*Информационные процессы, Том 12, № 4, 2001, стр. 372–388.*


**ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ ИНФОРМАЦИИ**

# Оценка активных расстояний сверточных кодов (частично)единичной памяти с малой плотностью проверок

**В.В.Зяблов {zyablov@iitp.ru},**
**К.А.Кондрашов {k_kondrashov@iitp.ru},**
**О.Д.Скопинцев {skopintsev@iitp.ru}**

*Институт проблем передачи информации им. А.А. Харкевича, Российская академия наук, Москва, Россия*

Поступила в редколлегию 15.11.2012

**Аннотация**—Построение сверточных кодов с (частично) единичной памятью из блочных кодов позволяет получать сверточные коды с высокими корректирующими свойствами. В данной работе вводится ансамбль двоичных сверточных кодов (частично)единичной памяти, полученных из блочных кодов с малой плотностью проверок. Рассматриваемый ансамбль задается полубесконечными проверочными матрицами, обладающими (частично) единичной памятью. Для кодов заданного ансамбля выводятся асимптотические оценки свободного расстояния и активных строчных расстояний, доказывается, что коды по ансамблю имеют положительный уклон активных строчных расстояний.

**КЛЮЧЕВЫЕ СЛОВА:** Коды с (частично) единичной памятью, сверточные коды, коды с малой плотностью проверок, свободное расстояние, активные строчные расстояния, уклон.

## 1. ВВЕДЕНИЕ

Вынесенные Ли в 1976 году в отдельный класс [1] коды с единичной памятью (ЕП) и параметрами $(n, k)$, где $n$ – длина кодового блока, а $k$ – размерность, являются сверточными $(n, k, m, \nu)$–кодами с памятью $m = 1$ и длиной кодового ограничения $\nu = k$. Каждый последующий кодовый блок такого сверточного кода зависит от текущего информационного блока и одного предыдущего. Длина кодового ограничения $\nu$ определяет количество символов сохраненного блока, участвующих в этой зависимости. Идея кодов с единичной памятью получила дальнейшее развитие в работах Лаэра. В работе [2] он представил $(n, k, \nu)$ - коды с *частично единичной памятью* (ЧЕП). Как и коды с полной единичной памятью, они являются сверточными кодами с памятью $m = 1$, однако длина их кодового ограничения меньше максимальной: $\nu < k$.

Простые верхние границы свободного расстояния (Ч)ЕП–кодов были получены Ли [1] и Лаэром [2] на основе общей границы сверточных кодов. Позже было установлено различие в корректирующих свойствах ЕП–кодов и сверточных кодов с большей памятью. В своей работе [3], К. Томмесен и Й. Юстесен показали, что ЕП–коды могут обладать свойствами, превосходящими свойства сверточных кодов с произвольной памятью при сравнимых параметрах.

Обладая относительно простой структурой, при которой выходной блок кодовой последовательности зависит лишь от текущего и предшествующего ему информационных блоков, (Ч)ЕП-коды предлагают богатые возможности для их исследования. Аналитические методы, разработанные для изучения блоковых кодов, могут быть применены и к (Ч)ЕП-кодам, которые имеют в своей основе те же блоковые коды [4], [6, 5].

В данной работе рассматривается ансамбль (Ч)ЕП–кодов, построенных на основе блоковых кодов с малой плотность проверок (МПП). Свойства МПП-кодов чаще всего исследуются через их разреженные проверочные матрицы. Аналогично, свойства рассматриваемых (Ч)ЕП-МПП-кодов исследуются на основе их проверочных матриц. В данной работе ансамбль строится из полубесконечных проверочных матриц, обладающих, (частично) единичной памятью. Для заданного ансамбля кодов выводятся нижние оценки активных строчных расстояний, свободного расстояния и уклона.

Данная работа имеет следующую структуру: в разделе 2 приводятся базовые определения, объясняется связь между порождающей и проверочной матрицами; в разделе 3 исследуется структура кодовых последовательностей; в разделе 4 дается оценка кодовых расстояний; в разделе 5 идет заключение.

## 2. БАЗОВЫЕ ОПРЕДЕЛЕНИЯ

Всякий линейный код может быть задан как порождающей, так и проверочной матрицей. Для построения ансамбля (Ч)ЕП-МПП–кодов используем проверочные матрицы блочных МПП–кодов Галлагера.

Коды с малой плотностью проверок, описываемые разреженными проверочными матрицами, были впервые предложены Галлагером [7]. Проверочная матрица $\mathbf{H}_{LDPC}$ кода Галлагера состоит из так называемых “слоев” следующего вида:

$$\mathbf{H}^* = \begin{pmatrix} \mathbf{H}_0 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0 \end{pmatrix}_{b \times bn_0},$$

где $\mathbf{H}_0$ – проверка на четность длины $n_0$:

$$\mathbf{H}_0 = \underbrace{(1\ 1\ \dots\ 1)}_{n_0}.$$

Пусть $\pi(\mathbf{H}^*)$ обозначает матрицу, полученную из матрицы $\mathbf{H}^*$ случайной перестановкой столбцов. Тогда проверочная матрица МПП-кода Галлагера с $\ell$ слоями имеет вид:

$$\mathbf{H}_{LDPC} = \begin{pmatrix} \pi_1(\mathbf{H}^*) \\ \pi_2(\mathbf{H}^*) \\ \vdots \\ \pi_l(\mathbf{H}^*) \end{pmatrix}_{\ell b \times bn_0}. \qquad (1)$$

Все возможные независимые равновероятные перестановки столбцов в разных слоях $\pi_1, \dots \pi_\ell$ порождают ансамбль $\mathcal{E}(n_0, \ell, b)$ МПП-кодов Галлагера со скоростью $R \geq 1 - \ell/n_0$ и длиной $n = bn_0$.

