Информационные процессы, Том 12, № 1, 2012, стр. 68–83

ПЕРЕДАЧА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Коды с малой плотностью проверок на четность, основанные на полях Галуа

Иванов Ф. И., Зяблов В. В., Потапов В. Г.

Институт проблем передачи информации, Российская академия наук, Москва, Россия

Поступила в редколлегию 13.03.2012

Аннотация—В работе предложены способы построения отображения элементов мультипликативной группы поля Галуа на симметрическую группу матриц перестановок. Предложен метод, минимизирующий порядок симметрической группы. На основании полученных результатов построен ансамбль регулярных двоичных кодов с малой плотностью проверок на четность. Представлены результаты моделирования полученных кодовых конструкций для итеративного алгоритма декодирования "распространения доверия" (Sum-Product) при передаче кодового слова по двоичному каналу с аддитивным белым гауссовским шумом.

1. ВВЕДЕНИЕ

В работе [1] Р. Галлагер впервые описал псевдослучайную конструкцию кодов с малой плотностью проверок (МПП-коды) и предложил алгоритм генерации проверочной матрицы $\mathbf{H}$ таких кодов. Идея, лежащая в основе построения, заключается в начальном построении проверочной матрицы $\mathbf{H}_0$ относительно небольшого размера с заданными характеристиками ($\mathbf{H}_0$ может быть проверочной матрицей кода проверки на четность [2], кода Хэмминга [3], кода Рида-Соломона [4] – [5], кода БЧХ [6] и т. д.). Данная матрица дублируется (тем самым увеличивается длина кода) и применяется случайная перестановка строк и столбцов полученной матрицы $\mathbf{H}$. Часто проверочную матрицу $\mathbf{H}$ МПП-кода удобно представлять в виде графа Таннера [7], в котором для представления строк и столбцов $\mathbf{H}$ используются определенным образом связанные между собой символьные и кодовые вершины.

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

Существует ряд работ, посвященных алгоритмам поиска и удаления циклов минимальных длин в проверочных матрицах МПП-кодов, например [8] – [10].

Помимо случайных МПП-кодов используют алгебраические МПП-коды, основанные на матрицах перестановок [11] – [15] и на проективных геометриях [16] – [17]. В частности, если проверочная матрица МПП-кода $\mathbf{H}$ состоит только из циклических сдвигов единичной матрицы $\mathbf{I}$, то такой код называют *квазициклическим.* Для квазициклических кодов достаточно легко сформулировать условие отсутствия циклов минимальных длин, как это сделано в работах [18] – [21].

МПП-коды так же принято классифицировать на две группы: *регулярные* (проверочная матрица содержит ровно l единиц в каждом столбце и n_0 единиц в каждой строке) и *нере-*

гулярные (количество единиц в строке и столбце является переменным). В данной работе рассматриваются только регулярные кодовые конструкции.

Наша задача заключается в разработке и исследовании конструкций проверочных матриц МПП-кодов, основанных на мультипликативных группах полей Галуа $GF^\star(q^m)$. Показан способ построения отображения ϕ произвольного элемента мультипликативной группы поля $\beta \in GF^\star(q^m)$ на элемент симметрической группы перестановок $\mathcal{S}_n$, где $n = q^m - 1$. Так же доказано, что для отображения произвольного элемента мультипликативной группы поля $\beta \in GF^\star(q^m)$ необходимо и достаточно построить отображение только для $\alpha \in GF^\star(q^m)$, где α – примитивный элемент поля. Показано, что если $q^m - 1 = \prod_{i=1}^{k} p_i^{a_i}$, то, используя разложение перестановки на произведение независимых циклов, длину перестановки n можно сократить до $n = \sum_{i=1}^{k} p_i^{a_i}$.

Статья организована следующим образом: в §2.1 приведены основные определения и обозначения, используемые в статье. В §2.2 приведен алгоритм построения отображения произвольного элемента мультипликативной группы поля $\beta \in GF^\star(q^m)$ на элемент симметрической группы перестановок $\mathcal{S}_n$, где $n = q^m - 1$. В §2.3 приведена общая конструкция проверочной матрицы $\mathbf{H}$ квазициклических МПП-кодов, сформулировано условие отсутствия в ней циклов длины 4. В §2.4 приведен основной результат, в котором утверждается существование гомоморфизма ϕ между $GF^\star(q^m)$ и симметрической группой $\mathcal{S}_d$, где $d = \sum_{i=1}^{k} p_i^{a_i}$. Приведен алгоритм построения ϕ, а так же пример использования алгоритма для мультипликативной группы поля $GF(2^4)$. В §2.5 приведена конструкция проверочной матрицы МПП-кода, основанного на мультипликативных группах полей Галуа, показана связь полученной кодовой конструкции с квазициклическими кодами, сформулировано условие отсутствия циклов длины 4 для построенных кодовых конструкций. В §3 приведены результаты компьютерного моделирования описанных в статье конструкций кодов.

2. МПП-КОДЫ, ОСНОВАННЫЕ НА ПОЛЯХ ГАЛУА

2.1. Основные определения и обозначения

Ниже мы приведем основные определения и обозначения, а так же известные результаты, которые понадобятся нам в дальнейшем.

Определение. Пусть $\mathbf{P}$ – квадратная $m \times m$ матрица, тогда число m назовем *размерностью* $\mathbf{P}$ и будем обозначать $dim\,\mathbf{P} = m$.

Определение. Пусть $\mathbf{P} = ||p_{ij}||$, $\mathbf{Q} = ||q_{ij}||$ – матрицы одинаковой размерности, тогда *произведением Адамара* матриц $\mathbf{P}$ и $\mathbf{Q}$ назовем матрицу $\mathbf{C} = \mathbf{P} \diamond \mathbf{Q} = ||p_{ij}q_{ij}||$

Определение. *Порядком* перестановки σ назовем наименьшее $n \in \mathbb{N}$, такое что $\sigma^n = \epsilon$, где ϵ – единичная перестановка. Будем записывать $n = ord\,\sigma$. Аналогично, если $\mathbf{P}_\pi$ –матрица перестановки, то под ее порядком будем понимать такое наименьшее $n \in \mathbb{N}$, что $\mathbf{P}_\pi^n = \mathbf{I}$, где $\mathbf{I}$ – единичная матрица. Будем записывать $ord\,\mathbf{P}_\pi = n$.

Теоремой, позволяющей связать произвольную конечную группу $\mathcal{G}$ с симметрической группой перестановок $\mathcal{S}_m$ (а значит и с группой матриц перестановок $\mathcal{P}_m$), является теорема Кэли.

Теорема. *(Кэли) Любая конечная группа $(\mathcal{G}, \circ)$ изоморфна некоторой группе перестановок множества элементов этой группы. При этом каждый элемент $g \in \mathcal{G}$ сопоставляется с*

перестановкой π_g, задаваемой тождеством $\pi_g(h) = g \circ h$, где h – произвольный элемент группы $\mathcal{G}$.

Доказательство. См. [22].

Данная теорема говорит не только о существовании гомоморфизма $\phi : \mathcal{G} \mapsto \mathcal{S}_m$, но и дает представление о его строении.

Теорема. *Для любой перестановки $\phi \in \mathcal{S}_m$ существует единственное (с точностью до порядка следования множителей) представление в виде*

$$\phi = \pi_1 \pi_2 \dots \pi_k,$$

где перестановки π_j являются попарно независимыми циклами (циклическими перестановками).

