Информационные процессы, Том 12, № 1, 2012, стр. 31–52

ПЕРЕДАЧА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Сравнение различных конструкций двоичных МПП-кодов, построенных на основе матриц перестановок

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

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

Поступила в редколлегию 01.01.2012

Аннотация—В работе рассматриваются ансамбли двоичных кодов с малой плотностью проверок, построенные на основе матриц перестановок. Предложены алгоритмы генерации проверочных матриц таких кодов. 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 конструкцию кодов с малой плотностью проверок (МПП-кодов Галлагера) и предложил алгоритм генерации проверочной матрицы $\mathbf{H}$ таких кодов. Проверочную матрицу $\mathbf{H_0}$ МПП-кода длины n_0 можно записать как $\mathbf{H_0} = \underbrace{111\ldots1}_{n_0}$. Запишем диагональную блочную матрицу $\mathbf{H_m}$ с m проверочными матрицами $\mathbf{H_0}$ на главной диагонали:

$$\mathbf{H_m} = \underbrace{\begin{pmatrix} \mathbf{H_0} & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{0} & \mathbf{H_0} & \ldots & \mathbf{0} \\ \vdots & \vdots & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \ldots & \mathbf{H_0} \end{pmatrix}}_{m},$$

где m достаточно велико. Так как размер матрицы $\mathbf{H_0}$ равен $1 \times n_0$, то размер матрицы $\mathbf{H_m}$ – $m \times mn_0$. Пусть $\pi(\mathbf{H_m})$ – случайная перестановка столблов матрицы $\mathbf{H_m}$. Тогда матрица $\mathbf{H}$, составленная из $l > 2$ таких перестановок в качестве слоев,

$$\mathbf{H} = \begin{pmatrix} \mathbf{H_1} \\ \mathbf{H_2} \\ \vdots \\ \mathbf{H_l} \end{pmatrix} = \begin{pmatrix} \pi_1(\mathbf{H_m}) \\ \pi_2(\mathbf{H_m}) \\ \vdots \\ \pi_l(\mathbf{H_m}) \end{pmatrix}$$

является разреженной проверочной матрицей размера $lm \times mn_0$, которая определяет ансамбль МПП-кодов Галлагера длины $n = n_0 m, n \gg n_0$. Обозначим этот ансамбль $\mathcal{E}(l, n_0, m)$. Элементы ансамбля $\mathcal{E}(l, n_0, m)$ получаются путем независимого выбора перестановок π_i, $i = 1, 2, \ldots, l$. Все перестановки π_i выбираются равновероятно, таким образом на ансамбле $\mathcal{E}(l, n_0, m)$ задано равномерное распределение.

Нижняя оценка на скорость R кода из $\mathcal{E}(l, n_0, m)$ определяется формулой $R \geq 1 - l(1 - R_0)$, где $R_0 = \dfrac{n_0 - 1}{n_0} = 1 - \dfrac{1}{n_0}$ – скорость кода проверки на четность. Таким образом, получим оценку на скорость МПП-кодов Галлагера:

$$R \geq 1 - \frac{l}{n_0}. \tag{1}$$

МПП-коды принято классифицировать на две группы: регулярные (проверочная матрица $\mathbf{H}$ содержит ровно n_0 и l единиц в каждой строке и столбце соответственно) и нерегулярные (количество единиц в строке и столбце является переменным).

Известно, что эффективность нерегулярных МПП-кодов оказывается выше, чем регулярных. Это преимущество связано с тем, что нерегулярных кодах из-за различного числа единиц в строках и столбцах информационные символы защищены по-разному. В результате при декодировании проявляется так называемый эффект волны, когда более защищенные биты декодируются быстрее и затем как бы помогают при декодировании менее защищенных бит.

В то же время регулярные конструкции позволяют использовать методы оптимизации процедур генерации, хранения, кодирования и декодирования, а также получать коды с более предсказуемыми характеристиками.

В практических приложениях, вместо кодов из ансамбля Галлагера, часто используют МПП-коды, проверочная матрица которых основана на матрицах перестановок. Такой подход был предложен Ричардсоном в [2]. Он так же развит во многих работах, например в [3]–[5].

В работах [6]–[8] рассмотрены квадратные матрицы, состоящие из циркулянтных перестановочных матриц размера q или $q - 1$, где $q = p^m$, p – простое.

Наша задача заключается в разработке и исследовании различных конструкций проверочных матриц регулярных МПП-кодов, основанных на матрицах перестановок. В статье предложено несколько алгоритмов генерации проверочных матриц такого вида, доказана верхняя оценка на кодовое расстояние. Подробно исследованы свойства оператора циклического сдвига, а так же свойства уравнений и систем уравнений с матричными коэффициентами относительно векторных неизвестных.

Статья организована следующим образом: в § 2.1 введены основные определения и обозначения, используемые в статье. В § 2.2 представлена общая конструкция проверочной матрицы МПП-кодов, построенных на основе матриц перестановок. В § 2.3 дано определение оператора циклического сдвига и доказаны некоторые его свойства. В § 2.4 рассмотрены линейные векторные уравнения с матричными коэффициентами. В § 2.5 исследованы системы линейных векторных уравнений с матричными коэффициентами, доказаны результаты, связанные с существованием их решений. В § 2.6 представлены алгоритмы построения проверочных матриц МПП-кодов специального вида. В § 3 приведены результаты компьютерного моделирования описанных в статье конструкций кодов.

2. МПП-КОДЫ, ПОСТРОЕННЫЕ НА ОСНОВЕ МАТРИЦ ПЕРЕСТАНОВОК

2.1. Основные определения и обозначения

Ниже приведем основные определения и обозначения, которые будут использоваться в статье.

Определение. *Перестановка* – биективное отображение σ множества $M = \{1, 2, \ldots, m\}$ в себя. То есть $\sigma : i \mapsto j,\ i, j \in M$. Обычно перестановку записывают в виде:
$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & m \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(m) \end{pmatrix}$. Число m называют *длиной* перестановки.

Определение. Перестановку ϵ будем называть *единичной*, если $\forall i = \overline{1,n}\ \epsilon(i) = i$.

Введем на множестве $\mathcal{M}$ всех перестановок длины m операцию суперпозиции следующим образом: пусть $\pi, \sigma \in \mathcal{M}$, $k \in M$, тогда суперпозицией данных перестановок назовем перестановку $\tau = (\pi \cdot \sigma)(k) = \pi(\sigma(k))$

Замечание. Для любой перестановки $\sigma \in \mathcal{M}$ существует перестановка σ^{-1} такая, что: $\sigma \cdot \sigma^{-1} = \epsilon$. Такую перестановку назовем *обратной.*

Замечание. Множество всех перестановок длины m образуют конечную группу $\mathcal{S}_m$ относительно операции суперпозиции. Обычно эту группу называют симметрической. Очевидно, что $|\mathcal{S}_m| = m!$, где $|\cdot|$ – количество элементов в группе.

Определение. Под k -й *степенью* перестановки σ будем понимать k -кратную суперпозицию $\tau = \underbrace{\sigma \cdot \sigma \cdot \ldots \cdot \sigma}_{k} = \sigma^k$.

Определение. *Порядком* перестановки σ назовем наименьшее $n \in \mathbb{N}$, такое что $\sigma^n = \epsilon$. Будем записывать $n = ord\,\sigma$.

Любую перестановку $\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & m \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(m) \end{pmatrix}$ длины m можно представить в виде ортогональной матрицы $\mathbf{P}_\sigma = \begin{pmatrix} \mathbf{e}_{\sigma(1)} \\ \mathbf{e}_{\sigma(2)} \\ \mathbf{e}_{\sigma(3)} \\ \vdots \\ \mathbf{e}_{\sigma(m)} \end{pmatrix}$, где $\mathbf{e}_i$ – m-мерный базисный вектор, содержащий единицу на i позиции, и 0 – во всех остальных.

Как было отмечено, множество перестановок длины m образуют группу относительно операции суперпозиции, таким образом множество $\mathcal{P}$ – всех матриц перестановок так же образуют группу, которую мы обозначим $\mathcal{P}_m$. Очевидно, что $|\mathcal{P}_m| = m!$.

Приведем алгоритм построения перестановок специального вида, который потребуется нам в дальнейшем.

Определение. Пусть $\sigma \in \mathcal{S}_m$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & m \\ a_1 & a_2 & a_3 & \ldots & a_m \end{pmatrix}$, где $a_i = \sigma(i)$, $b \in \mathbb{N} : (b,m) = 1$, $(\cdot\,,\cdot)$ – наибольший общий делитель. Определим перестановку σ_b следующим образом: $\sigma_b = \begin{pmatrix} 1 & 2 & 3 & \ldots & m \\ c_1 & c_2 & c_3 & \ldots & c_m \end{pmatrix}$, где $c_i = (a_i b \bmod m) + 1$. Перестановку σ_b назовем *перестановкой-умножением.*

Лемма. *Если $(b,m) = t > 1$, то σ_b не является перестановкой.*

Доказательство. Для того, чтобы σ_b было биекцией, необходимо, чтобы $\sigma_b(i) \neq \sigma_b(j)$, $i \neq j$, или $c_i \neq c_j, i \neq j$. Покажем, что данное условие нарушается как только $(b,m) = t > 1$. Обозначим через $\mathcal{A} = \{\underbrace{a_i - a_j}_{i \neq j}\} = \{1, 2, \ldots, m-1\}$. Рассмотрим условие, когда $c_i = c_j$, т. е.

$$(a_i b \bmod m) + 1 = (a_j b \bmod m) + 1,$$
$$(a_i b \bmod m) = (a_j b \bmod m),$$
$$(a_i - a_j) b \bmod m = 0.$$

Так как $(b,m)=t>1$, то $\frac{m}{t}\in\mathcal{A}$. Таким образом, найдутся $a_i^\star\neq a_j^\star:\ a_i^\star-a_j^\star=\frac{m}{t}$, поэтому $(a_i^\star-a_j^\star)b\ mod\ m=\frac{m}{t}b\ mod\ m=m\frac{b}{t}\ mod\ m$ Так как $(b,m)=t>1$, то $\frac{b}{t}=z\in\mathbb{N}$, поэтому $m\frac{b}{t}\,mod\,m=zm\,mod\,m=0$. Таким образом $c_i=c_j$ при $i\neq j$. Поэтому σ_b не является биекцией.