Определим ансамбль $(n, k, \nu)$ сверточных кодов с (частично) единичной памятью, полученных из блочных кодов с малой плотностью проверок, с помощью полубесконечных провероч-

ных матриц следующего вида:

$$\begin{bmatrix} \mathbf{H}_p(0) & & & \\ \mathbf{H}_c(0) & & & \\ \mathbf{H}_f(1) & \mathbf{H}_p(1) & & \\ & \mathbf{H}_c(1) & & \\ & \mathbf{H}_f(2) & \mathbf{H}_p(2) & \\ & & \mathbf{H}_c(2) & \ddots \\ & & \mathbf{H}_f(3) & \ddots \\ & & & \ddots \end{bmatrix}, \tag{2}$$

где подматрицы $\mathbf{H}_p(t)$, $\mathbf{H}_f(t)$ имеют размер $\nu \times n$ и выбираются независимо из ансамбля $\mathcal{E}\,(n_0, \nu/b, b)$ блочных МПП–кодов Галлагера, а подматрицы $\mathbf{H}_c(t)$ имеют размер $(n-k-\nu)\times n$ и выбираются независимо из ансамбля $\mathcal{E}\,(n_0, (n-k-\nu)/b, b)$ блочных МПП–кодов Галлагера. Значение $\nu$ ограничено следующими условиями: $\nu \le k$, $\nu + k \le n$.

По построению МПП–кодов Галлагера, их проверочные матрицы могут иметь неполный ранг. Будем считать, что $\mathrm{rk}\ \mathbf{H}_p(t) = \mathrm{rk}\ \mathbf{H}_f(t) = \nu' \le \nu$, а $\mathrm{rk}\ \mathbf{H}_c(t) = n - k' - \nu' \le n - k - \nu$. Отметим, что при $b \to \infty$ с вероятностью $p \to 1$ ранги $\mathrm{rk}\ \mathbf{H}_p(t)$, $\mathrm{rk}\ \mathbf{H}_f(t) \to \nu$ и $\mathrm{rk}\ \mathbf{H}_c(t) \to n - k - \nu$.

**Определение 1.** Ансамбль $\mathcal{E}_{punc}(n, k, \nu)$ (Ч)ЕП-МПП–кодов, $\nu \le k$, $\nu + k \le n$, состоит из проверочных матриц вида (2), полученных независимым случайным равновероятным выбором подматриц $\mathbf{H}_p(t)$, $\mathbf{H}_c(t)$, $\mathbf{H}_f(t)$ из соответствующих ансамблей блочных МПП-кодов Галлагера.

Можно показать, что проверочной матрице вида (2) соответствует порождающая матрица вида

$$\begin{bmatrix} \mathbf{G}_c(0) & & & \\ \mathbf{G}_f(0) & \mathbf{G}_p(1) & & \\ & \mathbf{G}_c(1) & & \\ & \mathbf{G}_f(1) & \mathbf{G}_p(2) & \\ & & \mathbf{G}_c(2) & \\ & & \mathbf{G}_f(2) & \mathbf{G}_p(3) \\ & & & \ddots \end{bmatrix}, \tag{3}$$

где подматрицы $\mathbf{G}_c(t)$ и $\mathbf{G}_f(t)$, $\mathbf{G}_p(t)$ — матрицы полного ранга размеров $(k' - \nu') \times n$ и $\nu' \times n$, соответственно.

Связь между информационной и кодовой последовательностями $\mathbf{u}$, $\mathbf{v}$ , где информационная последовательность $\mathbf{u}$ состоит из блоков $\mathbf{u}_i \in \mathbb{F}_2^{k'}$, а кодовая последовательность $\mathbf{v}$ из блоков $\mathbf{v}_i \in \mathbb{F}_2^n$, $i \in \mathbb{N}$:

$$\begin{aligned} \mathbf{u} &= \ldots \mathbf{u}_{i-1}\ \mathbf{u}_i\ \mathbf{u}_{i+1} \ldots \\ \mathbf{v} &= \ldots \mathbf{v}_{i-1}\ \mathbf{v}_i\ \mathbf{v}_{i+1} \ldots \end{aligned},$$

можно выразить как

$$\mathbf{v}_t = \mathbf{u}_t \begin{pmatrix} \mathbf{G}_c(t) \\ \mathbf{G}_f(t) \end{pmatrix} + \mathbf{u}_{t-1}\mathbf{G}_p(t).$$

Корректирующие свойства сверточного кода во многом опеределяются такими характеристиками, как *свободное расстояние*, *активные строчные расстояния* и *уклон* (средний линейный рост) *активных строчных расстояний*. Приведем их определения.

**Определение 2** (Свободное расстояние). Свободное расстояние $d_{free}$ линейного сверточного кода $\mathcal{C}$ – это минимальное Хэммингово расстояние между любыми двумя различными кодовыми последовательностями:

$$d_{free} = \min_{\mathbf{v},\mathbf{v}'\in\mathcal{C},\ \mathbf{v}\neq\mathbf{v}'} \operatorname{dist}\left(\mathrm{v},\mathrm{v}'\right).$$

Для линейного кода $\mathcal{C}$ выполняется $\min\limits_{\mathbf{v},\mathbf{v}'\in\mathcal{C},\ \mathbf{v}\neq\mathbf{v}'} \operatorname{dist}(\mathrm{v},\mathrm{v}') = \min\limits_{\mathbf{v}''\in\mathcal{C},\ \mathbf{v}''\neq\mathbf{0}} \operatorname{wt}(\mathbf{v}'')$, где функция $\operatorname{wt}(\cdot)$ – Хэммингов вес.

В каждый момент времени содержимое памяти определяет состояние кодера сверточного кода. Для кодов с (частично) единичной памятью кодер может быть переведен в нулевое состояние из любого состояния подачей одного нулевого информационного блока. При этом вес кодовой последовательности не увеличится. При частичной памяти ЧЕП-МПП–кода возможны переходы в нулевое состояние и по ненулевому информационному блоку. В разделе 3 будет показано, что в таком случае вес кодовой последовательности увеличивается. Обозначим с помощью $I_{t,j}$ множество всех информационных последовательностей $\mathbf{u}$ вида

$$\ldots \mathbf{0}\ \mathbf{0}\ \mathbf{u}_t\ \mathbf{u}_{t+1}\ \ldots\ \mathbf{u}_{t+j-1}\ \mathbf{0}\ \mathbf{0}\ldots,$$

где $\mathbf{u}_i \neq \mathbf{0}$ при $t \leq i < t+j$.

