1, t_2)$. Упорядочим столбцы матрицы $\mathbf{H}_{base}$ в порядке возрастания весов т.е. первый столбец имеет минимальный вес, тогда как последний – максимальный. В

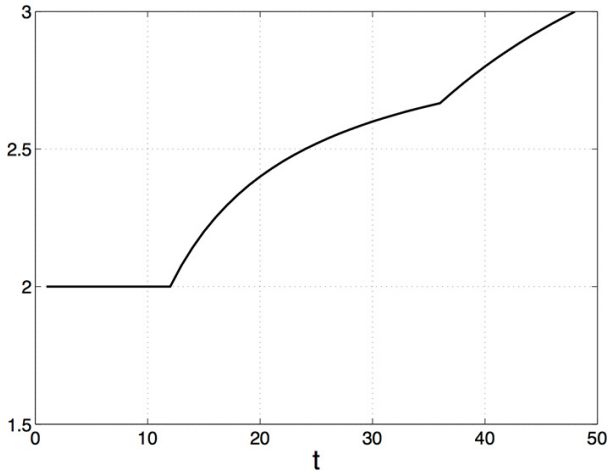

Рис. 1. Зависимость $\bar{l}(2,t)$

дальнейшем будем предполагать что столбцы матрицы $\mathbf{H}_{base}$ упорядочены в данном порядке. Пусть l_j- вес j-го столбца $\mathbf{H}_{base}$, $t_2 > t_1$, тогда

$$\bar{l}(t_1,t_2) = \frac{1}{t_2 - t_1 + 1} \sum_{i=t_1}^{t_2} l_i.$$

Пусть $l_{\max}$ и $l_{\min}$ являются максимальным и минимальным весом столбцов матрицы $\mathbf{H}_{base}$ соответственно (в нашем случае, в соответствии с введенным упорядочением, $l_{\max} = l_n$ и $l_{\min} = l_1$).

Пример 2. Рассмотрим матрицу $\mathbf{H}_{base}$ с $n = 48$. Пусть полином распределения весов столбцов для нее имеет вид $\Lambda(x) = 12x^2 + 24x^3 + 12x^4$

Напоминим, что

$$\Lambda(x) = \sum_{i=1}^{l_{\max}} \Lambda_i x^i,$$

где Λ_i – число столбцов веса i [21].

Зависимость $\bar{l}(2,t)$ для данного случая представлена на рисунке Рис. 1.

Теорема 2. *Пусть $\mathcal{C}$ КЦ МПП-код над GF(q) с базовой матрицей $\mathbf{H}_{base}$ размера $m \times n$,и пусть k такое целое число, что $0 \le k \le m$ и $\ell = \bar{l}(2, m+1-k)$ тогда*

$$D(\mathcal{C}) \le (m+1)k!\ell^{m-k}. \tag{2}$$

Доказательство. Напомним, что столбцы матрицы $\mathbf{H}_{base}$ упорядочены в порядке возрастания. Пусть $J = \{1, 2, \ldots, m+1\}$. Построим кодовое слово $\mathbf{c}(x)$ в соответствии с леммой 1. При этом последние $n - |J|$ позиций $\mathbf{c}(x)$ равны нулю.

Рассмотрим $\Delta_1(x)$. При этом

$$||\Delta_1(x)|| \le k! \prod_{j=2}^{m+1-k} l_j, \tag{3}$$

где l_j – вес j-го столбца в $\mathbf{H}_{base,J}$. Данное неравенство является следствием того факта, что сумма для $\Delta_1(x)$ содержит не более $k! \prod_{j=2}^{m+1-k} l_j$ слагаемых, каждое из которых является

мономом. Т.к.