Доказательство. См. [22].

Следствие. *Если $\phi = \pi_1 \pi_2 \dots \pi_k$, то $n = \sum_{j=1}^{k} s_j$, где n – длина перестановки ϕ, s_j – длина j цикла π_j.*

Теперь приведем необходимые сведения из теории групп.

Определение. Пусть $\mathcal{G}$ –конечная группа, под $|\mathcal{G}| = p$ будем понимать порядок $\mathcal{G}$, т. е. число ее элементов.

Определение. Пусть $GF^\star(q^m)$ – мультипликативная группа поля $GF(q^m)$, тогда под $< \beta >$ будем понимать ее циклическую подгруппу, порожденную элементом $\beta \in GF^\star(q^m)$.

Так как $|GF^\star(q^m)| = q^m - 1$, то если $| < \beta > | = p$, то по теореме Лагранжа $\dfrac{q^m - 1}{p} = s \in \mathbb{Z}$, причем $\beta = \alpha^s$, где α – примитивный элемент поля $GF(q^m)$. В заключение главы приведем формулировку китайской теоремы об остатках, которая потребуется нам для доказательства основого результата работы.

Теорема. *(Китайская теорема об остатках) Любое неотрицательное целое число n которое не превышает каждого из множителей модуля $M = m_1 m_2 \dots m_k$ можно однозначно восстановить если известны его остатки r_i по этим модулям.*

Доказательство. См. [22].

2.2. Построение гомоморфизма групп $GF^\star(q^m)$ и $\mathcal{S}_{q^m-1}$

Рассмотрим мультипликативную группу $GF^\star(q^m) = \{\alpha, \alpha^2, \dots, \alpha^{q^m-2}, \alpha^{q^m-1} = 1\}$ поля Галуа $GF(q^m)$, где α – примитивный элемент поля. По теореме Кэли, существует гомоморфизм ϕ, ставящий в соответствие каждому элементу $\beta \in GF^\star(q^m)$ перестановку $\pi_\beta \in \mathcal{S}_n$. Вначале рассмотрим случай, когда $n = q^m - 1$. Поскольку $|\mathcal{S}_n| = (q^m - 1)!$ и $|GF^\star(q^m)| = q^m - 1$, то $\dfrac{|\mathcal{S}_n|}{|GF^\star(q^m)|} = (q^m - 2)! \in \mathbb{Z}$, то такой гомоморфизм ϕ существует.

Прежде чем приступать к построению отображения, докажем теорему, которая утверждает, что для построения гомоморфизма групп необходимо и достаточно знать, куда перейдет примитивный элемент поля.

Теорема. *Пусть $\alpha \in GF^\star(q^m)$ – примитивный элемент поля $GF(q^m)$. Тогда для построения $\phi: GF^\star(q^m) \mapsto \mathcal{S}_n$ необходимо и достаточно вычислить $\phi(\alpha) = \pi_\alpha$.*

Доказательство. *(Необходимость)* Пусть известно, что $\phi(\alpha) = \pi_\alpha$, где α – примитивный элемент поля. Пусть β – произвольный элемент мультипликативной группы поля, тогда $\exists s \in \mathbb{N}$, такой, что $\beta = \alpha^s$, таким образом $\phi(\beta) = \phi(\alpha^s)$, так как ϕ – гомоморфизм, то $\phi(\beta) = (\phi(\alpha))^s$, поэтому $\phi(\beta) = \pi_\alpha^s$.

(Достаточность) Пусть известно отображение $\phi: GF^\star(q^m) \mapsto \mathcal{S}_n$. Это равносильно тому, что $\forall \beta \in GF^\star(q^m)$ известна такая перестановка π_β: $\phi(\beta) = \pi_\beta$, в частности известна и перестановка π_α, такая, что $\phi(\alpha) = \pi_\alpha$.

Определение. Если α –примитивный элемент поля, то перестановку π_α назовем *примитивной перестановкой.*

Таким образом, перестановка, в которую переходит произвольный элемент мультипликативной группы $GF^\star(q^m)$, является степенью примитивной перестановки.

Теперь приступим к непосредственному построению гомоморфизма.

Известно, что мультипликативную группу поля Галуа можно представить следующими способами:

1. В виде степеней примитивного элемента α
2. В виде векторов длины m над полем $GF(q)$
3. В виде натуральных чисел, соответствующих десятичному представлению вектора

Очевидно, что между всеми этими представлениями существует взаимно-однозначное соответствие.

Напомним, что согласно теореме Кэли, каждый $g \in \mathcal{G}$ сопоставляется с перестановкой π_g, задаваемой тождеством $\pi_g(h) = g \circ h$, где h – произвольный элемент группы $\mathcal{G}$. Если $\mathcal{G} = GF^\star(q^m)$, $\beta, \gamma \in GF^\star(q^m)$, то $\pi_\beta(\gamma) = \beta \cdot \gamma = \gamma \cdot \beta = \pi_\gamma(\beta)$, где $(\cdot)$ – групповая операция умножения.

Таким образом, перестановку π_β, отвечающую $\beta \in GF^\star(q^m)$, можно задать таблицей умножения β на все элементы группы (включая самого себя).

Проиллюстрируем сказанное выше следующим примером:

Пример. Рассмотрим $GF^\star(2^2) = \{x, x+1, 1\} = \{\alpha, \alpha^2, \alpha^3 = 1\}$, где $\alpha = x$ – примитивный элемент. Согласно доказанной выше теореме, нам достаточно построить перестановку π_α, тогда $\pi_{\alpha^2} = \pi_\alpha^2$, $\pi_{\alpha^3} = \pi_\alpha^3 = \epsilon$, где ϵ – единичная перестановка.

Отобразим каждый из элементов группы вначале на вектор длины 2 над полем $GF(2)$, а затем каждый из полученных векторов на его десятичное представление:

1. $\alpha \mapsto (1,0) \mapsto 2$
2. $\alpha^2 \mapsto (1,1) \mapsto 3$
3. $\alpha^3 \mapsto (0,1) \mapsto 1$

Составим таблицу:

$$\begin{pmatrix} \alpha^3 & \alpha & \alpha^2 \\ \alpha & \alpha^2 & \alpha^3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \pi_\alpha$$

Легко видеть, что полученная перестановка π_α является циклической. Отобразим π_α на соответствующую ей матрицу перестановки $\mathbf{P}_\alpha$:

$$\pi_\alpha \mapsto \mathbf{P}_\alpha = \begin{pmatrix} 0\,1\,0 \\ 0\,0\,1 \\ 1\,0\,0 \end{pmatrix}$$

Матрица $\mathbf{P}_\alpha$ является матрицей циклического сдвига единичной матрицы: $\mathbf{P}_\alpha = \mathbf{I}_1$. Легко проверить, что $\mathbf{P}_{\alpha^2} = \mathbf{P}_\alpha^2 = \mathbf{I}_2$, $\mathbf{P}_{\alpha^3} = \mathbf{P}_\alpha^3 = \mathbf{I}_3 = \mathbf{I}$.

Таким образом, отображение $\phi : GF^\star(2^2) \mapsto \mathcal{S}_3$ полностью задано.