**Определение 3** (Активное строчное расстояние). Активным строчным расстоянием $\hat{d}_j^r$ (Ч)ЕП-МПП–кода называется минимальный вес кодовой последовательности, выходящей из нулевого состояния, не проходящей через нулевое состояние по нулевому входу и возвращающейся в нулевое состояние после $j$ информационных блоков.

$$\hat{d}_j^r = \min_t \min_{\mathbf{u}\in I_{t,j}} \left\{\omega_H\left(\mathbf{uG}\right)\right\}.$$

Из определений 2, 3 следует,

$$d_{free} = \min_{j=1,2,\ldots} \{\hat{d}_j^r\}.$$

**Определение 4** (Уклон). Средний линейный рост активного строчного расстояния (уклон) определяется как предел

$$\alpha = \lim_{j\to\infty} \frac{\hat{d}_j^r}{j}.$$

## 3. СТРУКТУРА КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В данном разделе будет показано что кодовые последовательности с весом, равным активному расстоянию на некоторой длине $j$, могут быть получены только при кодировании информационных последовательностей определенного вида. Будет установлено, что если внутри информационной последовательности отсутствуют нулевые блоки, то внутри соответствующей кодовой последовательности (Ч)ЕП-кода все блоки ненулевые. Это потребуется в дальнейшем для получения асимптотических границ. Будут получены аналитические оценки на активные строчные расстояния, свободное расстояние и уклон.

Анализ активных строчных расстояний (Ч)ЕП МПП-кодов, в результате которого была получена аналитическая оценка свободного расстояния, был проведен в работе [8]. Мы повторим его, так как он является ключевым для дальнейшего получения оценок. Анализ проведем для кодов с частичной единичной памятью. За исключением некоторых деталей, он так же верен и для кодов с полной единичной памятью.

Рассмотрим все кодовые последовательности, порожденные информационными последовательностями различной длины $j$, начинающимися и заканчивающимися нулевой серией и не содержащими нулевых блоков внутри: $\mathbf{u} \in I_{t,j}$.

Разобьем информационные блоки на две части из $k' - \nu'$ и $\nu'$ двоичных символов, где $k' - \nu'$ – размерность матриц $\mathbf{G}_c(t)$, а $\nu'$ – размерность матриц $\mathbf{G}_p(t)$, $\mathbf{G}_f(t)$ соответственно: $\mathbf{u}_t = (\mathbf{u}_{t,0}\ \mathbf{u}_{t,1})$. В соответствии с кодирующим правилом,

$$\mathbf{v} = \begin{bmatrix} \vdots \\ \mathbf{u}_{t,0}^{\mathrm{T}} \\ \mathbf{u}_{t,1}^{\mathrm{T}} \\ \mathbf{u}_{t+1,0}^{\mathrm{T}} \\ \mathbf{u}_{t+1,1}^{\mathrm{T}} \\ \vdots \end{bmatrix}^{\mathrm{T}} \cdot \begin{pmatrix} & & & & \\ & \ddots & & & \\ \mathbf{G}_c(t) & \mathbf{0} & & & \\ \mathbf{G}_f(t) & \mathbf{G}_p(t+1) & & & \\ & \mathbf{G}_c(t+1) & \mathbf{0} & & \\ & \mathbf{G}_f(t+1) & \mathbf{G}_p(t+2) & & \\ & & \mathbf{G}_c(t+2) & & \\ & & \mathbf{G}_f(t+2) & & \\ & & & \ddots & \end{pmatrix}. \tag{4}$$

Из (4) видно, что каждый кодовый блок в кодовой последовательности принадлежит одному из множеств (здесь и далее, где это не играет роли, опустим временные индексы):

$$C_0 = \{\mathbf{x}\mathbf{G}_0\}_{\mathbf{x}\in\mathbb{F}_2^{k'}},\ C_c = \{\mathbf{x}\mathbf{G}_c\}_{\mathbf{x}\in\mathbb{F}_2^{k'-\nu'}},\ C_f = \{\mathbf{x}\mathbf{G}_f\}_{\mathbf{x}\in\mathbb{F}_2^{\nu'}},\ C_p = \{\mathbf{x}\mathbf{G}_p\}_{\mathbf{x}\in\mathbb{F}_2^{\nu'}},$$

$$C_{pc} = \left\{\mathbf{x}\begin{pmatrix}\mathbf{G}_p\\ \mathbf{G}_c\end{pmatrix}\right\}_{\mathbf{x}\in\mathbb{F}_2^{k'}},\ C_{pf} = \left\{\mathbf{x}\begin{pmatrix}\mathbf{G}_p\\ \mathbf{G}_f\end{pmatrix}\right\}_{\mathbf{x}\in\mathbb{F}_2^{2\nu'}},\ C_{pcf} = \left\{\mathbf{x}\begin{pmatrix}\mathbf{G}_p\\ \mathbf{G}_c\\ \mathbf{G}_f\end{pmatrix}\right\}_{\mathbf{x}\in\mathbb{F}_2^{k'+\nu'}}. \tag{5}$$

По построению (Ч)ЕП-МПП–кодов, множества слов $\mathcal{C}_0$, $\mathcal{C}_c$, $\mathcal{C}_f$, $\mathcal{C}_p$, $\mathcal{C}_{pc}$ являются кодами. Множества $\mathcal{C}_{pf}$ и $\mathcal{C}_{pcf}$ будут являться кодами только в том случае, если матрицы $\begin{pmatrix}\mathbf{G}_p\\ \mathbf{G}_f\end{pmatrix}$ и $\begin{pmatrix}\mathbf{G}_p\\ \mathbf{G}_c\\ \mathbf{G}_f\end{pmatrix}$ имеют полный ранг, а для $\mathcal{C}_{pcf}$ дополнительно требуется выполнение условия $\nu' + k' \le n$. Для выбранных блочных МПП-кодов при построении проверочной матрицы (2) при $b \to \infty$ с вероятностью $p \to 1$ порождающие матрицы $\mathcal{C}_{pf}$ и $\mathcal{C}_{pcf}$ будут иметь полный ранг, а при условии $\nu + k \le n$ так же выполняется и $\nu' + k' \le n$. Таким образом, большинство кодов из ансамбля удовлетворяют этим требованиям и для них множества (5) являются кодами. Дальнейший анализ и все полученные результаты верны только для таких, типичных, кодов из ансамбля.