$$\prod_{j=2}^{m+1-k} l_j \leq \ell^{m-k},$$

тогда

$$||\Delta_1(x)|| \leq k!\ell^{m-k}.$$

Подобные неравентсва также справедливы для всех $\Delta_j(x)$, $j \in J$. Исходя из того, что кодовое слово $\mathbf{c}(x)$ имеет $m+1$ ненулевых позиций, имеем

$$||\mathbf{c}(x)|| \leq (m+1)k!\ell^{m-k}.$$

Отдельно необходимо рассмотреть ситуацию когда $\Delta_j(x) = 0 \quad \forall j \in J$. В этом случае применение леммы 1 дает нулевое кодовое слово. Найдем ненулевой минор максимального порядка r, $r < m$ в матрице $\mathbf{H}_J(x)$. Пусть I номера строк, а S номера столбцов, такие что $\mathbf{H}_{I,S}(x)$ является данным минором. Пусть $S' = S \cup j$, $j \in J \backslash S$. Рассмотрим подматрицу $\mathbf{H}_{I,S'}(x)$. Построим кодовое слово для данной подматрицы в соответствии с леммой 1. При этом данное слово содержит хотя бы один ненулевой элемент. После добавления нулей на позиции $\{1, 2 \ldots, n\} \backslash S'$ мы получаем кодовые слова кода с проверочной матрицей $\mathbf{H}(x)$, т.к. все миноры большего порядка равны нулю. В данном случае

$$D(\mathcal{C}) \leq (r+1)k!\ell^{m-k} < (m+1)k!\ell^{m-k},$$

Замечание 2. Граница ведет себя лучше для случая регулярных кодов (см. рис. Рис. 1). В этом случае ($k = \ell$, где ℓ-вес столбца)

$$D(\mathcal{C}) \leq (m+1)\ell!\ell^{m-\ell}.$$

В случае если базовая матрица состоит из всех единиц ($\ell = m$) мы получаем границу из [20].

Замечание 3. Оценка (2) не зависит от s. Если m и n фиксированы и $s \to \infty$, тогда в соответствии с оценкой (2) $D(\mathcal{C})$ ограничена константой сверху.

Следствие 1. *Для линейного роста минимального кодового расстояния $D(\mathcal{C})$ с длиной кода $N = ns$ необходим линейный рост с N оценок* (1) *и* (2).

4. ОПИСАНИЕ АЛГОРИТМА ПОСТРОЕНИЯ ПРОВЕРОЧНЫХ МАТРИЦ КЦ МПП-КОДОВ НАД ПОЛЕМ GF(q)

В этом разделе мы опишем алгоритм построения проверочных матриц НД КЦ МПП-кодов. Алгоритм можно разделить на два шага:

1. Выбор базовой матрицы (протографа) с помощью анализа итеративного порога декодирования;
2. Расширение базовой матрицы с помощью циркулянтов и элементов поля GF(q).

Выбор базовой матрицы с помощью анализа итеративного порога декодирования может быть выполнен аналогично случаю двоичных МПП-кодов (см. детальное описание в [13], [14]). В дальнейшем остановимся только на методах расширения базовой матрицы.

Известно, псевдокодовые слова являются причиной плохой работы алгоритма распространения доверия. Псевдокодовые слова в свою очередь появляются из-за наличия коротких циклов в проверочной матрице. Таким образом, главная задача алгоритма заключается в устранении циклов при расширении базовой матрицы. На Рис. 2 приведен пример устранения цикла длины 4.

Рис. 2. Устранение цикла длины 4

Пусть I и J обозначают соответственно минимальные подмножества строк и столбцов, содержащих цикл. Легко видеть, что цикл устраняется, если выполнено следующее условие

$$\det(\mathbf{H}_{\exp_{I,J}}) \neq \mathbf{0}.$$

Таким образом, при расширении базовой матрицы алгоритм пытается разрушить как можно больше циклов. Если алгоритм не может разрушить цикл, то подсчитывается число ребер, выходящих из цикла наружу (так называемое значение ACE для цикла [15–17]). Так как в проверочной матрице много циклов (причем разной длины), то алгоритм работает с вектором ACE

$$\text{ace} = (e_4, e_6, \ldots),$$

где e_{2j} – это минимальное число ребер выходящих наружу цикла длины $2j$ (минимум берется по всем таким циклам в проверочной матрице). Если циклов длины $2j$ нет, то $e_{2j} = \infty$.