Следует отметить, что описанный выше алгоритм не всегда приводит к построению циклических перестановок даже в том случае, когда $\alpha = x$ является примитивным элементом. Следующий пример иллюстрирует это:

Пример. Пусть $GF^\star(2^4) = \{\alpha, \alpha^2, \ldots, \alpha^{15} = 1\}$, где $\alpha = x$ – примитивный элемент. Соответствующее группе поле построено по модулю примитивного многочлена $p(x) = x^4 + x + 1$. Отобразим каждый из элементов группы вначале на вектор длины 4 над полем $GF(2)$, а затем каждый из полученных векторов на его десятичное представление:

1. $\alpha \mapsto (0,0,1,0) \mapsto 2$
2. $\alpha^2 \mapsto (0,1,0,0) \mapsto 4$
3. $\alpha^3 \mapsto (1,0,0,0) \mapsto 8$
4. $\alpha^4 \mapsto (0,0,1,1) \mapsto 3$
5. $\alpha^5 \mapsto (0,1,1,0) \mapsto 6$
6. $\alpha^6 \mapsto (1,1,0,0) \mapsto 12$
7. $\alpha^7 \mapsto (1,0,1,1) \mapsto 11$
8. $\alpha^8 \mapsto (0,1,0,1) \mapsto 5$
9. $\alpha^9 \mapsto (1,0,1,0) \mapsto 10$
10. $\alpha^{10} \mapsto (0,1,1,1) \mapsto 7$
11. $\alpha^{11} \mapsto (1,1,1,0) \mapsto 14$
12. $\alpha^{12} \mapsto (1,1,1,1) \mapsto 15$
13. $\alpha^{13} \mapsto (1,1,0,1) \mapsto 13$
14. $\alpha^{14} \mapsto (1,0,0,1) \mapsto 9$
15. $\alpha^{15} \mapsto (0,0,0,1) \mapsto 1$

Построим таблицу умножения для примитивного элемента:

1. $\alpha \cdot \alpha^{15} = \alpha \Longrightarrow 1 \mapsto 2$
2. $\alpha \cdot \alpha = \alpha^2 \Longrightarrow 2 \mapsto 4$
3. $\alpha \cdot \alpha^4 = \alpha^5 \Longrightarrow 3 \mapsto 6$
4. $\alpha \cdot \alpha^2 = \alpha^3 \Longrightarrow 4 \mapsto 8$
5. $\alpha \cdot \alpha^8 = \alpha^9 \Longrightarrow 5 \mapsto 10$
6. $\alpha \cdot \alpha^5 = \alpha^6 \Longrightarrow 6 \mapsto 12$
7. $\alpha \cdot \alpha^{10} = \alpha^{11} \Longrightarrow 7 \mapsto 14$
8. $\alpha \cdot \alpha^3 = \alpha^4 \Longrightarrow 8 \mapsto 3$
9. $\alpha \cdot \alpha^{14} = \alpha^{15} \Longrightarrow 9 \mapsto 1$
10. $\alpha \cdot \alpha^9 = \alpha^{10} \Longrightarrow 10 \mapsto 7$
11. $\alpha \cdot \alpha^7 = \alpha^8 \Longrightarrow 11 \mapsto 5$
12. $\alpha \cdot \alpha^6 = \alpha^7 \Longrightarrow 12 \mapsto 11$
13. $\alpha \cdot \alpha^{13} = \alpha^{14} \Longrightarrow 13 \mapsto 9$

14. $\alpha \cdot \alpha^{11} = \alpha^{12} \Longrightarrow 14 \mapsto 15$
15. $\alpha \cdot \alpha^{12} = \alpha^{13} \Longrightarrow 15 \mapsto 13$

Полученная примитивная перестановка не является циклической.

Очевидно, что для того, примитивная перестановка была циклической, достаточно вместо таблицы умножения относительно десятичных представлений элементов группы, рассматривать таблицы умножения относительно степеней примитивного элемента. В таком случае

$$\pi_\alpha = \begin{pmatrix} 1\,2\,3 \ldots q^m-2 & q^m-1 \\ 2\,3\,4 \ldots q^m-1 & 1 \end{pmatrix},$$

следовательно

$$\mathbf{P}_\alpha = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ddots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 0 \end{pmatrix}. \tag{1}$$

Полученная матрица (циклический сдвиг вправо на единицу столбцов единичной матрицы) является частным видом циркулянта.

Определение. Матрицу $\mathbf{P}_\alpha$, а так же все ее степени $\mathbf{P}_\alpha^t$, будем называть *циклическими матрицами перестановки.*

2.3. Квазициклические МПП-коды

Определение. Пусть $\alpha_{ij} = \alpha^{r_{ij}} \in GF^\star(q^m)$, где α – примитивный элемент поля. Отобразим каждый α_{ij} на циклическую матрицу перестановки $\mathbf{P}_{\alpha_{ij}}$. Выберем $l, n_0 \in \mathbb{N}$, $n_0 > l$. Тогда проверочная матрица

$$\mathbf{H} = \begin{pmatrix} \mathbf{P}_{\alpha_{11}} & \mathbf{P}_{\alpha_{12}} & \ldots & \mathbf{P}_{\alpha_{1n_0}} \\ \mathbf{P}_{\alpha_{21}} & \mathbf{P}_{\alpha_{22}} & \ldots & \mathbf{P}_{\alpha_{2n_0}} \\ \ldots & \ldots & \ldots & \ldots \\ \mathbf{P}_{\alpha_{l1}} & \mathbf{P}_{\alpha_{l2}} & \ldots & \mathbf{P}_{\alpha_{ln_0}} \end{pmatrix} \tag{2}$$

определяет ансамбль регулярных двоичных МПП-кодов длины $n = (q^m - 1)n_0$, который мы обозначим $\mathcal{E}_{QC}(l, n_0, q^m - 1)$. Элементы ансамбля $\mathcal{E}_{QC}(l, n_0, q^m - 1)$ получаются путем равновероятного выбора (с возвращением) элементов мультипликативной группы $GF^\star(q^m)$. Произвольный код $\mathcal{C} \in \mathcal{E}_{QC}(l, n_0, q^m - 1)$ будем называть *квазициклическим МПП-кодом.*

Данный класс кодов достаточно хорошо исследован, в частности в работах [23] – [28]. К его преимуществам перед случайными кодами следует отнести тот факт, что необходимо хранить не ln_0 произвольных матриц перестановок, а ln_0 чисел, являющихся степенями матрицы (1).

Если переписать матрицу (2) в виде

$$\mathbf{H} = \begin{pmatrix} \mathbf{P}^{r_{11}} & \mathbf{P}^{r_{12}} & \ldots & \mathbf{P}^{r_{1n_0}} \\ \mathbf{P}^{r_{21}} & \mathbf{P}^{r_{22}} & \ldots & \mathbf{P}^{r_{2n_0}} \\ \ldots & \ldots & \ldots & \ldots \\ \mathbf{P}^{r_{l1}} & \mathbf{P}^{r_{l2}} & \ldots & \mathbf{P}^{r_{ln_0}} \end{pmatrix}, \tag{3}$$

где $\mathbf{P}^{r_{ij}} = \mathbf{P}_\alpha^{r_{ij}}$, $i = 1..l$, $j = 1..n_0$, $0 \le r_{ij} \le q^m - 1$, то условие отстутствия в матрице $\mathbf{H}$ циклов длины 4 можно сформулировать в следующем виде:

Теорема. *Матрица* $\mathbf{H}$ *не содержит циклов длины* 4 *тогда и только тогда, когда для любой ее подматрицы*

$$\begin{pmatrix} \mathbf{P}^{r_{i_1 j_1}} & \mathbf{P}^{r_{i_1 j_2}} \\ \mathbf{P}^{r_{i_2 j_1}} & \mathbf{P}^{r_{i_2 j_2}} \end{pmatrix},$$

$1 \le i_1 < i_2 \le l$, $1 \le j_1 < j_2 \le n_0$, *справедливо соотношение*

$$r_{i_2 j_1} - r_{i_1 j_1} \ne r_{i_2 j_2} - r_{i_1 j_2}.$$

Доказательство. См. следствие 1 к лемме 3 и теорему 1 в [29].