**Лемма 1.** *В ансамбле $\mathcal{E}_{рит}$ $(n, k, \nu)$ (Ч)ЕП МПП-кодов, $k+\nu < n$, кодовые слова, порожденные информационными последовательностями $\mathbf{u} \in I_{t,n}$ без нулевых блоков внутри имеют $n$ или $n+1$ ненулевых кодовых блоков.*

**Лемма 2.** *Кодовая последовательность (Ч)ЕПП МПП-кода из ансамбля $\mathcal{E}_{рит}$ $(n, k, \nu)$, полученная при кодировании информационной последовательности*
$\ldots \mathbf{0}\ \mathbf{0}\ \mathbf{u}_t\ \mathbf{u}_{t+1}\ \ldots\ \mathbf{u}_{t+j-1}\ \mathbf{0}\ \mathbf{0} \ldots$ *из $I_{t,j}$, где $\mathbf{u}_i = (\mathbf{u}_{i,0}\ \mathbf{u}_{i,1})$, может иметь вес, равный активному расстоянию $\hat{d}_j^r$, только в том случае, если*

$$\mathbf{u}_{i,0} \ne \mathbf{0},\ \mathbf{u}_{i,1} \ne \mathbf{0} \text{ при } t \le i < j-1,$$
$$\mathbf{u}_{j-1,0} \ne \mathbf{0}.$$

**Лемма 3.** *Активные расстояния кодов из ансамбля* $\mathcal{E}_{pur}\,(n,k,\nu)$ *(Ч)ЕП МПП-кодов,* $k+\nu < n$, $\nu \le k$ *удовлетворяют следующим условиям:*

$$\begin{aligned}
\hat{d}_1^r &\ge \min\left(d\left(C_c\right), d\left(C_0\right) + d\left(C_p\right)\right),\\
\hat{d}_2^r &\ge d\left(C_0\right) + \min\left(d\left(C_{pc}\right), d\left(C_{pcf}\right) + d\left(C_p\right)\right),\\
\hat{d}_j^r &\ge \hat{d}_2^r + (j-2)d\left(C_{pcf}\right),
\end{aligned}$$

*где* $d\left(C_i\right)$ *– минимальный вес кода* $C_i$.

Докажем утверждение лемм рассмотрением всех возможных случаев. Исследуем результаты произведения (4) при $j = 1,\ 2, \ldots$.

I. $j = 1$

Пусть $\mathbf{u} = [\ldots,\ \mathbf{0},\ \mathbf{u}_t,\ \mathbf{0},\ \ldots]$, где $\mathbf{u}_t = (\mathbf{u}_{t,0}\ \mathbf{u}_{t,1})$, $\mathbf{u}_t \ne \mathbf{0}$. Распишем результаты произведения (4):

$$\begin{aligned}
\mathbf{v} &= [\ldots,\ \mathbf{0},\ \mathbf{v}_t,\ \mathbf{v}_{t+1},\ \mathbf{0},\ \ldots],\\
\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c + \mathbf{u}_{t,1}\mathbf{G}_f,\\
\mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p.
\end{aligned}$$

Для случайного ненулевого информационного блока $\mathbf{u}_t = (\mathbf{u}_{t,0}\ \mathbf{u}_{t,1})$ возможны 3 случая.

1. На входе:
$$\mathbf{u}_{t,0} \ne \mathbf{0},\ \mathbf{u}_{t,1} = \mathbf{0}.$$
На выходе:
$$\begin{aligned}
\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c,\\
\mathbf{v}_{t+1} &= \mathbf{0}.
\end{aligned}$$
Блок $\mathbf{v}_t \in C_c$ и хэммингов вес кодовой последовательности $\mathrm{wt}\left(\mathbf{v}_t\ \mathbf{v}_{t+1}\right) \ge d\left(C_c\right)$.
2. На входе:
$$\mathbf{u}_{i,0} \ne \mathbf{0},\ \mathbf{u}_{i,1} \ne \mathbf{0}.$$
На выходе:
$$\begin{aligned}
\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c + \mathbf{u}_{t,1}\mathbf{G}_f,\\
\mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p.
\end{aligned}$$
Блоки $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_p$ и вес кодовой последовательности $\mathrm{wt}\left(\mathbf{v}_t\ \mathbf{v}_{t+1}\right) \ge d\left(C_0\right) + d\left(C_p\right)$.
3. На входе:
$$\mathbf{u}_{i,0} = \mathbf{0},\ \mathbf{u}_{i,1} \ne \mathbf{0}.$$
На выходе:
$$\begin{aligned}
\mathbf{v}_t &= \mathbf{u}_{t,1}\mathbf{G}_f,\\
\mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p.
\end{aligned}$$
Блоки $\mathbf{v}_t \in C_f$, $\mathbf{v}_{t+1} \in C_p$, результирующий вес $\mathrm{wt}\left(\mathbf{v}_t\ \mathbf{v}_{t+1}\right) \ge d\left(C_f\right) + d\left(C_p\right)$.