Предлагаемый в данной статье алгоритм максимизирует ACE вектор на каждом шагу. ACE векторы сравниваются лексикографически, т.е.

$$(1,2,3) < (2,2,3), (1,2,3) < (1,3,3), \ldots$$

Алгоритм построения проверочных матриц КЦ МПП-кодов над поле GF(q)

Вход: $\mathbf{H}_{\text{base}}$, q, s (размер циркулянта), t (максимальная длина цикла)
for $i \in \{1, 2, \ldots, n\}$ **do**
  for $j \in$ ones in row i **do**
    найти все циклы в матрице $\mathbf{H}_{\text{base}}$, проходящие через символ j до длины t
    for $test \in \{1, 2, \ldots, 100\}$ **do**
      $\mathbf{H}(i,j) \leftarrow (rand(s-1), rand(q-1))$
      вычислить ACE вектор
      if $\text{ace}_{\max} <$ ace **then** $\text{ace}_{\max} \leftarrow$ ace
      else вернуть предыдущее значение $\mathbf{H}(i,j)$
      end if
    end for
  end for
end for
Выход: **H**

---

5. РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

В этом разделе представлены результаты моделирования. Моделирование было проведено в канале с АБГШ и 64-QAM модуляцией. Пусть $q = 64$, $N = 4620$ и $K = 4060$. Рассмотрим результаты моделирования для лучших НД МПП-кодов над GF(64), не обладающих свойством

квазицикличности и двоичных турбо кодов. Также построим две проверочные матрицы НД КЦ МПП-кодов и проведем моделирование для соответствующих им кодов. В первом случае базовая матрица имеет размер 4×33 ($s = 140$), во втором случае 8×66 ($s = 70$). Полученные результаты представлены на графике Рис. 3

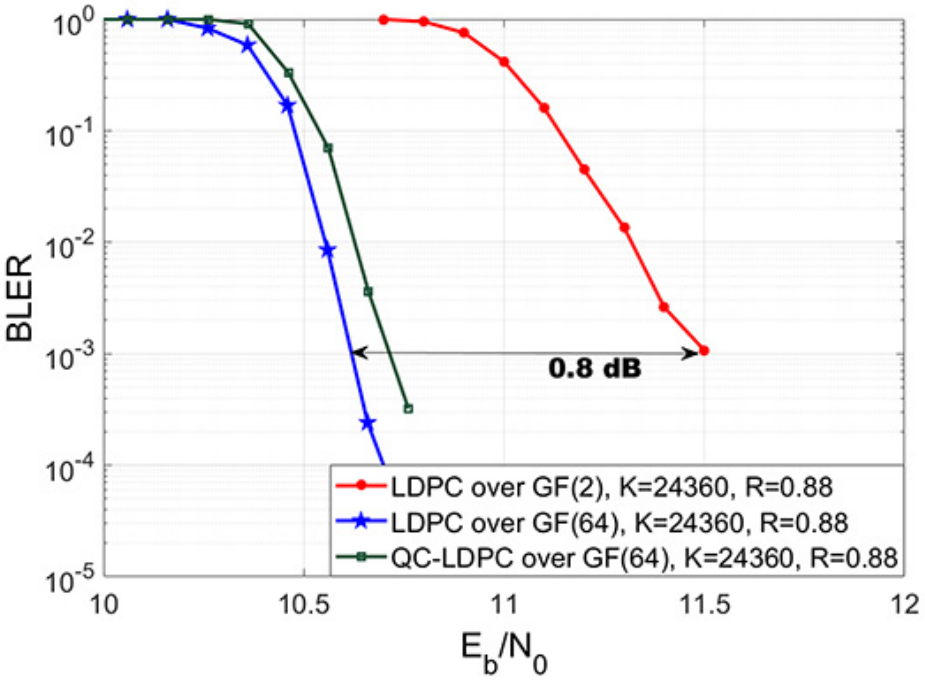

Рис. 3. Результаты моделирования. Параметры: канал с АБГШ, 64-QAM модуляцией, $q = 64$, длина кода $N = 4620$, число информационных символов $K = 4060$

Отметим что кривая для базовой матрицы размера 4×33 имеет полку вследствие небольшого кодового расстояния. В соответствии с теоремой 2 для матрицы размера 4×33 граница на минимальное расстояние принимает вид $D(\mathcal{C}) \leq 40$. В то же время для матрицы размера 8×66 границы гораздо лучше: $D(C) \leq 1152$. Корректирующая способность кода, соответсвующего последней матрице гораздо лучше. Данный ко проигрывает всего 0.1 дБ на уровне ошибки на блок $= 10^{-3}$.