2.4. Представление элементов группы $GF^\star(q^m)$ в виде произведения независимых циклических перестановок

Рассмотрим мультипликативную группу $GF^\star(q^m)$. Пусть $q^m - 1 = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Тогда существуют циклические подгруппы $< \beta_1 >, < \beta_2 >, \dots, < \beta_k >$, причем $| < \beta_i > | = p_i^{a_i}$, $i = 1..k$, $\beta_i = \alpha^{\frac{q^m-1}{p_i^{a_i}}}$, где α – примитивный элемент. Каждая из $< \beta_i >$ замкнута относительно операции умножения.

Так как наибольший общий делитель $(p_i^{a_i}, p_j^{a_j}) = 1$, $\forall i, j : \ 1 \le i, j \le k$, то, применив китайскую теорему об остатках, получим, что $\forall \gamma \in GF^\star(q^m)$ справедливо единственное представление:

$$\gamma = \beta_1^{r_1} \beta_2^{r_2} \dots \beta_k^{r_k}, \tag{4}$$

где $0 \le r_i < p_i^{a_i}$.

Так как $\gamma = \alpha^s$, $\beta_i = \alpha^{\frac{q^m-1}{p_i^{a_i}}}$, то представление (4) можно записать в следующем виде:

$$\alpha^s = \alpha^{r_1 \frac{q^m-1}{p_1^{a_1}}} \alpha^{r_2 \frac{q^m-1}{p_2^{a_2}}} \dots \alpha^{r_k \frac{q^m-1}{p_k^{a_k}}}$$

или

$$s = \sum_{i=1}^{k} r_i \frac{q^m - 1}{p_i^{a_i}} \, mod \, (q^m - 1). \tag{5}$$

Таким образом, задача представления γ в виде (4) эквивалента решению уравнения (5) относительно переменных $r_1, r_2, \dots, r_k$. Данное уравнение, согласно китайской теореме об остатках, имеет единственное решение.

Ранее было доказано, что для построения отображения $\phi : GF^\star(q^m) \mapsto \mathcal{S}_p$ необходимо и достаточно построить отображение примитивного элемента $\phi(\alpha)$, таким образом, уравнение (5) достаточно решить для случая, когда $s = 1$.

Каждый образующий элемент β_i циклической подгруппы $< \beta_i >$ можно отобразить на циклическую перестановку π_{β_i}, причем $|\pi_{\beta_i}| = p_i^{a_i}$. Таким образом, $\pi_{\beta_i^{r_i}} = \pi_{\beta_i}^{r_i}$. Так как $< \beta_i > \cap < \beta_j >= \{1\}$ при $i \ne j$, то полученные циклы можно считать независимыми. Таким образом справедлива теорема:

Теорема. *Если* $GF^\star(q^m)$*:* $q^m - 1 = \prod_{i=1}^{k} p_i^{a_i}$*, то существует гомоморфизм* $\phi : GF^\star(q^m) \mapsto \mathcal{S}_h$*,* $h = \sum_{i=1}^{k} p_i^{a_i}$*, причем* $\forall \gamma \in GF^\star(q^m)$ *справедливо равенство:*

$$\phi(\gamma) = \pi_{\beta_1}^{r_1} \pi_{\beta_2}^{r_2} \dots \pi_{\beta_k}^{r_k}, \tag{6}$$

где $\beta_i \in GF^\star(q^m)$ *является образующей циклической подгруппы* $< \beta_i >$: $| < \beta_i > | = p_i^{a_i}$, $i = 1..k$, $r_i < p_i^{a_i}$ *являются решениями уравнения (5). Разложение (6) является произведением независимых циклов* $\pi_{\beta_i}^{r_i}$.

Очевидно, что матрица $\mathbf{P}_\gamma$, соответствующая перестановке $\phi(\gamma)$ будет циклической тогда и только тогда, когда $q^m - 1$ – простое. Иначе $\mathbf{P}_\gamma$ будет иметь следующий вид:

$$\mathbf{P}_\gamma = \begin{pmatrix} \mathbf{I}_{r_1} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k} \end{pmatrix}, \tag{7}$$

где $\mathbf{I}_{r_i}$ – матрица r_i-кратного циклического сдвига, $dim\, \mathbf{I}_{r_i} = p_i^{a_i}$. Следующий пример иллюстрирует алгоритм построения подобной матрицы.

Пример. Рассмотрим мультипликативную группу $GF^\star(2^4)$. Так как $2^4 - 1 = 3 \cdot 5$, то существуют подгруппы $< \beta_1 >=< \alpha^5 >$ и $< \beta_2 >=< \alpha^3 >$, причем $| < \beta_1 > | = 3$, $| < \beta_2 > | = 5$. Таким образом, существует гомоморфизм $\phi : GF^\star(2^4) \mapsto \mathcal{S}_8$.

Вычислим $\phi(\alpha)$, где α – примитивный элемент. По доказанной выше теореме $\alpha = \beta_1^{r_1}\beta_2^{r_2}$.

Прежде всего найдем, куда переходят β_1 и β_2. Так как $< \beta_1 >$ и $< \beta_2 >$ являются группами, то существуют отображения ϕ_1 и ϕ_2, отображающие эти группы на симметрические группы $\mathcal{S}_3$ и $\mathcal{S}_5$ соответственно. Следуя алгоритму, приведенному в §2.2,

$$\phi_1(\beta_1) = \pi_{\beta_1} = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}.$$

Аналогично построим

$$\phi_2(\beta_2) = \pi_{\beta_2} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,5\,1 \end{pmatrix}.$$

Для того, чтобы π_{β_1} и π_{β_2} являлись независимыми циклами, а их произведение принадлежало группе $\mathcal{S}_8$, достаточно в перестановке π_{β_2} сделать следующее переобозначение переставляемых элементов:

$$\pi_{\beta_2} = \begin{pmatrix} 4\,5\,6\,7\,8 \\ 5\,6\,7\,8\,4 \end{pmatrix}.$$

Таким образом, произведение

$$\pi_{\beta_1}^{r_1}\pi_{\beta_2}^{r_2} = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}^{r_1} \begin{pmatrix} 4\,5\,6\,7\,8 \\ 5\,6\,7\,8\,4 \end{pmatrix}^{r_2}. \tag{8}$$

есть произведение независимых циклов (в каждой перестановке указаны только переставляемые элементы) при любых натуральных r_1 и r_2.