Активное расстояние $d_1^r$ соответствует минимальному весу рассмотренных выше кодовых последовательностей. Пусть при равной длине кодов, коды с меньшей скоростью имеют большее кодовое расстояние. В асимптотическом случае, лучшие блоковые МПП–коды могут лежать сколь угодно близко к границе Варшамова–Гилберта и для них данное предположение выполняется. Тогда $d\left(C_0\right) < d\left(C_f\right)$ и минимальный возможный вес в случае 2 меньше, чем в случае 3. Сравним случаи 1 и 2. Кодовое расстояние $d\left(C_c\right)$ больше $d\left(C_0\right)$. Однако $d\left(C_c\right)$ может быть меньше суммы $d\left(C_0\right) + d\left(C_p\right)$. Последняя определяется отношением между $k'$ и $\nu'$. Так, если $k' - \nu' > \nu'$, то $d\left(C_c\right) < d\left(C_p\right)$ и $d_1^r = d\left(C_c\right)$. Таким образом,

$$\hat{d}_1^r = \min\left(d\left(C_c\right), d\left(C_0\right) + d\left(C_p\right)\right).$$

II. $j = 2$

Пусть информационная последовательность $\mathbf{u}$ состоит из 2 последовательных ненулевых блоков $\mathbf{u} = [\ldots,\ \mathbf{0},\ \mathbf{u}_t,\ \mathbf{u}_{t+1},\ \mathbf{0},\ \ldots]$, где $\mathbf{u}_i = (\mathbf{u}_{i,0}\ \mathbf{u}_{i,1})$, $i = t, t+1$. Исследуем все возможные кодовые последовательности, порождаемые информационной последовательностью такого вида. Из уравнения (4):

$$\begin{aligned}\mathbf{v} &= [\ldots,\ \mathbf{0},\ \mathbf{v}_t,\ \mathbf{v}_{t+1},\ \mathbf{v}_{t+2},\ \mathbf{0},\ \ldots],\\ \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c + \mathbf{u}_{t,1}\mathbf{G}_f,\\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p + \mathbf{u}_{t+1,0}\mathbf{G}_c + \mathbf{u}_{t+1,1}\mathbf{G}_f,\\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_p.\end{aligned}$$

Рассмотрим возможные случаи.

1. На входе:

$$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} = \mathbf{0},\ \text{блок } \mathbf{u}_{t+1}\text{произвольный ненулевой.}$$

На выходе:

$$\begin{aligned}\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c,\\ \mathbf{v}_{t+1} &= \mathbf{u}_{t+1,0}\mathbf{G}_c + \mathbf{u}_{t+1,1}\mathbf{G}_f,\\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_p.\end{aligned}$$

Получаем, $\mathbf{v}_t \in C_c$, а блоки $\mathbf{v}_{t+1}$, $\mathbf{v}_{t+2}$ соответствуют кодовым блокам, рассмотренным в случае $n = 1$. Таким образом, $\mathrm{wt}\,(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}) \geq d\,(C_c) + \hat{d}_1^r$.

2. На входе:

$$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \mathbf{u}_{t+1,0} \neq \mathbf{0},\ \mathbf{u}_{t+1,1} = \mathbf{0}.$$

На выходе:

$$\begin{aligned}\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c + \mathbf{u}_{t,1}\mathbf{G}_f,\\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p + \mathbf{u}_{t+1,0}\mathbf{G}_c,\\ \mathbf{v}_{t+2} &= \mathbf{0}.\end{aligned}$$

Блок $\mathbf{v}_{i+1} \in C_{pc}$ и $\mathbf{v}_{i+1} \neq \mathbf{0}$, так как порождающий его информационный блок ненулевой: $\mathbf{u}_{t,1} \neq \mathbf{0}$, $\mathbf{u}_{t+1,0} \neq \mathbf{0}$. Получаем, $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_{pc}$ и $\mathrm{wt}\,(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{0}) \geq d\,(C_0) + d\,(C_{pc})$.

3. На входе:

$$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \mathbf{u}_{t+1,0} = \mathbf{0},\ \mathbf{u}_{t+1,1} \neq \mathbf{0}$$

На выходе:

$$\begin{aligned}\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c + \mathbf{u}_{t,1}\mathbf{G}_f,\\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p + \mathbf{u}_{t+1,1}\mathbf{G}_f,\\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_p.\end{aligned}$$

Блок $\mathbf{v}_{i+1} \neq \mathbf{0}$. Получаем, $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_{pf}$, $\mathbf{v}_{t+2} \in C_p$ и $\mathrm{wt}\,(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}) \geq d\,(C_0) + d\,(C_{pf}) + d\,(C_p)$.

4. На входе:

$$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \mathbf{u}_{t+1,0} \neq \mathbf{0},\ \mathbf{u}_{t+1,1} \neq \mathbf{0}.$$

На выходе:

$$\begin{aligned}\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c + \mathbf{u}_{t,1}\mathbf{G}_f,\\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p + \mathbf{u}_{t+1,0}\mathbf{G}_c + \mathbf{u}_{t+1,1}\mathbf{G}_f,\\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_p.\end{aligned}$$

Получаем, $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_{pcf}$, $\mathbf{v}_{t+2} \in C_p$б $\mathbf{v}_{i+1} \neq \mathbf{0}$. Вес кодовой последовательности $\mathrm{wt}\,(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}) \geq d\,(C_0) + d\,(C_{pcf}) + d\,(C_p)$.

5. На входе:

$$\mathbf{u}_{t,0} = \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \text{ненулевой } \mathbf{u}_{t+1}.$$

В зависимости от $\mathbf{u}_{i+1}$, этот случай будет покрываться случаями 2–4 с тем исключением, что $\mathbf{v}_t \notin C_0$, $\mathbf{v}_t \in C_f$. Так как $d(C_f) > d(C_0)$, то вес получившейся последовательности будет всегда больше, чем в случаях 2–4.