Легко показать, что $b_i:\ (b_i,m)=1$ при фиксированном m образуют мультипликативную группу $G_m^\star$. $|G_m^\star|=\phi(m)$, где $\phi(\cdot)$ – функция Эйлера. Если m – простое, то $|G_m^\star|=m-1$

2.2. Общая конструкция проверочной матрицы МПП-кодов, основанных на матрицах перестановок

Пусть m, l, $n_0\in\mathbb{N}$, причем $n_0>l$, $m!>ln_0$. Рассмотрим группу $\mathcal{P}_m$, введенную нами ранее. Выберем ln_0 случайных матриц $\{\mathbf{P_{ij}}\}\subset\mathcal{P}_m$, $i=\overline{1,l}$, $j=\overline{1,n_0}$. Потребуем так же, что если $\mathbf{P_{ij}}=\mathbf{P_{ks}}$, то $i=j$, $k=s$. Ясно, что такие условия выбора матриц $\mathbf{P_{ij}}$ соответствуют урновой модели без возвращений. Построим проверочную матрицу $\mathbf{H_{l\times n_0}}$:

$$\mathbf{H}=\begin{pmatrix}\mathbf{P_{11}}&\mathbf{P_{12}}&\mathbf{P_{13}}&\dots&\mathbf{P_{1n_0}}\\ \mathbf{P_{21}}&\mathbf{P_{22}}&\mathbf{P_{23}}&\dots&\mathbf{P_{2n_0}}\\ \vdots&\vdots&\vdots&\vdots&\vdots\\ \mathbf{P_{l\,1}}&\mathbf{P_{l\,2}}&\mathbf{P_{l\,3}}&\dots&\mathbf{P_{l\,n_0}}\end{pmatrix}. \tag{2}$$

Указанный выше способ построения матрицы $\mathbf{H}$ гарантирует, что все матрицы в каждой строке и в каждом столбце будут различны. Так как $\mathbf{P_{ij}}$ – квадратная матрица размера $m\times m$, то размерность $\mathbf{H}$ – $ml\times mn_0$. $\mathbf{H}$ определяет ансамбль регулярных МПП-кодов Галлагера длины $n=n_0m$, который мы обозначим $\mathcal{E}_R(l,n_0,m)$. Элементы ансамбля $\mathcal{E}_R(l,n_0,m)$ получаются путем выбора без возвращений матриц перестановок $\mathbf{P_{ij}}\in\mathcal{P}_m$, $i=1,2,\dots,l$, $j=1,2,\dots,n_0$. Легко показать, что

$$|\mathcal{E}_R(l,n_0,m)|=\frac{(m!)!}{(ln_0)!}.$$

Согласно (1), скорость R кода из $\mathcal{E}_R(l,n_0,m)$ может быть оценена следующим образом:

$$R\geq 1-\frac{l}{n_0}.$$

Пример. Фиксируем $l=5$, тогда для скоростей $R=0.1,\ 0.2,\dots,0.9$ получим следующие значения n_0:

Таблица 1.

R	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
n_0	6	6	8	9	10	13	17	25	50

Аналогично, для $l=7$ получим:

Таблица 2.

R	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
n_0	8	9	10	12	14	18	24	35	70

Докажем теорему, дающую верхнюю оценку на кодовое расстояние кода $\mathcal{C} \in \mathcal{E}_R(l, n_0, m)$.

Теорема. *$d_{\mathcal{C}} \leq 2m \; \forall \mathcal{C} \in \mathcal{E}_R(l, n_0, m)$, где $d_{\mathcal{C}}$ – кодовое расстояние кода $\mathcal{C}$.*

Доказательство. Для доказательства достаточно показать, что что вектор

$$\mathbf{c} = (\underbrace{1, 1, 1 \ldots, 1}_{2m}, \underbrace{0, 0, \ldots, 0}_{n-2m})$$

является кодовым словом, то есть $\mathbf{c}\mathbf{H}^{\mathrm{T}} = \mathbf{0}$. Данное равенство эквивалентно сложению первых $2m$ строк проверочной матрицы $\mathbf{H}$ по модулю 2. Первые $2m$ строк соответствуют первым 2 слоям проверочной матрицы $\mathbf{H}$. Каждый столбец данной двуслойной матрицы содержит ровно 2 единицы. Таким образом $\mathbf{c}$ действительно является кодовым словом. Так как $w(\mathbf{c}) = 2m$, то $d_{\mathcal{C}} \leq 2m$.

Согласно теореме Варшамова–Гилберта при достаточно большом n не существует двоичного кода со скоростью R, имеющего кодовое расстояние больше, чем расстояние, которое находится из уравнения $R = 1 - \mathcal{H}\Big(\dfrac{d_{\mathcal{C}}}{n}\Big)$, где $\mathcal{H}(\delta) = -\delta \log_2(\delta) - (1-\delta)\log_2(1-\delta)$ – энтропийная функция Шеннона двоичного информационного источника. Мы доказали, что $d_{\mathcal{C}} \leq 2m$, поэтому $\dfrac{d_{\mathcal{C}}}{n} \leq \dfrac{2m}{n_0 m} = \dfrac{2}{n_0}$. Таким образом

$$n_0 \leq \frac{2}{\delta}. \tag{3}$$

Построим таблицу зависимости между R и n_0 в соответствии с (3).

Таблица 3.

R	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
δ	0.32	0.24	0.19	0.15	0.11	0.08	0.05	0.03	0.01
n_0	7	9	11	14	19	25	40	67	200

Данная таблица показывает, каким должно быть значение n_0, чтобы, код имел возможность достигать границы Варшамова–Гилберта. С другой стороны, скорость R так же связана с n_0 и l. Легко заметить, что $R \geq \dfrac{1}{n_0}$, $\forall n_0$. Таким образом $\dfrac{1}{R} \leq n_0 \leq \dfrac{2}{\delta}$. Таким образом, при малых значениях n_0, и, соответсвтвенно, при малых скоростях (согласно таблице 3), не существует кодов с параметрами, которые близки к оптимальным.

2.3. Оператор циклического сдвига

Определение. Под $V^m(2)$ будем понимать множество векторов $\{\mathbf{a_1}, \mathbf{a_2}, \ldots \mathbf{a_{2^m}}\}$, $\mathbf{a_i} = (a_{i1}, a_{i2}, \ldots, a_{im})$, $m \in \mathbb{N}$, $m \geq 2$, $a_{ij} \in GF(2)$.

Определение. Под *суммой* векторов $\mathbf{a} + \mathbf{b}$, где $\mathbf{a}, \mathbf{b} \in V^m(2)$ будем понимать вектор $\mathbf{c} = (c_1, c_2, \ldots c_m)$, где $c_i = (a_i + b_i) \; mod \, 2$.

Определение. *Весом* $w(\mathbf{a})$, где $\mathbf{a} \in V^m(2)$, будем называть количество ненулевых координат вектора $\mathbf{a}$.

Очевидно, что $V^m(2)$ является линейным пространством над полем $GF(2)$. Введем в пространстве $V^m(2)$ операцию циклического сдвига. Введем ряд необходимых определений.

Определение. Под *матрицей h-кратного циклического сдвига* $\mathbf{E} \oplus h$, где $\mathbf{E}$ – единичная матрица размера $m \times m$, $h \in \mathbb{Z}$, $0 \le h \le m$, будем понимать квадратную матрицу следующего вида:

$$\mathbf{E} \oplus h = \begin{pmatrix} 0 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ & & & & & & & \ddots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & & \\ 0 & 0 & 0 & \dots & \dots & \dots & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & \dots & \dots & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & \dots & \dots & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & \dots & \dots & \dots & 0 & 0 \\ & & & \ddots & & & & & \\ \dots & \dots & \dots & & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 & 1 & 0 & \dots & \dots & 0 \end{pmatrix}, \tag{4}$$

где $h+1$ – позиция единицы в 1 столбце, а $m-h+1$ – позиция единицы в 1 строке. Будем считать, что $\mathbf{E} \oplus 0 = \mathbf{E} \oplus m = \mathbf{E}$.

Определение. *h-кратной циклической перестановкой* назовем такую перестановку $\lambda_h \in \mathcal{S}_m$, что $\mathbf{P}_{\lambda_\mathbf{h}} = \mathbf{E} \oplus h$.

Исходя из построения видно, что множество $\mathcal{P}_m^s = \{\mathbf{E},\ \mathbf{E} \oplus 1,\ \mathbf{E} \oplus 2, \dots, \mathbf{E} \oplus (m-1)\} \subset \mathcal{P}_m$. Данное множество образует циклическую группу порядка m.

Замечание. Легко заметить, что $(\mathbf{E} \oplus h)^{-1} = \mathbf{E} \oplus (m-h)$.

Определение. Оператор $\mathcal{A}_h : V^m(2) \mapsto V^m(2)$, который сопоставляет каждому вектору $\mathbf{a} \in V^m(2)$ вектор $\mathbf{a_h} \in V^m(2)$ по правилу $\mathcal{A}_h(\mathbf{a}) = (\mathbf{E} \oplus h)\mathbf{a}$ будем называть *оператором h - кратного циклического сдвига.*

Рассмотрим свойства построенного оператора $\mathcal{A}_h$:

1. $\mathcal{A}_h$ имеет 2 неподвижные точки – нулевой и единичный вектора;
2. $\mathcal{A}_h$ инвариантен относительно веса: если $\mathbf{a} \in V^m(2)$, $w(\mathbf{a}) = k$, то $w(\mathcal{A}_h(\mathbf{a})) = k$;
3. $\mathcal{A}_h$ является аддитивным: если $\mathbf{a_1}, \mathbf{a_2} \in V^m(2)$, то $\mathcal{A}_h(\mathbf{a_1} + \mathbf{a_2}) = \mathcal{A}_h(\mathbf{a_1}) + \mathcal{A}_h(\mathbf{a_2})$;
4. $\mathcal{A}_h$ является однородным.

Свойства (3) и (4) позволяют сделать заключение о линейности оператора $\mathcal{A}_h$.

Определение. *Суперпозицией* операторов $\mathcal{A}_{h_1}$ и $\mathcal{A}_{h_2}$ назовем оператор $\mathcal{A}_{h_1} \cdot \mathcal{A}_{h_2} = \mathcal{A}_{(h_1+h_2) \bmod m}$.