Для того, чтобы найти перестановку $\pi_\alpha \in \mathcal{S}_8$, соответсвующую примитивному элементу α, требуется найти r_1 и r_2 в разложении (8). Для этого достаточно решить сравнение:

$$5r_1 + 3r_2 = 1\, mod\, 15.$$

Очевидно, что такими решениями являются числа $r_1 = r_2 = 2$, таким образом

$$\pi_\alpha = \pi_{\beta_1}^2\pi_{\beta_2}^2 = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}^2 \begin{pmatrix} 4\,5\,6\,7\,8 \\ 5\,6\,7\,8\,4 \end{pmatrix}^2. \tag{9}$$

Представив разложение (9) в матричной форме, получим

$$\mathbf{P}_\alpha = \begin{pmatrix} 0\,0\,1\,0\,0\,0\,0\,0 \\ 1\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1 \\ 0\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0 \end{pmatrix}.$$

Таким образом,

$$\mathbf{I}_{r_1} = \begin{pmatrix} 0\,0\,1 \\ 1\,0\,0 \\ 0\,1\,0 \end{pmatrix}$$

и

$$\mathbf{I}_{r_2} = \begin{pmatrix} 0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1 \\ 1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0 \end{pmatrix}.$$

Нетрудно убедиться, что $ord\,\mathbf{P}_\alpha = 15$.

2.5. МПП-коды, основанные на полях Галуа

Определение. Пусть $\alpha_{ij} = \alpha^{s_{ij}} \in GF^\star(q^m)$, где α – примитивный элемент поля. Представим $q^m - 1$ в каноническом виде: $q^m - 1 = \prod\limits_{i=1}^{k} p_i^{a_i}$. Отобразим каждый элемент α_{ij} на матрицу перестановки $\mathbf{P}_{\alpha_{ij}}$, $dim\,\mathbf{P}_{\alpha_{ij}} = \sum\limits_{i=1}^{k} p_i^{a_i}$. Выберем $l, n_0 \in \mathbb{N}$, $n_0 > l$. Тогда проверочная матрица

$$\mathbf{H} = \begin{pmatrix} \mathbf{P}_{\alpha_{11}} & \mathbf{P}_{\alpha_{12}} & \dots & \mathbf{P}_{\alpha_{1n_0}} \\ \mathbf{P}_{\alpha_{21}} & \mathbf{P}_{\alpha_{22}} & \dots & \mathbf{P}_{\alpha_{2n_0}} \\ \dots & \dots & \dots & \dots \\ \mathbf{P}_{\alpha_{l1}} & \mathbf{P}_{\alpha_{l2}} & \dots & \mathbf{P}_{\alpha_{ln_0}} \end{pmatrix} \tag{10}$$

определяет ансамбль регулярных двоичных МПП-кодов длины $n = \Big(\sum\limits_{i=1}^{k} p_i^{a_i}\Big) n_0$, который мы обозначим $\mathcal{E}_{GF}(l, n_0, q^m - 1)$. Элементы ансамбля $\mathcal{E}_{GF}(l, n_0, q^m - 1)$ получаются путем равновероятного выбора (с возвращением) элементов мультипликативной группы $GF^\star(q^m)$. Произвольный код $\mathcal{C} \in \mathcal{E}_{GF}(l, n_0, q^m - 1)$ будем называть *МПП-кодом, основанным на поле Галуа* или *GF-кодом*.

Так как каждую матрицу $\mathbf{P}_{\alpha_{ij}}$ можно представить в виде

$$\mathbf{P}_{\alpha_{ij}} = \mathbf{P}_\alpha^{s_{ij}} = \begin{pmatrix} \mathbf{I}_{r_1} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k} \end{pmatrix}^{s_{ij}} = \begin{pmatrix} \mathbf{I}_{r_1}^{s_{ij}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{ij}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{ij}} \end{pmatrix},$$

то проверочную матрицу (10) можно представить в виде

$$\mathbf{H} = \begin{pmatrix} \begin{pmatrix} \mathbf{I}_{r_1}^{s_{11}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{11}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{11}} \end{pmatrix} & \begin{pmatrix} \mathbf{I}_{r_1}^{s_{12}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{12}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{12}} \end{pmatrix} \dots \begin{pmatrix} \mathbf{I}_{r_1}^{s_{1n_0}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{1n_0}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{1n_0}} \end{pmatrix} \\ \vdots \qquad\qquad & \vdots \qquad\qquad & \vdots \qquad\qquad & \vdots \qquad\qquad \\ \begin{pmatrix} \mathbf{I}_{r_1}^{s_{l1}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{l1}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{l1}} \end{pmatrix} & \begin{pmatrix} \mathbf{I}_{r_1}^{s_{l2}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{l2}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{l2}} \end{pmatrix} \dots \begin{pmatrix} \mathbf{I}_{r_1}^{s_{ln_0}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{ln_0}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{ln_0}} \end{pmatrix} \end{pmatrix}. \qquad (11)$$

Таким образом, проверочная матрица GF-кода $\mathcal{C} \in \mathcal{E}_{GF}(l, n_0, q^m - 1)$ представляет собой k проверочных матриц $\mathbf{H}_i$, $i = 1..k$ квазициклических кодов длин $n_i = p_i^{a_i} n_0$, соединенных специальным образом:

$$\mathbf{H}_i = \begin{pmatrix} \mathbf{I}_{r_i}^{s_{11}} & \mathbf{I}_{r_i}^{s_{12}} & \dots & \mathbf{I}_{r_i}^{s_{1n_0}} \\ \dots & \dots & \dots & \dots \\ \mathbf{I}_{r_i}^{s_{l1}} & \mathbf{I}_{r_i}^{s_{l2}} & \dots & \mathbf{I}_{r_i}^{s_{ln_0}} \end{pmatrix}$$

В то же время, как было отмечено ранее, код $\mathcal{C} \in \mathcal{E}_{GF}(l, n_0, q^m - 1)$ является квазициклическим тогда и только тогда, когда $q^m - 1$ – простое.

Тем не менее для GF-кодов, как и для квазициклических кодов, можно сформулировать утверждение об отсутствии циклов длины 4.

В [29] доказано, что блочная матрица $\begin{pmatrix} \mathbf{R} & \mathbf{S} \\ \mathbf{P} & \mathbf{Q} \end{pmatrix}$, составленная из матриц перестановок, не имеет циклов длины 4 тогда и только тогда, когда $(\mathbf{P}\mathbf{R}^T) \diamond (\mathbf{Q}\mathbf{S}^T) = \mathbf{0}$, где $\diamond$ –произведение Адамара.

Теорема 1 в [29] утверждает, что матрица $\mathbf{H}$, составленная из матриц перестановок

$$\mathbf{H} = \begin{pmatrix} \mathbf{P}_{11} & \mathbf{P}_{12} & \dots & \mathbf{P}_{1n_0} \\ \dots & \dots & \dots & \dots \\ \mathbf{P}_{l1} & \mathbf{P}_{12} & \dots & \mathbf{P}_{ln_0} \end{pmatrix},$$

не имеет циклов длины 4 тогда и только тогда, когда любая ее подматрица вида

$$\mathbf{H}_1 = \begin{pmatrix} \mathbf{P}_{i_1 j_1} & \mathbf{P}_{i_1 j_2} \\ \mathbf{P}_{i_2 j_1} & \mathbf{P}_{i_2 j_2} \end{pmatrix} \qquad (12)$$

$(0 < i_1 < i_2 \le l,\ 0 < j_1 < j_2 \le n_0)$ не имеет циклов длины 4.