Определим минимальный вес среди возможных случаев. Сравним случаи 3 и 4:

$$d(C_0) + d(C_{pf}) + d(C_p) > d(C_0) + d(C_{pcf}) + d(C_p),$$

так как $d(C_{pf}) > d(C_{pcf})$: $\dim(C_{pf}) = 2\nu'$, $\dim(C_{pcf}) = k' + \nu'$, а $2\nu' < k' + \nu'$.
Сравним случаи 1 и 2:

$$d(C_c) + \min(d(C_c),\ d(C_0) + d(C_p)) > d(C_0) + d(C_{pc}),$$

так как $d(C_c) > d(C_{pc})$, $d(C_c) > d(C_0)$, а $\min(d(C_c),\ d(C_0) + d(C_p))$ больше $d(C_0)$ в любом случае. Сравним случаи 4 и 2:

$$d(C_0) + d(C_{pcf}) + d(C_p)\ \ V\ \ d(C_0) + d(C_{pc}).$$

Вес $d(C_{pc}) > d(C_{pcf})$: $\dim(C_{pc}) = k'$, $\dim(C_{pcf}) = k' + \nu'$. Однако вес $d(C_{pc})$ может оказаться как меньше, так и больше суммарного веса $d(C_{pcf}) + d(C_p)$. Таким образом,

$$\hat{d}_2^r = d(C_0) + \min(d(C_{pc}), d(C_{pcf}) + d(C_p)).$$

### III. $j = 3$

Пусть информационная последовательность $\mathbf{u}$ состоит из 3 последовательных ненулевых блоков $\mathbf{u} = [\ldots,\ \mathbf{0},\ \mathbf{u}_t,\ \mathbf{u}_{t+1},\ \mathbf{u}_{t+2},\ \mathbf{0},\ \ldots]$, где $\mathbf{u}_i = (\mathbf{u}_{i,0}\ \mathbf{u}_{i,1})$, $i = t, t+1, t+2$. Исследуем все возможные кодовые последовательности, порождаемые информационной последовательностью такого вида. Из уравнения (4):

$$\begin{aligned}
\mathbf{v} &= [\ldots,\ \mathbf{0},\ \mathbf{v}_t,\ \mathbf{v}_{t+1},\ \mathbf{v}_{t+2},\ \mathbf{v}_{t+3},\ \mathbf{0},\ \ldots],\\
\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c + \mathbf{u}_{t,1}\mathbf{G}_f,\\
\mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p + \mathbf{u}_{t+1,0}\mathbf{G}_c + \mathbf{u}_{t+1,1}\mathbf{G}_f,\\
\mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_p + \mathbf{u}_{t+2,0}\mathbf{G}_c + \mathbf{u}_{t+2,1}\mathbf{G}_f,\\
\mathbf{v}_{t+3} &= \mathbf{u}_{t+2,1}\mathbf{G}_p.
\end{aligned}$$

Рассмотрим основные случаи.

1. На входе:

$$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} = \mathbf{0},\ \text{произвольные } \mathbf{u}_{t+1}, \mathbf{u}_{t+2}.$$

На выходе:

$$\begin{aligned}
\mathbf{v}_t &= \mathbf{u}_{i,0}\mathbf{G}_c,\\
\mathbf{v}_{t+1} &= \mathbf{u}_{t+1,0}\mathbf{G}_c + \mathbf{u}_{t+1,1}\mathbf{G}_f,\\
\mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_p + \mathbf{u}_{t+2,0}\mathbf{G}_c + \mathbf{u}_{t+2,1}\mathbf{G}_f,\\
\mathbf{v}_{t+3} &= \mathbf{u}_{t+2,1}\mathbf{G}_p.
\end{aligned}$$

Блок $\mathbf{v}_t \in C_c$. В зависимости от распределения нулевых частей в $\mathbf{u}_{t+1}$ и $\mathbf{u}_{t+2}$ кодовые блоки $\mathbf{v}_{t+1}$, $\mathbf{v}_{t+2}$, $\mathbf{v}_{t+3}$ относятся к кодам и случаям, рассмотренным при изучении $\hat{d}_2^r$. Вес кодовой последовательности $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}\ \mathbf{v}_{t+3}) \geq d(C_c) + \hat{d}_2^r$.

2. На входе:

$$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \mathbf{u}_{t+1,0} \neq \mathbf{0},\ \mathbf{u}_{t+1,1} = \mathbf{0},\ \text{ненулевой } \mathbf{u}_{t+2}.$$

На выходе:

$$\begin{aligned}\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c + \mathbf{u}_{t,1}\mathbf{G}_f,\\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p + \mathbf{u}_{t+1,0}\mathbf{G}_c,\\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+2,0}\mathbf{G}_c + \mathbf{u}_{t+2,1}\mathbf{G}_f,\\ \mathbf{v}_{t+3} &= \mathbf{u}_{t+2,1}\mathbf{G}_p.\end{aligned}$$

Блоки $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_{pc}$, а блоки $\mathbf{v}_{t+2}$, $\mathbf{v}_{t+3}$ соответствуют случаям, рассмотренным при анализе $\hat{d}_1^r$. Вес последовательности $\mathrm{wt}\,(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}\ \mathbf{v}_{t+3}) \geq d\,(C_0) + d\,(C_{pc}) + \hat{d}_1^r$. Далее мы опустим случай отличающийся только тем, что $\mathbf{u}_{t,0} = \mathbf{0}$. Результат будет аналогичным, за исключением $\mathbf{v}_i \in C_c$, а это увеличит вес.

3. На входе:

$$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \mathbf{u}_{t+1,0} \neq \mathbf{0},\ \mathbf{u}_{t+1,1} \neq \mathbf{0},\ \text{ненулевой } \mathbf{u}_{i+2,0}.$$

На выходе:

$$\begin{aligned}\mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_c + \mathbf{u}_{t,1}\mathbf{G}_f,\\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_p + \mathbf{u}_{t+1,0}\mathbf{G}_c + \mathbf{u}_{t+1,1}\mathbf{G}_f,\\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_p + \mathbf{u}_{t+2,0}\mathbf{G}_c + \mathbf{u}_{t+2,1}\mathbf{G}_f,\\ \mathbf{v}_{t+3} &= \mathbf{u}_{t+2,1}\mathbf{G}_p.\end{aligned}$$

Блоки $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_{pcf}$, а блоки $\mathbf{v}_{t+2}$, $\mathbf{v}_{t+3}$ соответствуют случаям 2–4 анализа $\hat{d}_2^r$. Вес последовательности $\mathrm{wt}\,(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}\ \mathbf{v}_{t+3}) \geq d\,(C_0) + d\,(C_{pcf}) + \min\left(d\,(C_{pc}),\ d\,(C_{pcf}) + d\,(C_p)\right)$.