Из определения следует коммутативность операции суперпозиции: $\mathcal{A}_{h_1} \cdot \mathcal{A}_{h_2} = \mathcal{A}_{h_2} \cdot \mathcal{A}_{h_1}$.

Теперь докажем теорему, в которой утверждается, что оператор $\mathcal{A}_h$ имеет ровно две неподвижные точки.

Теорема. *(О неподвижных точках) Если $\mathcal{A}_h$ – оператор циклического сдвига, $h_1, h_2 \in \mathbb{N}$, $h_1, h_2 < m$, $h_1 \ne h_2$, $\mathbf{a} = (a_1, a_2, \dots, a_m)$, $\mathbf{a} \in V^m(2)$, то из условия $\mathcal{A}_{h_1}(\mathbf{a}) = \mathcal{A}_{h_2}(\mathbf{a})$ следует, что $\mathbf{a} = (0, 0, \dots, 0)$ или $\mathbf{a} = (1, 1, \dots, 1)$.*

Доказательство. Пусть $\mathcal{A}_{h_1}(\mathbf{a}) = \mathcal{A}_{h_2}(\mathbf{a})$, по определению оператора циклического сдвига это значит, что $(\mathbf{E} \oplus h_1)\mathbf{a} = (\mathbf{E} \oplus h_2)\mathbf{a}$.

Подействуем на обе стороны данного равенства оператором $\mathcal{A}_{m-h_1}$, получим: $\mathcal{A}_{m-h_1} \cdot \mathcal{A}_{h_1}(\mathbf{a}) = \mathcal{A}_{m-h_1} \cdot \mathcal{A}_{h_2}(\mathbf{a})$ По определению суперпозиции операторов $\mathcal{A}_{m-h_1} \cdot \mathcal{A}_{h_1}(\mathbf{a}) = \mathcal{A}_{m-h_1+h_1}(\mathbf{a}) = \mathcal{A}_m(\mathbf{a}) = \mathbf{E}\mathbf{a} = \mathbf{a}$. Тогда условие равенства операторов примет вид:

$$\mathbf{E}\mathbf{a} = (\mathbf{E} \oplus h)\mathbf{a},$$

$$(\mathbf{E} \oplus h)\mathbf{a} + \mathbf{E}\mathbf{a} = \mathbf{0},$$

$$((\mathbf{E} \oplus h) + \mathbf{E})\mathbf{a} = \mathbf{0},$$

где $h = (m - h_1 + h_2) \, mod \, m$.

Пусть $\mathbf{S} = (\mathbf{E} \oplus h) + \mathbf{E}$. Исследуем матричное уравнение $\mathbf{S}\mathbf{a} = \mathbf{0}$, где

$$\mathbf{S} = \begin{pmatrix} 1 & 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \ddots & \dots \\ 0 & 0 & 0 & \dots & \dots & \dots & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & \dots & \dots & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & \dots & \dots & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & \dots & \dots & \dots & 0 & 0 \\ \dots & \dots & \dots & \ddots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & 0 & 1 & 0 & \dots & \dots & 1 \end{pmatrix}.$$

Каждая строка и каждый столбец матрицы $\mathbf{S}$ содержат ровно 2 единицы. Из структуры $\mathbf{S}$ видно, что матричное уравнение $\mathbf{S}\mathbf{a} = \mathbf{0}$ порождает m уравнений для коэффициентов вектора $\mathbf{a}$:

$$\begin{cases} a_{i_1} + a_{j_1} = 0 \\ a_{i_2} + a_{j_2} = 0 \\ \quad \dots \\ a_{i_m} + a_{j_m} = 0 \, . \end{cases}$$

Причем каждый коэффициент вектора присутствует ровно в двух уравнениях. Рассмотрим два таких связанных уравнения:

$$\begin{cases} a_{i_k} + a_{j_s} = 0 \\ a_{i_k} + a_{j_t} = 0 \, . \end{cases}$$

Из данной системы следует, что $a_{j_s} = a_{j_t} = a_{i_k}$. Однако, каждая из данных координат вновь учавствует в построении 2 уравнений. Проводя аналогичные рассуждения, получим, что $a_i = a_j \; \forall i, j \leq m$. Таким образом $\mathbf{a} = (0, 0, \dots, 0)$ или $\mathbf{a} = (1, 1, \dots, 1)$.

Данная теорема имеет полезное следствие, которое необходимо для исследования систем векторных уравнений с матричными коэффициентами.

Следствие. *Если* $\mathbf{a} \neq (0, 0, \dots, 0)$ *и* $\mathbf{a} \neq (1, 1, \dots, 1)$, *то* $\mathcal{A}_{h_1}(\mathbf{a}) = \mathcal{A}_{h_2}(\mathbf{a})$ *тогда и только тогда, когда* $h_1 = h_2$.

2.4. Линейные векторные уравнения с матричными коэффициентами

Рассмотрим уравнение

$$\mathbf{P_1 a_1} + \mathbf{P_2 a_2} = \mathbf{0}, \tag{5}$$

где $\mathbf{P_i} \in \mathcal{P}_m^s$, $\mathbf{a_i} \in V^m(2)$. Такое уравнение назовем *однородным линейным уравнением.* Изучение уравнения (5) начнем с тривиального случая, когда $\mathbf{P_1} = \mathbf{E}$, $\mathbf{P_2} = \mathbf{E} \oplus 1$. Очевидно, что $\mathbf{a_1} = \mathbf{a_2} = (0, 0, \ldots, 0)$ и $\mathbf{a_1} = \mathbf{a_2} = (1, 1, \ldots, 1)$ являются решениями уравнения (5). Такие решения будем называть *тривиальными.* Выясним, существуют ли нетривиальные решения уравнения (5). Для этого преобразуем его следующим образом:

$$\mathbf{E a_1} + (\mathbf{E} \oplus 1)\mathbf{a_2} = \mathbf{0},$$

$$\mathbf{a_1} = (\mathbf{E} \oplus 1)\mathbf{a_2}.$$

По определению оператора циклического сдвига последнее равенство означает, что

$$\mathbf{a_1} = \mathcal{A}_1(\mathbf{a_2}).$$

Таким образом мы установили, что частный вид уравнения (5) имеет 2^m различных пар решений вида $\{\mathbf{a_2}, \mathcal{A}_1(\mathbf{a_2})\}$. Аналогичными рассуждениями можно показать, что решение уравнения

$$\mathbf{E a_1} + (\mathbf{E} \oplus t)\mathbf{a_2} = \mathbf{0} \tag{6}$$

имеет вид $\{\mathbf{a_2}, \mathcal{A}_t(\mathbf{a_2})\}$.

Легко показать, что решение частного случая уравнения (5) инвариантно относительно k - кратного циклического сдвига при $k + 1 \leq m$. В самом деле, подействуем на обе стороны уравнения оператором $\mathcal{A}_k$:

$$\mathcal{A}_k\Big(\mathbf{E a_1} + (\mathbf{E} \oplus 1)\mathbf{a_2}\Big) = \mathcal{A}_k(\mathbf{0}).$$

Так как оператор циклического сдвига линеен и $\mathbf{0}$ – его неподвижная точка, то

$$\mathcal{A}_k(\mathbf{a_1}) + \mathcal{A}_{k+1}(\mathbf{a_2}) = \mathbf{0},$$

$$\mathcal{A}_k(\mathbf{a_1}) = \mathcal{A}_{k+1}(\mathbf{a_2}).$$

Подействовав на последнее выражение оператором $\mathcal{A}_{m-k}$ получим

$$\mathcal{A}_m(\mathbf{a_1}) = \mathcal{A}_{m+1}(\mathbf{a_2}).$$

Так как $\mathcal{A}_m(\mathbf{a_1}) = \mathbf{a_1}$ и $\mathcal{A}_{m+1}(\mathbf{a_2}) = \mathcal{A}_m\Big(\mathcal{A}_1(\mathbf{a_2})\Big) = \mathcal{A}_1(\mathbf{a_2})$, то получим

$$\mathbf{a_1} = \mathcal{A}_1(\mathbf{a_2}),$$

что эквивалентно уравнению (5).

Применяя аналогичные рассуждения легко доказать следующую теорему.

Теорема. *(О структуре решения однородного линейного уравнения) Если в уравнении* (5) $\mathbf{P_1} = \mathbf{E} \oplus i_1$, $\mathbf{P_2} = \mathbf{E} \oplus i_2$, $i_1 < i_2$, *то уравнение имеет* 2^m *различных пар решений вида* $\{\mathbf{a_2}, \mathcal{A}_{i_2 - i_1}(\mathbf{a_2})\}$ $\forall \mathbf{a_2} \in V^m(2)$.

Полученный результат легко обобщается на случай, когда уравнение (5) содержит произвольное число переменных $\mathbf{a_1}, \mathbf{a_2}, \ldots \mathbf{a_n}$, $n \leq 2^m$, а именно справедлива

Теорема. *Пусть в уравнении* $\sum\limits_{j=1}^{n} \mathbf{P_{i_j}} \mathbf{a_j} = \mathbf{0}$, $i_1 < i_k$, $\forall k > 1$, *тогда уравнение имеет* $2^{m(n-1)}$ *решений, которые могут быть найдены по формуле* $\{\mathbf{a_1} = \sum\limits_{k=2}^{n} \mathcal{A}_{i_k - i_1}(\mathbf{a_k}), \mathbf{a_2}, \ldots, \mathbf{a_n}\}$ $\forall \mathbf{a_k} \in V^m(2)$, $1 < k \leq n$.