Выберем в матрице (11) подматрицу вида (12):

$$\mathbf{H}_1 = \begin{pmatrix} \begin{pmatrix} \mathbf{I}_{r_1}^{s_{i_1 j_1}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{i_1 j_1}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{i_1 j_1}} \end{pmatrix} & \begin{pmatrix} \mathbf{I}_{r_1}^{s_{i_1 j_2}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{i_1 j_2}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{i_1 j_2}} \end{pmatrix} \\ \begin{pmatrix} \mathbf{I}_{r_1}^{s_{i_2 j_1}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{i_2 j_1}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{i_2 j_1}} \end{pmatrix} & \begin{pmatrix} \mathbf{I}_{r_1}^{s_{i_2 j_2}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{i_2 j_2}} & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{i_2 j_2}} \end{pmatrix} \end{pmatrix}$$

Пусть

$$\mathbf{R} = \begin{pmatrix} \mathbf{I}_{r_1}^{s_{i_1j_1}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{i_1j_1}} & \dots & \mathbf{0} \\ & & \ddots & \\ \dots & \dots & & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{i_1j_1}} \end{pmatrix},$$

$$\mathbf{P} = \begin{pmatrix} \mathbf{I}_{r_1}^{s_{i_2j_1}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{i_2j_1}} & \dots & \mathbf{0} \\ & & \ddots & \\ \dots & \dots & & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{i_2j_1}} \end{pmatrix},$$

$$\mathbf{S} = \begin{pmatrix} \mathbf{I}_{r_1}^{s_{i_1j_2}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{i_1j_2}} & \dots & \mathbf{0} \\ & & \ddots & \\ \dots & \dots & & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{i_1j_2}} \end{pmatrix},$$

$$\mathbf{Q} = \begin{pmatrix} \mathbf{I}_{r_1}^{s_{i_2j_2}} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{r_2}^{s_{i_2j_2}} & \dots & \mathbf{0} \\ & & \ddots & \\ \dots & \dots & & \dots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{I}_{r_k}^{s_{i_2j_2}} \end{pmatrix},$$

тогда, учитывая, что $\mathbf{I}_{r_i}^{s_{ij}} = \mathbf{I}_{r_i s_{ij}}$, $\mathbf{I}_{r_i}\mathbf{I}_{r_j} = \mathbf{I}_{r_i+r_j}$, $\mathbf{I}_{r_i}^T = \mathbf{I}_{r_i}^{-1} = \mathbf{I}_{p_i^{a_i}-r_i}$, получим, что условие $(\mathbf{P}\mathbf{R}^T) \diamond (\mathbf{Q}\mathbf{S}^T) = \mathbf{0}$ равносильно

$$\begin{pmatrix} \mathbf{I}_{p_1^{a_1}-r_1(s_{i_1j_1}-s_{i_2j_1})} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{p_2^{a_2}-r_2(s_{i_1j_1}-s_{i_2j_1})} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_{p_3^{a_3}-r_3(s_{i_1j_1}-s_{i_2j_1})} & \dots & \mathbf{0} \\ & & & \ddots & \\ \dots & \dots & \dots & & \dots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{I}_{p_k^{a_k}-r_k(s_{i_1j_1}-s_{i_2j_1})} \end{pmatrix} \diamond$$
$$\diamond \begin{pmatrix} \mathbf{I}_{p_1^{a_1}-r_1(s_{i_1j_2}-s_{i_2j_2})} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{p_2^{a_2}-r_2(s_{i_1j_2}-s_{i_2j_2})} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_{p_3^{a_3}-r_3(s_{i_1j_2}-s_{i_2j_2})} & \dots & \mathbf{0} \\ & & & \ddots & \\ \dots & \dots & \dots & & \dots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{I}_{p_k^{a_k}-r_k(s_{i_1j_2}-s_{i_2j_2})} \end{pmatrix} \neq \mathbf{0}. \tag{13}$$

Путем несложных преобразований и учитывая, что $\mathbf{P}_i \diamond \mathbf{P}_j = \mathbf{0} \iff i \neq j$ ($\mathbf{P}_i$, $\mathbf{P}_j$ – циклические матрицы перестановки), можно показать, что соотношение (13) выполняется тогда и только тогда, когда $s_{i_2j_2} - s_{i_1j_2} \neq s_{i_2j_1} - s_{i_1j_1}$. Последнее условие эквивалентно условию отсутствия циклов длины 4 у квазициклических МПП-кодов (см. §2.3).

3. РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

Для генерации проверочных матриц МПП -кодов были написаны функции для MatLab. Моделирование производилось методами иммитационного моделирования с использованием среды MatLab. В качестве канала передачи информации был выбран двоичный канал с аддитивным белым гауссовским шумом (АБГШ). В качестве алгоритма декодирования был выбран итеративный алгоритм Sum-Product с “мягким” входом, работающий с представлением кода в виде двудольного графа Таннера. Максимальное число итераций составило 50. Подробнее с методами декодирования можно ознакомиться в работах [30]–[31].

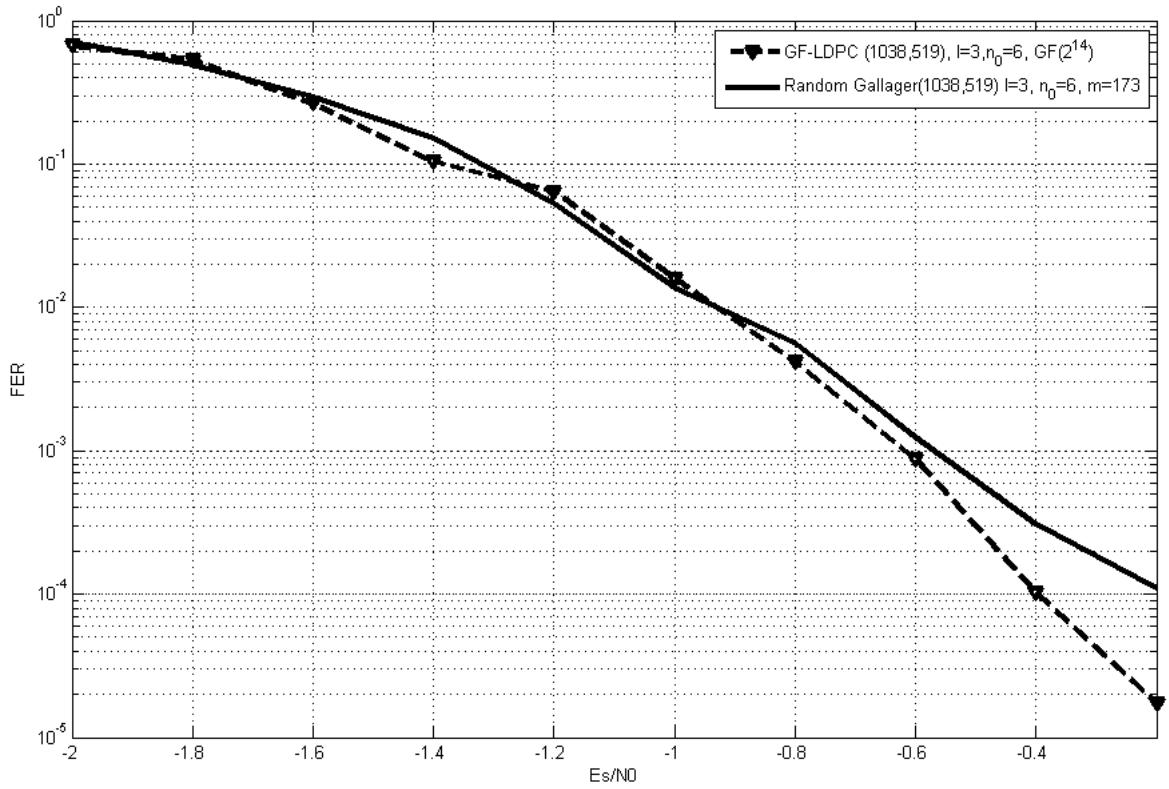

Рис 1. Зависимость вероятности ошибки на блок от отношения сигнал-шум на кодовый символ для случайного кода и кода над полем $GF(2^{14})$

Как следует из рис. 1, GF-код над полем $GF(2^{14})$, длиной $n = 1038$, который содержит ровно 3 единицы в каждом столбце и 6 единиц в каждой строке, выигрывает практически порядок по вероятности ошибки на блок у случайного кода из ансамбля Галлагера при отношении сигнал-шум -0.2 Дб.