Из рассмотрения опущены случаи, когда $\mathbf{u}_{t,0} = \mathbf{0}$, $\mathbf{u}_{t,1} \neq \mathbf{0}$ или $\mathbf{u}_{t+1,0} = \mathbf{0}$, $\mathbf{u}_{t+1,1} \neq \mathbf{0}$. Они дают результаты, похожие на результаты в случаях 2 или 3, но с большим весом. Определим минимальный вес среди возможных случаев. Вычтем общие части и сравним случаи 1 и 3:

$$d\,(C_c) > d\,(C_{pcf})\,.$$

Вычтем общие части и сравним случаи 2 и 3:

$$d\,(C_{pc}) + \min\left(d\,(C_c)\,, d\,(C_0) + d\,(C_p)\right) > d\,(C_{pcf}) + \min\left(d\,(C_{pcf})\,,\ d\,(C_{pc}) + d\,(C_p)\right).$$

Получаем,

$$\hat{d}_3^r = \hat{d}_2^r + d\,(C_{pcf})\,.$$

Продолжая анализ, можно показать, что начиная с $j = 2$, активные строчные расстояния растут по закону

$$\hat{d}_j^r \geq \hat{d}_2^r + (j-2)d\,(C_{pcf})$$

с уклоном

$$\alpha = d\,(C_{pcf})\,.$$

Таким образом, утверждения лемм 1–3 справедливы. Отметим, что при полной памяти один ненулевой блок всегда порождает два ненулевых кодовых блока. Таким образом, при $\nu = k$, активное расстояние $\hat{d}_1^r = d\,(C_0) + d\,(C_p)$, а $\hat{d}_2^r = d\,(C_0) + d\,(C_{pcf}) + d\,(C_p)$.

## 4. ОЦЕНКА КОДОВЫХ РАССТОЯНИЙ

В результате проведенного в разделе 3 анализа было показано, что кодовые последовательности кодов из ансамбля (Ч)ЕП-МПП–кодов с весами, равными активным расстояниям $\hat{d}_j^r$, состоят из $j$ (возможно только для ЧЕП-кодов) или $j+1$ идущих подряд ненулевых блоков. В соответствии с проверочной матрицей (2) каждая пара соседних блоков должна удовлетворять системе рекуррентных линейных уравнений

$$\begin{cases} \mathbf{H}_c(t-1)\mathbf{v}_{t-1}^{\mathrm{T}} = \mathbf{0} \\ \mathbf{H}_f(t)\mathbf{v}_{t-1}^{\mathrm{T}} + \mathbf{H}_p(t)\mathbf{v}_t^{\mathrm{T}} = \mathbf{0} \\ \mathbf{H}_c(t)\mathbf{v}_t^{\mathrm{T}} = \mathbf{0} \end{cases}$$

Дополнительно, первый ненулевой и последний ненулевой блоки должны удовлетворять условиям

$$\mathbf{H}_p(0)\mathbf{v}_0^{\mathrm{T}} = \mathbf{0},\ \mathbf{H}_f(j)\mathbf{v}_j^{\mathrm{T}} = \mathbf{0}.$$

Уравнение

$$\mathbf{H}_f(t)\mathbf{v}_{t-1}^{\mathrm{T}} + \mathbf{H}_p(t)\mathbf{v}_t^{\mathrm{T}} = \mathbf{0}$$

описывает проверочную матрицу

$$[\mathbf{H}_f(t)\ \mathbf{H}_p(t)] \tag{6}$$

и отвечает за память сверточного кода. В соответствии с леммами 1 – 2, память между кодовыми блоками не обнуляется и при проверках кодовых блоков матрицами $\mathbf{H}_f(t)$ и $\mathbf{H}_p(t)$ возникают совпадающие синдромы:

$$\mathbf{H}_f(t)\mathbf{v}_{t-1}^{\mathrm{T}} = \mathbf{S},\ \mathbf{H}_p(t)\mathbf{v}_t^{\mathrm{T}} = \mathbf{S},$$

где $\mathbf{S}$ – некоторый синдром. Частный случай блочных МПП-кодов с проверочной матрицей вида (6) был исследован Ф. Хугом, В. Зябловым и Р. Йоханнесеном в работе [9]. В нашем случае, при расчете минимального веса двух последовательных кодовых блоков необходимо анализировать проверочную матрицу следующего вида:


В зависимости от расположения пары кодовых блоков внутри кодовой последовательности, матрицы $\mathbf{H}_i$ будут меняться. Например, при расчете веса $d(C_0) + d(C_p)$ для активного расстояния $\hat{d}_1^r$ матрица $\mathbf{H}_1 = \begin{pmatrix} \mathbf{H}_p(t) \\ \mathbf{H}_c(t) \end{pmatrix}$, матрицы $\mathbf{H}_2 = \mathbf{H}_f(t+1)$, $\mathbf{H}_3 = \mathbf{H}_p(t+1)$ и $\mathbf{H}_4 = \begin{pmatrix} \mathbf{H}_c(t+1) \\ \mathbf{H}_f(t+2) \end{pmatrix}$. В общем случае, пусть матрицы $\mathbf{H}_i$, $1 \le i \le 4$ принадлежат ансамблям $\mathcal{E}(n_0, \ell_i, b)$ МПП-кодов, $\ell_2 = \ell_3$. Пусть представленная блочная матрица принадлежит ансамблю $\mathcal{E}_{ch}$. Оценим кодовое расстояние в ансамбле $\mathcal{E}_{ch}$.