2.5. Исследование систем линейных векторных уравнений с матричными коэффициентами

Рассмотрим ансамбль $\mathcal{E}_R(l, n_0, m)$ регулярных двоичных МПП -кодов. Рассмотрим подмножество этого ансамбля: пусть $\mathbf{H_s} \in \mathcal{E}_R(l, n_0, m)$ – проверочная матрица вида

$$\mathbf{H_s} = \begin{pmatrix} \mathbf{P_{11}} & \mathbf{P_{12}} & \mathbf{P_{13}} & \ldots & \mathbf{P_{1n_0}} \\ \mathbf{P_{21}} & \mathbf{P_{22}} & \mathbf{P_{23}} & \ldots & \mathbf{P_{2n_0}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{P_{l1}} & \mathbf{P_{l2}} & \mathbf{P_{l3}} & \ldots & \mathbf{P_{ln_0}} \end{pmatrix}, \tag{7}$$

где $\mathbf{P_{ij}} = \mathbf{E} \oplus i_j \in \mathcal{P}_s^m$, $i = \overline{1, n_0}$, $j = \overline{1, l}$. Если $n = n_0 m$ – длина кодового слова, то условие различия всех матриц в каждой строке и каждом столбце проверочной матрицы эквивалентно условию $m \geq l n_0$. Таким образом $\mathbf{H_s}$ определяет ансамбль двоичных МПП -кодов, который мы обозначим $\mathcal{E}_S(l, n_0, m)$. Из построения ансамбля ясно, что $\mathcal{E}_S(l, n_0, m) \subset \mathcal{E}_R(l, n_0, m)$. Элементы ансамбля $\mathcal{E}_S(l, n_0, m)$ получаются путем выбора без возвращений матриц перестановок $\mathbf{P_{ij}} \in \mathcal{P}_m^s$, $i = 1, 2, \ldots, l$, $j = 1, 2, \ldots, n_0$. Легко показать, что

$$|\mathcal{E}_S(l, n_0, m)| = \frac{m!}{(l n_0)!}.$$

Преимущество ансамбля $\mathcal{E}_S(l, n_0, m)$ перед ансамблем $\mathcal{E}_R(l, n_0, m)$ заключается в том, что нам достаточно хранить не $l n_0$ матриц перестановок, а $l n_0$ чисел, так как матрица $\mathbf{E} \oplus h$ полностью определяется числом h.

Пусть $\mathbf{c}$ – кодовое слово двоичного МПП –кода из ансамбля $\mathcal{E}_S(l, n_0, m)$. Рассмотрим проверочное соотношение $\mathbf{c}\mathbf{H}_s^{\mathrm{T}} = \mathbf{0}$. Так как длина кодового слова равна $n = n_0 m$, то можно разбить $\mathbf{c}$ на n_0 векторов $\mathbf{a_1}$, $\mathbf{a_2}, \ldots, \mathbf{a_{n_0}}$, $\mathbf{a_i} \in V^m(2)$. Тогда проверочное соотношение является недоопределенной системой векторных уравнений с матричными коэффициентами, а именно

$$\begin{cases} \mathbf{P_{11}}\mathbf{a_1} + \mathbf{P_{12}}\mathbf{a_2} + \ldots + \mathbf{P_{1n_0}}\mathbf{a_{n_0}} = \mathbf{0} \\ \mathbf{P_{21}}\mathbf{a_1} + \mathbf{P_{22}}\mathbf{a_2} + \ldots + \mathbf{P_{2n_0}}\mathbf{a_{n_0}} = \mathbf{0} \\ \quad \ldots \\ \mathbf{P_{l1}}\mathbf{a_1} + \mathbf{P_{l2}}\mathbf{a_2} + \ldots + \mathbf{P_{ln_0}}\mathbf{a_{n_0}} = \mathbf{0} \end{cases}. \tag{8}$$

Вопрос о структуре решения системы (8) в настоящее время является открытым. Мы рассмотрим частный случай, а именно

$$\begin{cases} \mathbf{P_{11}}\mathbf{a_1} + \mathbf{P_{12}}\mathbf{a_2} = \mathbf{0} \\ \mathbf{P_{21}}\mathbf{a_1} + \mathbf{P_{22}}\mathbf{a_2} = \mathbf{0} \\ \quad \ldots \\ \mathbf{P_{l1}}\mathbf{a_1} + \mathbf{P_{l2}}\mathbf{a_2} = \mathbf{0} \end{cases}. \tag{9}$$

При $l = 2$ она является однородной системой крамеровского типа

$$\begin{cases} \mathbf{P_{11}}\mathbf{a_1} + \mathbf{P_{12}}\mathbf{a_2} = \mathbf{0} \\ \mathbf{P_{21}}\mathbf{a_1} + \mathbf{P_{22}}\mathbf{a_2} = \mathbf{0} \end{cases}. \tag{10}$$

Пусть $\mathbf{P_{11}} = \mathbf{E} \oplus i_1$, $\mathbf{P_{12}} = \mathbf{E} \oplus i_2$, $\mathbf{P_{21}} = \mathbf{E} \oplus j_1$, $\mathbf{P_{22}} = \mathbf{E} \oplus j_2$, всегда можно считать, что $i_2 > i_1$, $j_2 > j_1$. Очевидно, $\mathbf{a_1} = \mathbf{a_2} = (0, 0, \ldots, 0)$ и $\mathbf{a_1} = \mathbf{a_2} = (1, 1, \ldots, 1)$ являются тривиальными решениями системы (10). Исследуем систему на нетривиальные решения. Из первого уравнения следует, что $\mathbf{a_1} = \mathcal{A}_{i_2-i_1}(\mathbf{a_2})$, а из второго – $\mathbf{a_1} = \mathcal{A}_{j_2-j_1}(\mathbf{a_2})$. Таким образом, $\mathcal{A}_{j_2-j_1}(\mathbf{a_2}) = \mathcal{A}_{i_2-i_1}(\mathbf{a_2})$. Из следствия из теоремы о неподвижных точках это означает, что

$$i_2 - i_1 = j_2 - j_1. \tag{11}$$

Уравнение (11) назовем *уравнением равномерности*. Понятие равномерности заменяет определение линейной зависимости в пространстве $V^m(2)$. Систему, для которой выполняется уравнение равномерности назовем *равномерной системой*.

Теперь покажем, что из уравнения (11) следует существование нетривиальных решений системы (10).

В самом деле, из системы

$$\begin{cases} (\mathbf{E} \oplus i_1)\mathbf{a_1} + (\mathbf{E} \oplus i_2)\mathbf{a_2} = \mathbf{0} \\ (\mathbf{E} \oplus j_1)\mathbf{a_1} + (\mathbf{E} \oplus j_2)\mathbf{a_2} = \mathbf{0} \end{cases}$$

следует, что

$$\begin{cases} \mathbf{a_1} = \mathcal{A}_{i_2-i_1}(\mathbf{a_2}) \\ \mathbf{a_1} = \mathcal{A}_{j_2-j_1}(\mathbf{a_2}) \end{cases},$$

но так как $i_2 - i_1 = j_2 - j_1$, то из следствия теоремы о неподвижных точках, получим, что $\forall \mathbf{a_2} \in V^m(2)\ \mathcal{A}_{i_2-i_1}(\mathbf{a_2}) = \mathcal{A}_{j_2-j_1}(\mathbf{a_2})$. Таким образом, оба уравнения последней системы являются эквивалентными. Решения системы (10) совпадают с решениями любого из этих уравнений. Как было показано выше, однородное линейное уравнение всегда имеет 2^m решений, из которых $2^m - 2$ являются нетривиальными.

Таким образом доказана

Теорема. *Система* (10) *имеет нетривиальные решения тогда и только тогда, когда она является равномерной.*

Замечание. Легко заметить, что уравнение равномерности можно получить методами классической матричной алгебры. Известно, что однородная система крамеровского типа над полем $\mathbb{R}$ вещественных чисел имеет ненулевые решения тогда и только тогда, когда определитель матрицы системы равен нулю. В нашем случае это означает, что

$$det \begin{pmatrix} \mathbf{P_{11}} & \mathbf{P_{12}} \\ \mathbf{P_{21}} & \mathbf{P_{22}} \end{pmatrix} = \mathbf{P_{11}P_{22}} + \mathbf{P_{21}P_{12}} = \mathbf{0}.$$

Так как $\mathbf{P_{11}} = \mathbf{E} \oplus i_1$, $\mathbf{P_{12}} = \mathbf{E} \oplus i_2$, $\mathbf{P_{21}} = \mathbf{E} \oplus j_1$, $\mathbf{P_{22}} = \mathbf{E} \oplus j_2$, то $\mathbf{P_{11}P_{22}} + \mathbf{P_{21}P_{12}} = \mathbf{E} \oplus (i_1 + j_2) + \mathbf{E} \oplus (j_1 + i_2) = \mathbf{0}$, откуда $i_1 + j_2 = j_1 + i_2$, что эквивалентно уравнению равномерности.

Уравнение равномерности легко обобщается для случая, когда $l > 2$. Поэтому предыдущую теорему можно обобщить для и системы (9).

Теорема. *Система* (9) *имеет нетривиальные решения тогда и только тогда, когда она является равномерной.*

Исследование систем большей размерности является затруднительным, так как при их анализе возникают матрицы вида $\mathbf{P_i} + \mathbf{P_j}$ ($\mathbf{P_i}, \mathbf{P_j} \in \mathcal{P}_s^m$), которые не только не являются матрицами циклического сдвига, но и не принадлежат группе $\mathcal{P}^m$. Например, можно показать, что при четном m определитель матрицы $\mathbf{P_i} + \mathbf{P_j}$ равен нулю, а при нечетных – 2. Тем не менее для системы (8) справедлива

Теорема. *Если система* (8) *является равномерной, то она имеет нетривиальные решения.*

Поясним, что означает равномерность для системы (8). Для этого представим $\mathbf{P_{ks}}$ в виде $\mathbf{E} \oplus i_{ks}$, тогда получим

$$\begin{cases} (\mathbf{E} \oplus i_{11})\mathbf{a_1} + (\mathbf{E} \oplus i_{12})\mathbf{a_2} + \ldots + (\mathbf{E} \oplus i_{1n_0})\mathbf{a_2} = \mathbf{0} \\ (\mathbf{E} \oplus i_{21})\mathbf{a_1} + (\mathbf{E} \oplus i_{22})\mathbf{a_2} + \ldots + (\mathbf{E} \oplus i_{2n_0})\mathbf{a_2} = \mathbf{0} \\ \quad \ldots \\ (\mathbf{E} \oplus i_{l1})\mathbf{a_1} + (\mathbf{E} \oplus i_{l2})\mathbf{a_2} + \ldots + (\mathbf{E} \oplus i_{ln_0})\mathbf{a_2} = \mathbf{0} \quad . \end{cases} \tag{12}$$

Равномерность системы (12), а значит и (8) равносильна выполнению следующих $(l-1)n_0$ соотношений:

$$i_{21} = (i_{11} + h_1)\ mod\, m, i_{22} = (i_{12} + h_1)\ mod\, m, \ldots, i_{2n_0} = (i_{1n_0} + h_1)\ mod\, m$$

$$i_{31} = (i_{11} + h_2)\ mod\, m, i_{32} = (i_{12} + h_2)\ mod\, m, \ldots, i_{3n_0} = (i_{1n_0} + h_2)\ mod\, m$$

$$\ldots$$

$$i_{l1} = (i_{11} + h_{l-1})\ mod\, m, i_{l2} = (i_{12} + h_{l-1})\ mod\, m, \ldots, i_{ln_0} = (i_{1n_0} + h_{l-1})\ mod\, m.$$

2.6. Специальные виды проверочных матриц МПП-кодов.