6. ЗАКЛЮЧЕНИЕ

Предложен алгоритм построения проверочных матриц квазициклических кодов с малой плотностью проверок (КЦ МПП-коды) над полем GF(q). Алгоритм состоит из двух шагов. На первом шаге на основе анализа порога итеративого декодирования выбирается базовая матрица (протограф). На втором шаге алгоритм находит короткие циклы в базовой матрице и пытается их разрушить путем выбора циркулянтов и элементов поля GF(q). В первую очередь алгоритм старается разрушить циклы с наименьшим числом ребер, выходящих наружу цикла. Эффективность алгоритма продемонстрирована с помощью имитационного моделирования. С целью объяснения экспериментальных результатов нами была получена верхняя граница на кодовое расстояние НД КЦ МПП-кодов.

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. 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.

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

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

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

6. 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.

7. 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.

8. M. Davey and D. MacKay, Low-density parity check codes over GF(q), IEEE Commun. Lett., vol. 2, no. 6, pp. 165–167, Jun. 1998

9. H. Song, J. R. Cruz, Reduced-Complexity Decoding of Q-ary LDPC Codes for Magnetic Recording, IEEE Trans. on Magnetics, vol. 39, no. 2, March 2003

10. H. Wymeersch, H.Steendam, M.Moeneclaey, Log-domain decoding of LDPC codes over GF(q), IEEE Int. Conf. on Communications, 2004, pp 772–776

11. L. Barnault and D. Declercq, Fast Decoding Algorithm for LDPC over GF(2^q), The Proc. 2003 Inform. Theory Workshop, Paris, France, pp. 70–73, Mar. 2003

12. D.Declercq, M. Fossorier, Decoding Algorithms for Nonbinary LDPC Codes over GF(q), IEEE Trans. On Communications, vol.55, no.4, April 2007, pp 633–643

13. G. Liva and M. Chiani. Protograph LDPC Codes Design Based on EXIT Analysis. IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference, Washington, DC, 2007, pp. 3250–3254.

14. T. Y. Chen, K. Vakilinia, D. Divsalar and R. D. Wesel. Protograph-Based Raptor-Like LDPC Codes. *IEEE Trans. on Comm.*, vol. 63, no. 5, pp. 1522–1532, May 2015.

15. *A. Bazarsky, N. Presman and S. Litsyn*, Design of Non-Binary Quasi-Cyclic LDPC Codes by ACE Optimization // IEEE Information Theory Workshop 2013, Sevilla, Spain

16. H.Xiao, A. H. Banihashemi, Improved Progressive-Edge-Growth (PEG) Construction of Irregular LDPC Codes, IEEE Comm. Letters, vol.8, no. 12, December 2004, pp.715–717

17. X. Hu, E. Eleftheriou, D. Arnold, Irregular Progressive Edge-Growth (PEG) Tanner Graphs, ISIT 2002, Lausanne, Switzerland, June 30–July 5, 2002

18. T. Richardson and R. Urbanke. *Modern Coding Theory.* Cambridge University Press, 2008.

19. R. Smarandache, P. O. Vontobel. Quasi-Cyclic LDPC Codes: Influence of Proto- and Tanner-Graph Structure on Minimum Hamming Distance Upper Bounds. *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 585–607, Feb. 2012.

20. 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.

21. T. Richardson, R. Urbanke. *Modern Coding Theory.* Cambridge, U.K.: Cambridge Univ. Press, 2008.

A Method for Constructing Parity-Check Matrices of Quasi-Cyclic LDPC Codes over GF(q)

S.A. Kruglik, V.S. Potapova, A.A. Frolov

An algorithm for constructing parity-check matrices of quasi-cyclic LDPC (QC-LDPC) codes over GF(q) is proposed. The algorithm consists of two steps. In the first step, the base matrix (protograph) is selected based on the iterative decoding threshold analysis. In the second step, the algorithm finds short cycles in the base matrix and tries to eliminate them by selecting the circulants and the elements of GF(q). Firstly the algorithm tries to eliminate the cycles with the smallest number edges going outside the cycle. The efficiency of the algorithm is demonstrated by means of simulations.

KEYWORDS: LDPC code, parity-check matrix, iterative decoding threshold, Tanner graph, cycle, Galois field.