Теперь приведем результаты моделирования GF-кода и случайного кода длин $n = 1960$.

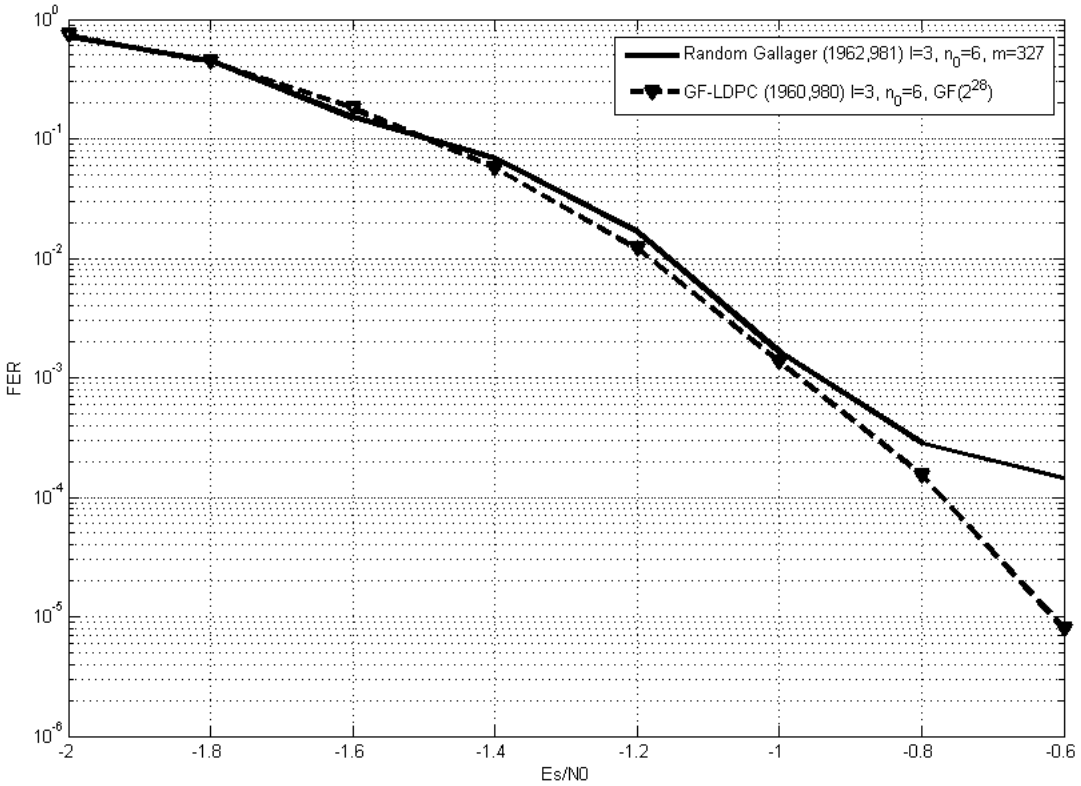

Рис 2. Зависимость вероятности ошибки на блок от отношения сигнал-шум на кодовый символ для случайного кода и кода над полем $GF(2^{28})$

Как следует из рис. 2, GF-код над полем $GF(2^{28})$, длиной $n = 1960$, который содержит ровно 3 единицы в каждом столбце и 6 единиц в каждой строке, так же выигрывает практически порядок по вероятности ошибки на блок у случайного кода из ансамбля Галлагера при отношении сигнал-шум -0.6 Дб.

В заключение приведем результаты моделирования GF-кода и случайного кода длин $n = 3078$.

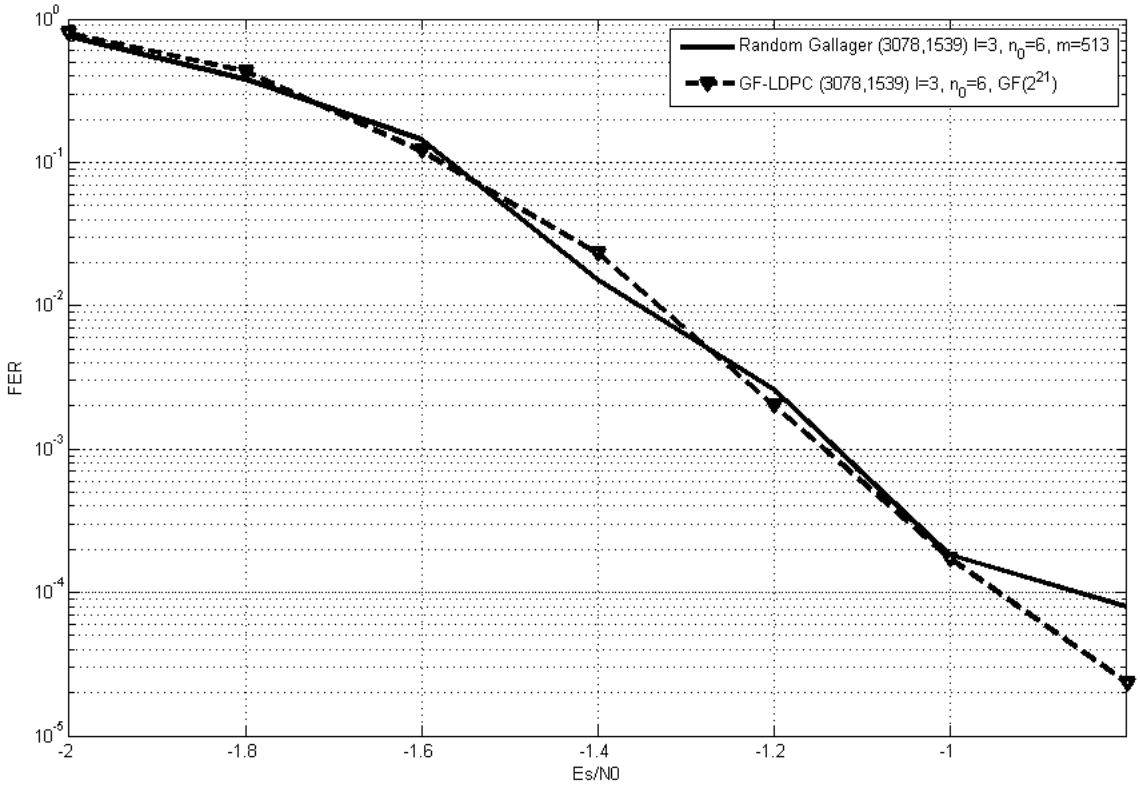

Рис 2. Зависимость вероятности ошибки на блок от отношения сигнал-шум на кодовый символ для случайного кода и кода над полем $GF(2^{21})$

Как следует из рис. 2, GF-код над полем $GF(2^{28})$, длиной $n = 3078$, который содержит ровно 3 единицы в каждом столбце и 6 единиц в каждой строке, так же выигрывает половину порядка по вероятности ошибки на блок у случайного кода из ансамбля Галлагера при отношении сигнал-шум -0.8 Дб.