МПП-коды, основанные на перестановках-умножениях

Пусть $\sigma \in \mathcal{S}_m$, возьмем случайное $b_1 \in \mathbb{N}$, $(b_1, m) = 1$, $b_1^x = 1\, mod\, m$, $x \geq l$. Тогда существует перестановки-умножения σ_{b_1}, $\sigma_{b_1^2}$, $\ldots$, $\sigma_{b_1^l}$, причем условия $b_1^x = 1\, mod\, m$ и $x \geq l$ гарантируют, что $\sigma_{b_1^i} = \sigma_{b_1^j}$ тогда и только тогда, когда $i = j$ $(i, j \leq l)$.

Каждой перестановке $\sigma_{b_1^i}$ поставим в соответствие матрицу перестановок $\mathbf{P}_{\sigma_{\mathbf{b_1^i}}}$. Построим столбец $\mathbf{P_1}$, состоящий из таких матриц, получим

$$\mathbf{P_1} = \begin{pmatrix} \mathbf{P}_{\sigma_{\mathbf{b_1}}} \\ \mathbf{P}_{\sigma_{\mathbf{b_1^2}}} \\ \mathbf{P}_{\sigma_{\mathbf{b_1^3}}} \\ \vdots \\ \mathbf{P}_{\sigma_{\mathbf{b_1^l}}} \end{pmatrix}.$$

Выберем $b_2 \in \mathbb{N}$, $(b_2, m) = 1$, $b_2 \neq b_1^i\ mod\, m$, $i = \overline{1, l}$. Построим перестановки-умножения $\sigma_{b_2 b_1}$, $\sigma_{b_2 b_1^2}$, $\ldots$, $\sigma_{b_2 b_1^l}$. Из алгоритма построения следует, что $\sigma_{b_1^i} \neq \sigma_{b_2 b_1^j}$ $\forall i, j \leq l$. Вновь отобразим каждую перестановку $\sigma_{b_2 b_1^i}$ на матрицу перестановок $\mathbf{P}_{\sigma_{\mathbf{b_2 b_1^i}}}$. Построим столбец $\mathbf{P_2}$, состоящий из таких матриц, получим

$$\mathbf{P_2} = \begin{pmatrix} \mathbf{P}_{\sigma_{\mathbf{b_2 b_1}}} \\ \mathbf{P}_{\sigma_{\mathbf{b_2 b_1^2}}} \\ \mathbf{P}_{\sigma_{\mathbf{b_2 b_1^3}}} \\ \vdots \\ \mathbf{P}_{\sigma_{\mathbf{b_2 b_1^l}}} \end{pmatrix}.$$

Для $b_3 \in \mathbb{N}$ потребуем выполнения всех условий, описанных выше, и, кроме того, $b_3 \neq b_2 b_1^i \ mod \ m$. Вообще, для b_j необходимо выполнение $j-1$ соотношения

$$\begin{cases} b_j \neq b_1^i \, mod \, m \\ b_j \neq b_2 b_1^i \, mod \, m \\ b_j \neq b_3 b_1^i \, mod \, m \\ \dots \\ b_j \neq b_{j-1} b_1^i \, mod \, m \, , \end{cases}$$

тогда способом, описанным выше, построим множества $\left\langle \{\sigma_{b_j b_1^i}\}_{i=1}^{l} \right\rangle_{j=3}^{n_0}$. Каждому $\{\sigma_{b_j b_1^i}\}_{i=1}^{l}$ поставим в соответствие

$$\mathbf{P_j} = \begin{pmatrix} \mathbf{P}_{\sigma_{\mathbf{b_j b_1}}} \\ \mathbf{P}_{\sigma_{\mathbf{b_j b_1^2}}} \\ \mathbf{P}_{\sigma_{\mathbf{b_j b_1^3}}} \\ \vdots \\ \mathbf{P}_{\sigma_{\mathbf{b_j b_1^l}}} \end{pmatrix} .$$

Тогда матрица

$$\mathbf{H_m} = (\mathbf{P_1}, \mathbf{P_2}, \dots, \mathbf{P_{n_0}}) = \begin{pmatrix} \mathbf{P}_{\sigma_{\mathbf{b_1}}} & \mathbf{P}_{\sigma_{\mathbf{b_2 b_1}}} & \dots & \mathbf{P}_{\sigma_{\mathbf{b_{n_0} b_1}}} \\ \mathbf{P}_{\sigma_{\mathbf{b_1^2}}} & \mathbf{P}_{\sigma_{\mathbf{b_2 b_1^2}}} & \dots & \mathbf{P}_{\sigma_{\mathbf{b_{n_0} b_1^2}}} \\ \mathbf{P}_{\sigma_{\mathbf{b_1^3}}} & \mathbf{P}_{\sigma_{\mathbf{b_2 b_1^3}}} & \dots & \mathbf{P}_{\sigma_{\mathbf{b_{n_0} b_1^3}}} \\ \vdots & \vdots & \vdots & \vdots \\ \mathbf{P}_{\sigma_{\mathbf{b_1^l}}} & \mathbf{P}_{\sigma_{\mathbf{b_2 b_1^l}}} & \dots & \mathbf{P}_{\sigma_{\mathbf{b_{n_0} b_1^l}}} \end{pmatrix} \tag{13}$$

определяет ансамбль регулярных МПП-кодов Галлагера длины $n = n_0 m$, который мы обозначим $\mathcal{E}_M(l, n_0, m)$. Элементы ансамбля получаются путем случайного выбора числа b_1 : $(b_1, m) = 1$, а так же случайного выбора перестановки $\sigma \in \mathcal{S}_m$. Указанный выше способ построения матрицы $\mathbf{H_m}$ гарантирует, что все матрицы в каждой строке и в каждом столбце будут различны (они все будут являться классами смежности).

Описанный выше алгоритм генерации проверочной матрицы можно модифицировать, если вместо одной перестановки $\sigma \in \mathcal{S}_m$, взять $\sigma^{(1)}, \dots \sigma^{(n_0)} \in \mathcal{S}_m$ таких, что $\forall i, j \leq n_0$ если $i \neq j$, то $\{\sigma^{(i)}, (\sigma^{(i)})^2, \dots, (\sigma^{(i)})^{ord\, \sigma_i - 1}\} \cap \{\sigma^{(j)}, (\sigma^{(j)})^2, \dots, (\sigma^{(j)})^{ord\, \sigma_j - 1}\} = \emptyset$.

Тогда матрица

$$\mathbf{H_{m^\star}} = \begin{pmatrix} \mathbf{P}_{\sigma^{(1)}} & \mathbf{P}_{\sigma^{(2)}} & \dots & \mathbf{P}_{\sigma^{(n_0)}} \\ \mathbf{P}_{\sigma^{(1)}_{\mathbf{b_1}}} & \mathbf{P}_{\sigma^{(2)}_{\mathbf{b_2}}} & \dots & \mathbf{P}_{\sigma^{(n_0)}_{\mathbf{b_{n_0}}}} \\ \mathbf{P}_{\sigma^{(1)}_{\mathbf{b_1^2}}} & \mathbf{P}_{\sigma^{(2)}_{\mathbf{b_2^2}}} & & \mathbf{P}_{\sigma^{(n_0)}_{\mathbf{b_{n_0}^2}}} \\ \vdots & \vdots & \vdots & \vdots \\ \mathbf{P}_{\sigma^{(1)}_{\mathbf{b_1^{l-1}}}} & \mathbf{P}_{\sigma^{(2)}_{\mathbf{b_2^{l-1}}}} & \dots & \mathbf{P}_{\sigma^{(n_0)}_{\mathbf{b_{n_0}^{l-1}}}} \end{pmatrix}, \tag{14}$$

где $\forall i \ ord \sigma_j^{(i)} \geq l-1$, определяет ансамбль регулярных МПП-кодов Галлагера длины $n = n_0 m$, который мы обозначим $\mathcal{E}_{M^\star}(l, n_0, m)$. Элементы ансамбля получаются путем случайного и равновероятного выбора без возвращения перестановок $\sigma^{(1)}, \dots \sigma^{(n_0)} \in \mathcal{S}_m$, а так же чисел $b_1, b_2, \dots, b_{n_0}$, $(b_i, m) = 1$.

Очевидно, что $|\mathcal{E}_{M^\star}(l, n_0, m)| > |\mathcal{E}_M(l, n_0, m)|$. Это обусловлено тем, что в построении проверочной матрицы (14) МПП-кода учавствует не одна, как в (13), а набор из n_0 различных перестановок. Как будет показано далее, коды из $\mathcal{E}_{M^\star}(l, n_0, m)$ обладают значительно лучшими корректирующими способностями, нежели коды из $\mathcal{E}_M(l, n_0, m)$.

МПП-коды, основанные степенях перестановок

Пусть $\mathbf{P_1}, \mathbf{P_2}, \ldots, \mathbf{P_{n_0}} \in \mathcal{P}^m$, причем если $G_i = \{\mathbf{P_i}, \mathbf{P_i^2}, \ldots, \mathbf{P_i^{n_i} = E}\}$, $G_j = \{\mathbf{P_j}, \mathbf{P_j^2}, \ldots, \mathbf{P_j^{n_j} = E}\}$, то

1. $(G_i/\mathbf{E}) \cap (G_j/\mathbf{E}) = \emptyset$ при $i \neq j$,
2. $\forall i = \overline{1, n_0}$, $n_i \geq l$.

Тогда матрица

$$\mathbf{H_w} = \begin{pmatrix} \mathbf{P_1} & \mathbf{P_2} & \mathbf{P_3} & \ldots & \mathbf{P_{n_0}} \\ \mathbf{P_1^2} & \mathbf{P_2^2} & \mathbf{P_3^2} & \ldots & \mathbf{P_{n_0}^2} \\ \mathbf{P_1^3} & \mathbf{P_2^3} & \mathbf{P_3^3} & \ldots & \mathbf{P_{n_0}^3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{P_1^l} & \mathbf{P_2^l} & \mathbf{P_3^l} & \ldots & \mathbf{P_{n_0}^l} \end{pmatrix} \tag{15}$$

определяет ансамбль регулярных МПП-кодов Галлагера длины $n = n_0 m$, который мы обозначим $\mathcal{E}_W(l, n_0, m)$. Указанный выше способ построения матрицы $\mathbf{H_w}$ гарантирует, что все матрицы в каждой строке и в каждом столбце будут различны. Элементы ансамбля $\mathcal{E}_W(l, n_0, m)$ получаются путем выбора без возвращений матриц перестановок $\mathbf{P_i} \in \mathcal{P}_m$, $i = 1, 2, \ldots, n_0$, обладающих свойствами (1) и (2).

Замечание. В конструкции матрицы (15) можно увидеть аналогию определителя Вандермонда, однако $\mathbf{H_w}$ не является квадратной матрицей, ее размерность – $lm \times mn_0$.

Модифицирование кодов из ансамбля $\mathcal{E}_S(l, n_0, m)$

Напомним, что ансамбль $\mathcal{E}_S(l, n_0, m)$ задается своей проверочной матрицей

$$\mathbf{H_s} = \begin{pmatrix} \mathbf{P_{11}} & \mathbf{P_{12}} & \mathbf{P_{13}} & \ldots & \mathbf{P_{1n_0}} \\ \mathbf{P_{21}} & \mathbf{P_{22}} & \mathbf{P_{23}} & \ldots & \mathbf{P_{2n_0}} \\ \vdots & \vdots & \vdots & \vdots\ \vdots & \\ \mathbf{P_{l1}} & \mathbf{P_{l2}} & \mathbf{P_{l3}} & \ldots & \mathbf{P_{ln_0}} \end{pmatrix},$$

где $\mathbf{P_{ij}} \in \mathcal{P}_s^m$.

Предположим, что $\mathbf{P_{1j}} \in \mathcal{P}^m/\mathcal{P}_s^m$, $j = \overline{1, n_0}$. Каждой матрице $\mathbf{P_{1j}}$ соответствует перестановка $\sigma_j \in \mathcal{S}_m$, причем $\forall h \in \mathbb{N}$ σ_j не является перестановкой h-кратного циклического сдвига.

Пусть $h_1, \ldots, h_{l-1} \in \mathbb{N}$, причем $h_i = h_j$ тогда и только тогда, когда $i = j$. Тогда построим перестановки h_1-кратного, h_2-кратного,..., h_{l-1}-кратного циклических сдвигов $\lambda_{h_1}, \lambda_{h_2}, \ldots, \lambda_{h_{l-1}}$.

Для каждой σ_j вычислим $\tau_{jh_1} = \sigma_j \cdot \lambda_{h_1}$, $\tau_{jh_2} = \sigma_j \cdot \lambda_{h_2}, \ldots, \tau_{jh_{l-1}} = \sigma_j \cdot \lambda_{h_{l-1}}$.

Так как все h_i и σ_j различны, то и все τ_{jh_i} будут так же различны, тогда матрица

$$\mathbf{H_{s^\star}} = \begin{pmatrix} \mathbf{P}_{\tau_{\mathbf{1h_1}}} & \mathbf{P}_{\tau_{\mathbf{2h_1}}} & \mathbf{P}_{\tau_{\mathbf{3h_1}}} & \ldots & \mathbf{P}_{\tau_{\mathbf{n_0h_1}}} \\ \mathbf{P}_{\tau_{\mathbf{1h_2}}} & \mathbf{P}_{\tau_{\mathbf{2h_2}}} & \mathbf{P}_{\tau_{\mathbf{3h_2}}} & \ldots & \mathbf{P}_{\tau_{\mathbf{n_0h_2}}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{P}_{\tau_{\mathbf{1h_{l-1}}}} & \mathbf{P}_{\tau_{\mathbf{2h_{l-1}}}} & \mathbf{P}_{\tau_{\mathbf{3h_{l-1}}}} & \ldots & \mathbf{P}_{\tau_{\mathbf{n_0h_{l-1}}}} \end{pmatrix} \tag{16}$$

определяет ансамбль регулярных МПП-кодов Галлагера длины $n = n_0 m$, который мы обозначим $\mathcal{E}_{S^\star}(l, n_0, m)$. Элементы ансамбля $\mathcal{E}_{S^\star}(l, n_0, m)$ получаются путем выбора без возвращений матриц перестановок $\mathbf{P_{1j}} \in \mathcal{P}_m / \mathcal{P}_s^m$, $j = 1, 2, \ldots, n_0$, а так же чисел $h_1, \ldots, h_{l-1} \in \mathbb{N}$.

3. РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

Для генерации проверочных матриц МПП -кодов были написаны программы на языке Borland Delphi, а так же 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 (АГБШ). В качестве алгоритма декодирования был выбран итеративный алгоритм Sum-Product с “мягким” входом, работающий с представлением кода в виде двудольного графа Таннера [9]. Максимальное число итераций составило 50. Подробнее с методами декодирования можно ознакомиться в работах [10]–[11].

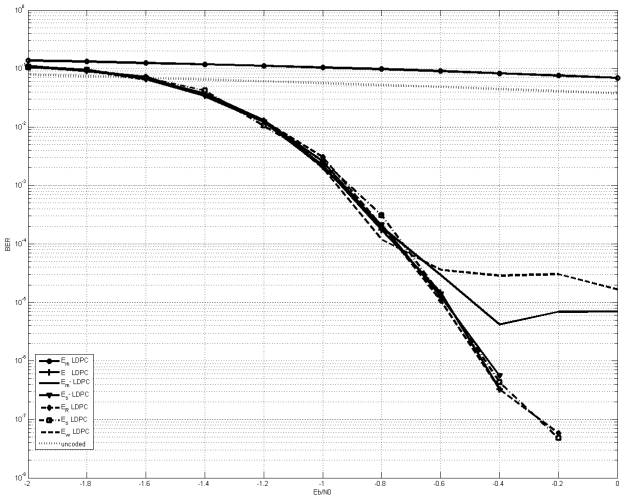

Рис. 1. Зависимость вероятности битовой ошибки от отношения сигнал-шум для кодов $n = 2592$, $l = 4$, $n_0 = 8$, $R = 0.5$, взятых из различных ансамблей.

Как следует из рис. 1, коды из ансамблей $\mathcal{E}_{M^\star}(l, n_0, m)$ и $\mathcal{E}_W(l, n_0, m)$ при одинаковых параметрах имеют похожее поведение, выходя на полку при вероятностях битовой ошибки $P_{e_1} = 10^{-4.5}$ и $P_{e_2} = 10^{-5.5}$ соответственно. Лучшим оказывается поведение кодов из ансамблей $\mathcal{E}_S(l, n_0, m)$, $\mathcal{E}_{S^\star}(l, n_0, m)$, $\mathcal{E}_R(l, n_0, m)$ и $\mathcal{E}(l, n_0, m)$, которые показывают схожие корректирующие способности. Так же видно, что код из ансамбля $\mathcal{E}_M(l, n_0, m)$ оказывается неприменимым для практических приложений. Аналогичная ситуация наблюдается и для зависимости вероятности ошибки на блок (кодовое слово) от отношения сигнал-шум:

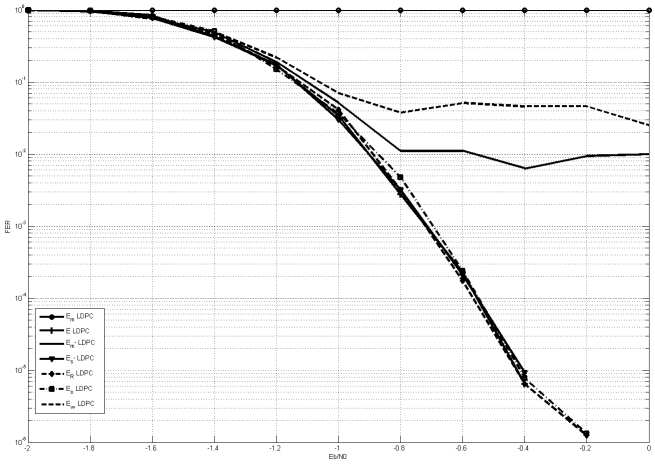

Рис. 2. Зависимость вероятности вероятности ошибки на блок от отношения сигнал-шум для кодов $n = 2592$, $l = 4$, $n_0 = 8$, $R = 0.5$, взятых из различных ансамблей.

Все дальнейшие сравнительные характеристики будут приведены только для этих кодов из ансамблей $\mathcal{E}_S(l, n_0, m)$ и $\mathcal{E}_{S^\star}(l, n_0, m)$.

3.1. Результаты моделирования кодов из ансамбля $\mathcal{E}_S(l, n_0, m)$

Рассмотрим ансамбль $\mathcal{E}_S(l, n_0, m)$ двоичных МПП-кодов. Фиксируем $n = n_0 m = 2592$, $R = \dfrac{1}{2}$. Построим коды, проверочные матрицы $\mathbf{H_s}$ которых содержат $l = 3, 4, 5, 6$ слоев. Для каждого из таких кодов построим кривую зависимости между вероятностью ошибки на бит и отношением сигнал-шум.

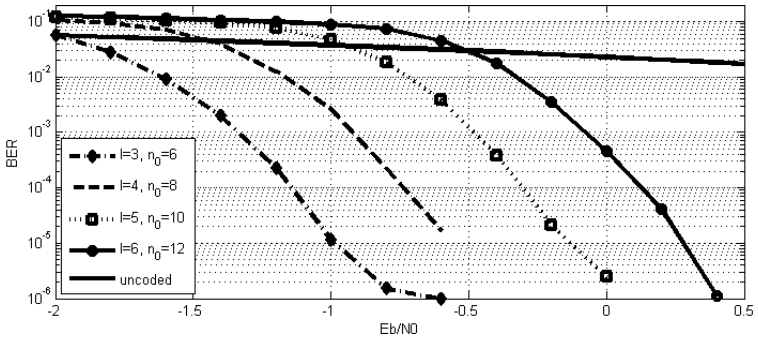

Рис. 3. Зависимость вероятности вероятности ошибки на бит от отношения сигнал-шум для кодов $n = 2592$, $R = 0.5$, при разном числе слоев l.