4. ЗАКЛЮЧЕНИЕ

Результаты моделирования показывают, что описанные в статье GF-коды не уступают по корректирующим способностям кодам из ансамбля Галлагера, имея при этом более простую структуру проверочной матрицы.

Более того, результаты моделирования позволяют сделать вывод о возможности практического использования приведенных кодовых конструкций.

Кодовую конструкцию, описанную в §2.5 можно обобщить, абстрагируясь от мультипликативной группы поля , выбирая произвольные величины сдвигов и произвольную размерность матриц перестановок.

СПИСОК ЛИТЕРАТУРЫ

1. Gallager R. G. *Low-Density Parity-Check Codes.* Massachusetts: MIT Press, 1963.
2. Richardson T. J., Shokrollahi M. A., Urbanke R. L. Design of capacity-approaching irregular low-density parity check codes. *IEEE Trans. on Inform. Theory*, 2001, vol. 47, no. 2, pp. 619-637.

3. Lentmaier M., Zigangirov K. S. On generalized low-density paritycheck codes based on Hamming component codes. *IEEE Communication Letters*, 1999, vol. 3, no. 8, pp. 248-250.

4. Djurdjevic I., Xu J., Abdel-Ghaffar K., Lin S. A class of low-density parity-check codes constructed based on Reed-Solomon codes with two information symbols. *IEEE Commun. Lett,* 2003, vol. 7, pp. 317-319.

5. Groshev F.V., Zyablov V.V., Potapov V. G. Low-complexity decoded LDPC Codes with Reed-Solomon constituent codes. *In Proc. of the 11-th International Workshop on Algebraic and Combinatorial Coding Theory ACCT'08*, Pomporovo, Bulgaria, 2008.

6. Yi Y., Shaobo L., Dawei H. Construction of LDPC codes based on narrow-sense primitive BCH codes. *Vehicular Technology Conference*, Stockholm, Sweden, 2005, pp. 1571-1574.

7. Tanner M. A Recursive Approach to Low Complexity Codes. *IEEE Trans. Inform. Theory*, 1981, vol. 27, no. 5, pp. 533-547.

8. Kim S., Chung H., Shin D.-J. Girth analysis of Tanner's (3,5) QC LDPC codes. *In Proceedings of IEEE International Symposium on Information Theory (ISIT '05)*, 2005, pp. 1632-1636.

9. Djidjev Hristo N. A faster algorithm for computing the girth of planar and bounded genus graphs. *ACM Transactions on Algorithms (TALG)*, 2010, vol. 7, no. 1.

10. Xiaofu W., Xiaohu Y., Chunming Z. An Efficient Girth-Locating Algorithm for Quasi-Cyclic LDPC Codes. *In Proceedings of IEEE International Symposium on Information Theory (ISIT '06)*, 2006, pp. 817-820.

11. Fossorier P. C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. *IEEE Trans. Inform. Theory*, 2004, vol. 50, no. 8, pp. 1788-1793.

12. Okamura T. Designing LDPC codes using cyclic shifts. *Proc. IEEE Int. Symp. Information Theory.* Yokohama, 2003, p. 151.

13. Davydov A. A., Giulietti M., Marcugini S., Pambianco F. On the spectrum of possible parameters of symmetric configurations. *XII International Symposium on problems of redundancy in information and control systems*. 2009, pp. 69-54.

14. Levy Y., Costello D. J. An algebraic approach to constructing convolutional codes from quasi-cyclic codes. *DIMACS Ser. Discr.Math. Theor. Comput. Sci.*, 1993, vol. 14, pp. 188-198.

15. Fan J. L. Array codes as low-density parity check codes. *in Proc. 2nd Int. Symp. Turbo Codes and Related Topics*, 2000, Brest, France, pp. 543-546.

16. Ling Alan C. H. Difference Triangle Sets From Affine Planes. *IEEE Trans. Inform. Theory*, 2002, vol. 48, no. 8, pp. 2399-2401.

17. Kou Y., Lin S., Fossorier M. Low-destiny parity check codes based on finite geometries: A rediscovery and new results. *IEEE Trans. Inform. Theory*, 2001, vol. 47, pp. 2711-2736.

18. Hagiwara M., Nuida K., Kitagawa T. On the minimal length of quasi-cyclic ldpc codes with girth greater than or equal to 6. *in International Symposium on Information Theory and its Applications*, 2006.

19. Wang Y., Yedidia J., Draper S. Construction of high-girth QCLDPC codes. *in Proc. 5th Int. Symp. on Turbo Codes and Related Topics*, 2008, pp. 180-185.

20. Kim S., No J.-S., Chung H., Shin D.-J. Quasi-cyclic low-density parity-check codes with girth larger than 12. *IEEE Int. Symp. Inf. Theory*, 2007, vol. 53, no. 8, pp. 2885-2891.

21. Milenkovic O., Kashyap N., Leyba D. Shortened array codes of large girth. *IEEE Trans. Inf. Theory*, 2006, vol. 52, no. 8, pp. 3707-3722.

22. Яцкин Н. И. *Алгебра. Теоремы и алгоритмы.* Иваново: издательство Ивановского государственного университета, 2006.

23. Esmaeili M., Gholami M. Structured quasi-cyclic LDPC codes with girth 18 and column-weight J>3. *Int. Journal of Electron. and Commun. (AEU)*, 2010, vol. 64, no. 3, pp. 202-217.

24. Bocharova I. E., Kudriashov B. D., Satuikov R. V., Stiglmayr S. Short quasi-cyclic LDPC codes from convolutional codes. *Proc. IEEE Int. Symp. Information Theory*, 2010, Austin, Texas, pp. 551-555.

25. Liva G., Rayan W.E., Chiani M. Quasi-Cyclic Generalized LDPC Codes with Low Error Floors. *IEEE Transaction on Communications*, 2008, vol. 56, no. 1, pp. 49-57.

26. Huang C. M., Huang J. F., Yang C. C. Cyclic LDPC Codes from Quadratic Congruences. *IEEE Commun. Lett*, 2008, vol. 12, no. 4, pp. 313-315.

27. Myung S., Yang K., Kim J. Quasi-cyclic LDPC codes for fast encoding. *IEEE Trans. Inform. Theory*, 2008, vol. 51, no. 8, pp. 2894-2901.

28. Milenkovic O., Prakash K., Vasic B. Regular and irregular low density parity check codes for iterative decoding based on cycle-invariant difference sets. *in Proc. 41st Allerton Conf. Communication, Control and Computing*, 2003, Monticello, IL.

29. Gabidulin E., Moinian A., Honary B. Generalized construction of quasi-cyclic regular LDPC codes based on permutation matrices. *Proc. IEEE Int. Symp. Inf. Theory.* 2006, pp. 679-683.

30. Жилин И.В., Рыбин П.С., Зяблов В.В. Сравнение алгоритмов декодирования двоичных МПП-кодов с жёстким входом. 34 *международная конференция молодых ученых и специалистов ИППИ РАН "Информационные технологии и системы". Тезисы докладов.* Геленджик, 2011, стр. 221-227.

31. Kschischang F. R., Frey B. J., Loeliger H.A. Factor graphs and the sum-product algorithm. *IEEE Trans. Inform. Theory*, 2001, vol. 47, no. 2, pp. 498-519.