Рис. 3 показывает, что лучшими характеристиками обладают коды, имеющие $l = 3$ слоя. Увеличение числа слоев на единицу приводит к проигрышу порядка 0.5 Дб. На рис.4 продемонстрирована зависимость между вероятностью ошибки на блок от отношения сигнал-шум для кодов $N = 2592$, $R = 0.5$, при разном числе слоев l.

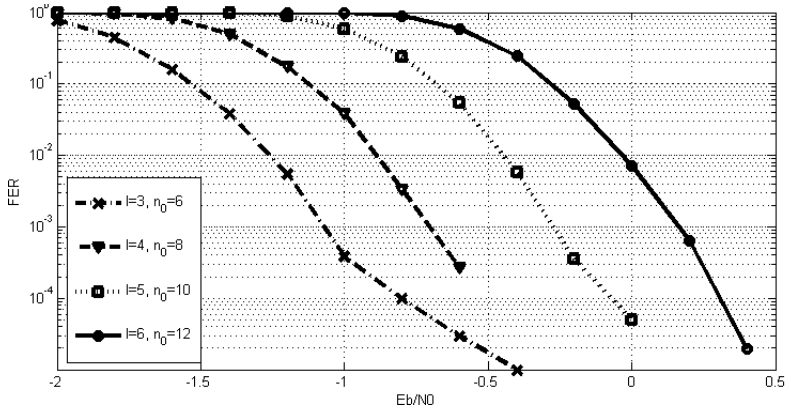

Рис. 4. Зависимость вероятности вероятности ошибки на блок от отношения сигнал-шум для кодов $n = 2592$, $R = 0.5$, при разном числе слоев l.

Теперь в ансамбле $\mathcal{E}_S(l, n_0, m)$ фиксируем $l = 3$, $n_0 = 6$, $R = \dfrac{1}{2}$ и рассмотрим коды длин $n = 648, 1296, 2592, 5184$. Длина кода варьируется за счет изменения m. Для каждого из 4 полученных кодов построим графики зависимости вероятности ошибки на бит и на блок от отношения сигнал-шум.

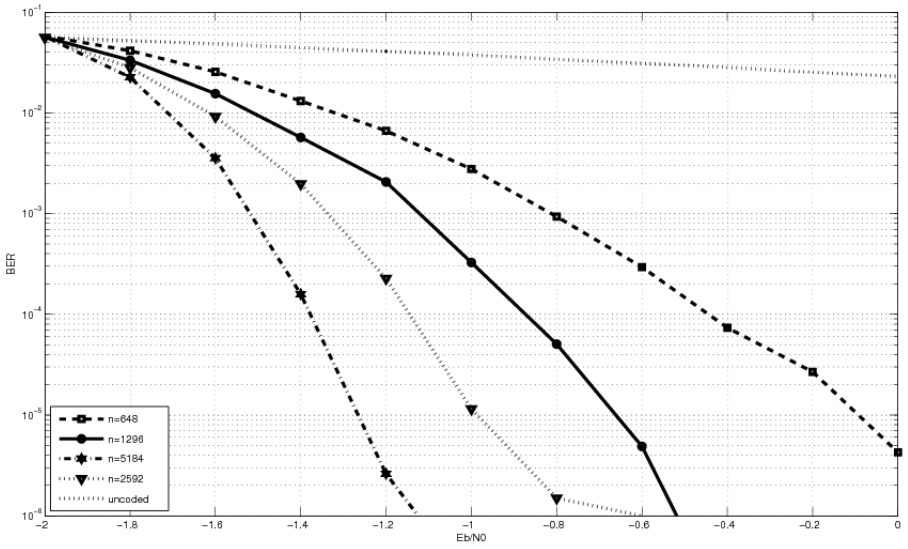

Рис. 5. Зависимость вероятности ошибки на бит от отношения сигнал-шум для кодов разных длин.

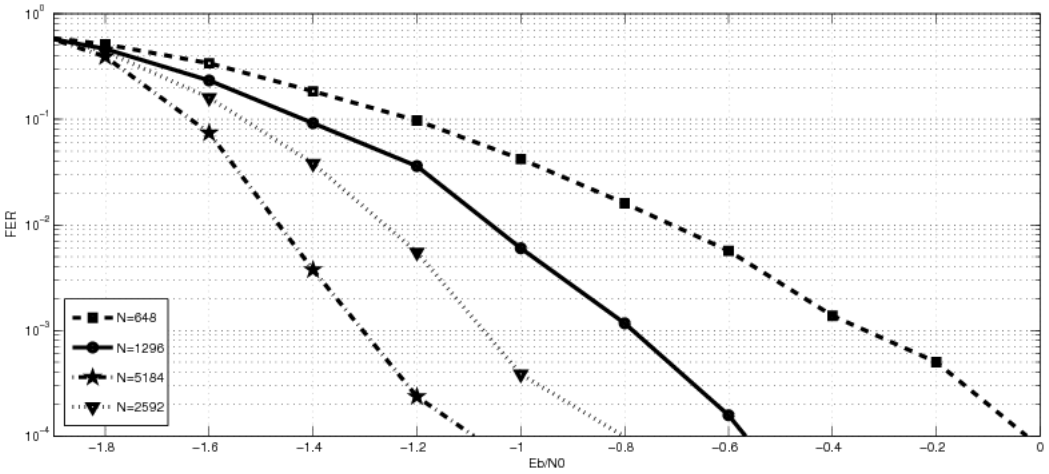

Рис. 6. Зависимость вероятности ошибки на блок от отношения сигнал-шум для кодов разных длин.

Рис. 5 и 6 показывают, что лучшими корректирующими способностями обладают коды с большей длиной. Выигрыш от перехода с кода длины 648 к коду длины 1296 составил около 0.6 Дб (по уровню вероятности битовой ошибки 10^{-5}). Однако в то же время переход от кода длины 1296 к коду длины 2592 по аналогичному уровню вероятности ошибки уже дал выигрыш порядка 0.3 Дб. Та же ситуация наблюдается при переходе от кода длины 2592 к коду длины 5184: выигрыш вновь составил порядка 0.3 Дб.

Покажем, как изменяется корректирующая способность кода из ансамбля $\mathcal{E}_S(l, n_0, m)$ при изменении его скорости. Напомним, что скорость кода R оценивается по формуле:

$$R \geq 1 - \frac{l}{n_0}.$$

Выберем в ансамбле $\mathcal{E}_S(l, n_0, m)$ 5 кодов, обладающих следующими характеристиками:

Таблица 4.

n_0	l	R	n
4	3	0.25	2592
5	3	0.4	2590
6	3	0.5	2592
10	4	0.6	2590
12	3	0.75	2592

Для каждого кода, указанного в таблице 4, построим графики зависимости вероятности ошибки на бит и на блок от отношения сигнал-шум.

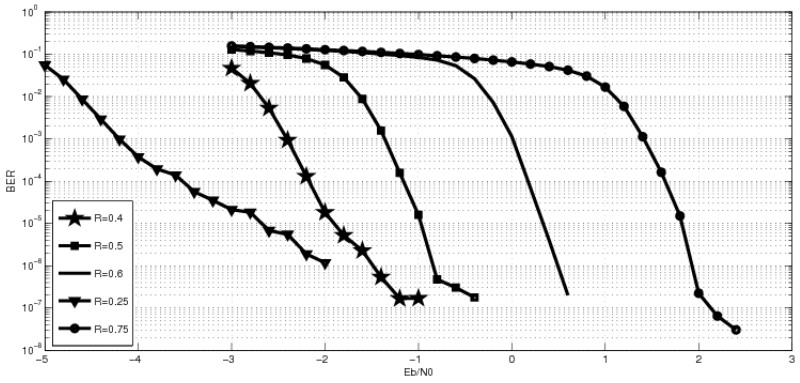

Рис. 7. Зависимость вероятности ошибки на бит от отношения сигнал-шум для кодов с разными скоростями.

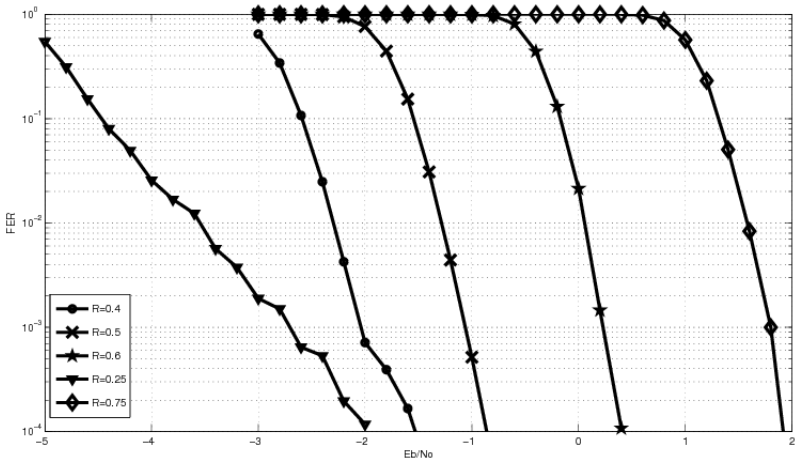

Рис. 8. Зависимость вероятности ошибки на блок от отношения сигнал-шум для кодов с разными скоростями.

Рис. 7 и 8 показывают, что код с $R = 0.25$ обладает "плохими" корректирующими способностями: при увеличении отношения сигнал-шум уменьшение вероятности ошибки на бит и на блок крайне незначительно в сравнении с остальными кодами.

3.2. Результаты моделирования кодов из ансамбля $\mathcal{E}_{S^\star}(l, n_0, m)$

В данном разделе мы приведем результаты моделирования кодов из ансамбля $\mathcal{E}_{S^\star}(l, n_0, m)$. Отметим, что их поведение во многом напоминает поведение кодов из уже рассмотренного нами ансамбля $\mathcal{E}_S(l, n_0, m)$.

Вначале рассмотрим зависимость кодов от числа слоев l при фиксированной скорости $R = \dfrac{1}{2}$ и длине $n = 2592$. Рис. 9 и 10 иллюстрируют зависимость вероятности ошибки на бит и на блок соответственно от отношения сигнал-шум.

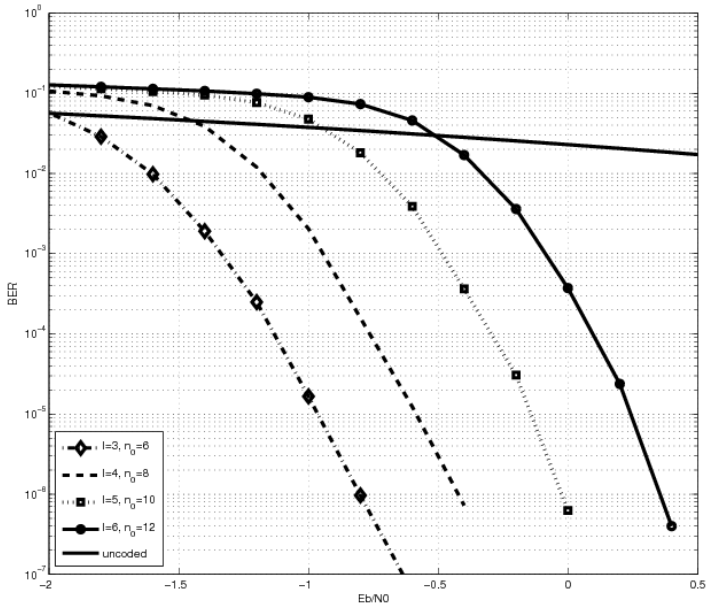

Рис. 9. Зависимость вероятности вероятности ошибки на бит от отношения сигнал-шум для кодов $n = 2592$, $R = 0.5$, при разном числе слоев l.

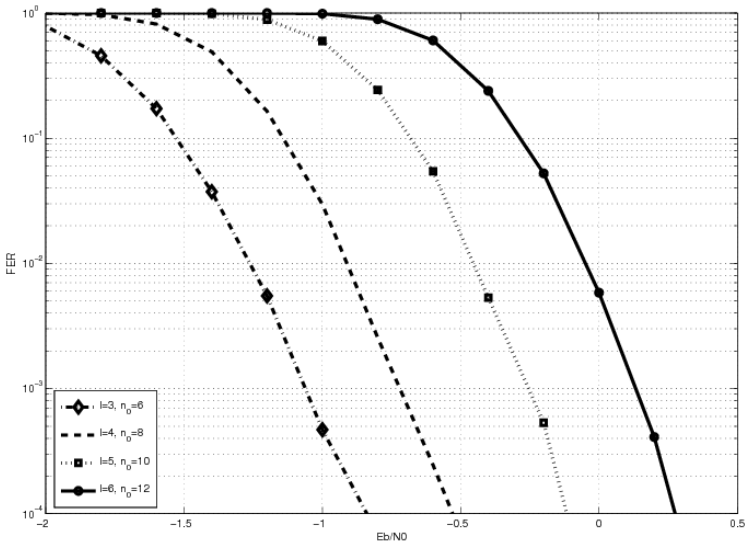

Рис. 10. Зависимость вероятности вероятности ошибки на блок от отношения сигнал-шум для кодов $n = 2592$, $R = 0.5$, при разном числе слоев l.

Как и в случае ансамбля $\mathcal{E}_S(l, n_0, m)$ лучшими корректирующими свойствами обладают трехслойные коды, увеличение числа слоев на 1 приводит к проигрышу в среднем около 0.4 Дб.

Теперь в ансамбле $\mathcal{E}_{S^\star}(l, n_0, m)$ фиксируем $l = 3$, $n_0 = 6$, $R = \dfrac{1}{2}$ и рассмотрим коды длин $n = 648, 1296, 2592, 5184$. Для каждого из кодов построим графики зависимости вероятности ошибки на бит и на блок от отношения сигнал-шум.

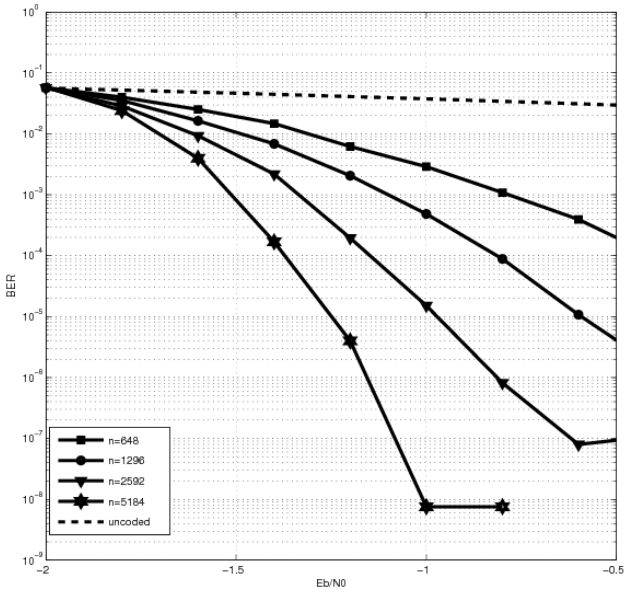

Рис. 11. Зависимость вероятности ошибки на бит от отношения сигнал-шум для кодов разных длин.

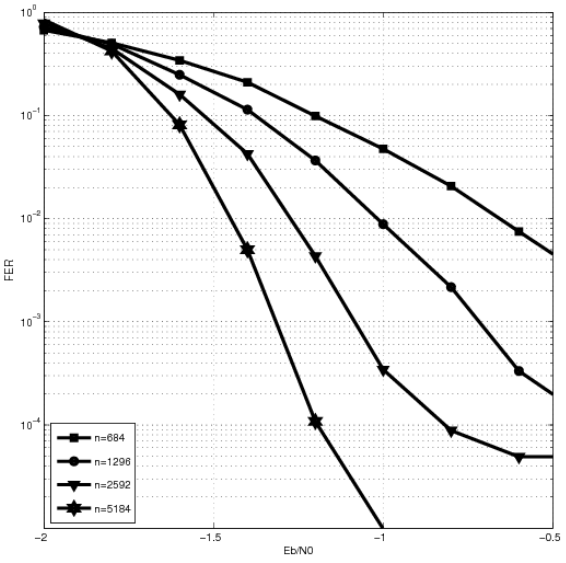

Рис. 12. Зависимость вероятности ошибки на блок от отношения сигнал-шум для кодов разных длин.

В ансамбле $\mathcal{E}_{S^\star}(l, n_0, m)$ построим коды, параметры которых приведены в таблице 4. Для каждого из них построим зависимость вероятности ошибки на бит и на блок от отношения сигнал-шум (рис. 13 и 14).

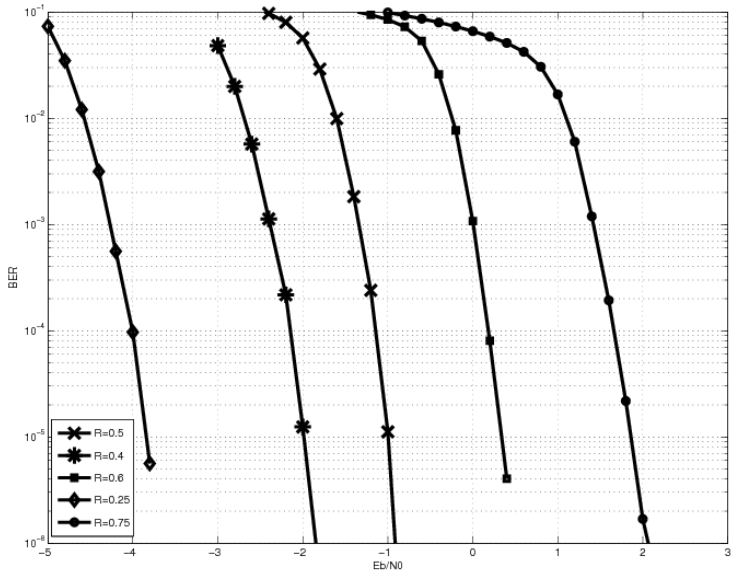

Рис. 13. Зависимость вероятности ошибки на бит от отношения сигнал-шум для кодов с разными скоростями.

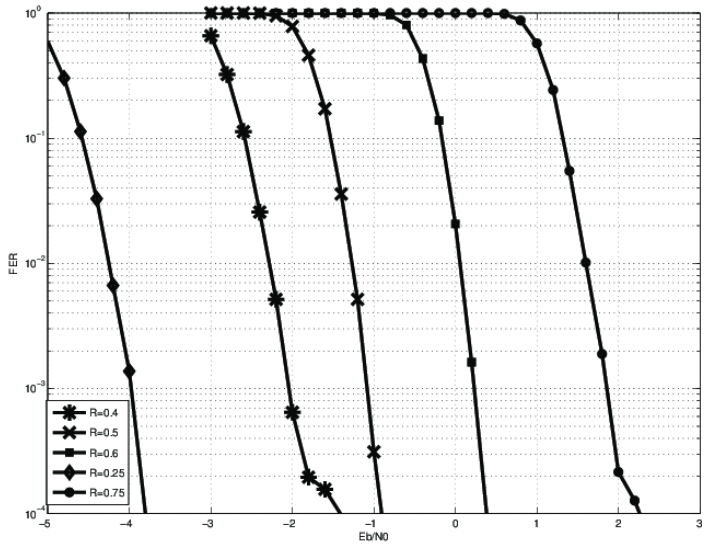

Рис. 14. Зависимость вероятности ошибки на блок от отношения сигнал-шум для кодов с разными скоростями.

4. ЗАКЛЮЧЕНИЕ

Результаты моделирования показывают, что конструкции, основанные на случайных матрицах перестановок, случайных сдвигах единичной матрицы, случайных сдвигах строки из n_0 различных матриц, имеют корректирующие способности, не уступающие корректирующим способностям кодов из ансамбля Галлагера. В то же время, регулярные конструкции провероч-

ных матриц МПП-кодов, основанных на перестановках-умножениях и степенях перестановок, имеют существенно худшие характеристики. Так же установлено, что декодер $Sum - Product$ показывает наилучшие результаты декодирования, когда число слоев l проверочной матрицы $\mathbf{H}$ равно 3.

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. 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.
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. Okamura T. Designing LDPC codes using cyclic shifts. *Proc. IEEE Int. Symp. Information Theory.* Yokohama, 2003, p. 151.
6. 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.
7. 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.
8. Ling Alan C. H. Difference Triangle Sets From Affine Planes. *IEEE Trans. Inform. Theory*, 2002, vol. 48, no. 8, pp. 2399–2401.
9. Tanner M. A Recursive Approach to Low Complexity Codes. *IEEE Trans. Inform. Theory*, 1981, vol. 27, no. 5, pp. 533–547.
10. 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.
11. 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.