Воспользуемся методом Галлагера [7]. Пусть $N_{ch}(W)$ – среднее число кодовых слов веса $W$ в ансамбле $\mathcal{E}_{ch}$. Тогда, до тех пор пока $\sum\limits_{W=2}^{W_0} N_{ch}(W) < 1$, в ансамбле найдется хотя бы один код с минимальным расстоянием $d_{ch} > W_0$.

Выразим среднее число кодовых слов заданного веса в ансамбле $\mathcal{E}_{ch}$ через вероятность $P(W)$ случайного слова $\mathbf{r} = (\mathbf{r}_{12}\ \mathbf{r}_{34})$ веса $W$ оказаться кодовым в ансамбле:

$$N_{ch}(W) = \binom{2n}{W} P(W).$$

Для произвольного кода из ансамбля $\mathcal{E}_{ch}$, слово $\mathbf{r}$ будет кодовым, если выполняется система

$$\begin{cases} \mathbf{H}_1 \mathbf{r}_{12}^{\mathrm{T}} = \mathbf{0} \\ \mathbf{H}_2 \mathbf{r}_{12}^{\mathrm{T}} + \mathbf{H}_3 \mathbf{r}_{34}^{\mathrm{T}} = \mathbf{0} \\ \mathbf{H}_4 \mathbf{r}_{34}^{\mathrm{T}} = \mathbf{0} \end{cases}. \tag{7}$$

Совместность системы (7) зависит от распределения веса $W$ по блокам $\mathbf{r}_{12}$ и $\mathbf{r}_{34}$, при этом слова $\mathbf{r}_{12}$ и $\mathbf{r}_{34}$ должны принадлежать кодам с проверочными матрицами $\mathbf{H}_1$ и $\mathbf{H}_4$ из ансамблей $\mathcal{E}(n_0, \ell_1, b)$ и $\mathcal{E}(n_0, \ell_4, b)$, соответственно, а синдромы $\mathbf{H}_2 \mathbf{r}_{12}^{\mathrm{T}} = \mathbf{S}_{12}$, $\mathbf{H}_3 \mathbf{r}_{34}^{\mathrm{T}} = \mathbf{S}_{34}$ должны совпадать. Распределение веса $W$ между словами может быть различно, поэтому необходимо найти случай с наибольшей вероятностью.

Пусть $N_i(W)$ – среднее число кодовых слов веса $W$ в ансамбле МПП-кодов $\mathcal{E}(n_0, \ell_i, b)$, а $P_i(\mathbf{S}_j|x)$ – вероятность получить для слова веса $x$ синдром $\mathbf{S}_j$ в ансамбле кодов $\mathcal{E}(n_0, \ell_i, b)$. Среднее число кодовых пар с заданными весами $W_1 2$ и $W_3 4$ в ансамблях $\mathcal{E}(n_0, \ell_1, b)$ и $\mathcal{E}(n_0, \ell_4, b)$ оценивается произведением $N_1(W_{12}) N_4(W_{34})$. Вероятность в зависимости от веса получить совпадающие синдромы для ансамблей $\mathcal{E}(n_0, \ell_2, b)$ и $\mathcal{E}(n_0, \ell_3, b)$ можно описать суммой по всем возможным синдромам:

$$\sum_{\mathbf{S}_j} P_2(\mathbf{S}_j|W_{12}) P_3(\mathbf{S}_j|W_{34}).$$

Таким образом, слово веса $W$ окажется кодовым в ансамбле $\mathcal{E}_{ch}$ с вероятностью

$$P(W) = \frac{\sum\limits_{y=0}^{W} \left( N_1(y) N_4(W-y) \sum\limits_{\mathbf{S}_j} P_2(\mathbf{S}_j|y) P_3(\mathbf{S}_j|W-y) \right)}{\binom{2n}{W}}, \tag{8}$$

**Утверждение 1.** *Наибольшая вероятность случайного слова* $\mathbf{r} = (\mathbf{r}_{12}\ \mathbf{r}_{34})$ *веса* $W$ *и длины* $2n$ *оказаться кодовым в ансамбле* $\mathcal{E}_{ch}$ *в зависимости от распределения веса между частями* $\mathbf{r}_{12}$ *и* $\mathbf{r}_{34}$ *достигается при* $\mathrm{wt}(\mathbf{v_{12}}) = \mathrm{wt}(\mathbf{v_{12}}) = W/2$.

Докажем утверждение 1.
Рассмотрим по отдельности вероятность $\sum\limits_{\mathbf{S}_j} P_2(\mathbf{S}_j|y) P_3(\mathbf{S}_j|W-y)$ совпадения синдромов и среднее число $N_1(y) N_4(W-y)$ кодовых пар в ансамблях.

Пусть $g_0(s)$ – производящая функция кодовых слов кодов-компонентов МПП-кодов Галлагера, а $g_1(s)$ – производящая функция ошибок.

$$g_0(s) = \left( \frac{(1+s)^k + (1-s)^k}{2} \right),$$
$$g_1(s) = \left( \frac{(1+s)^k - (1-s)^k}{2} \right).$$

Тогда среднее число кодовых слов веса $W$ в ансамбле $\mathcal{E}_i$ можно оценить как

$$N_i(W) \le \frac{\min\limits_{s>0}\{\frac{g_0^b(s)}{s^W}\}^{\ell_i}}{\binom{n}{W}^{\ell_i-1}}.$$

Так как в слоях проверочных матриц МПП–кодов выполняются независимые перестановки, то вероятности синдромов можно рассмотреть как произведение независимых вероятностей подсиндромов в слоях. Все возможные сочетания невыполненных проверок в слое на совпадающих позициях матриц $\mathbf{H}_2$ и $\mathbf{H}_3$ дадут все возможные совпадающие подсиндромы. Тогда,

$$\sum_{\mathbf{S}_j} P_2(\mathbf{S}_j|y)P_3(\mathbf{S}_j|W-y) =$$

$$\prod_{\ell_2}\sum_i \binom{b}{i} \frac{\min\limits_{s_2>0} s_2^{-y} g_1^i(s_2) g_0^{b-i}(s_2)}{\binom{n}{y}} \frac{\min\limits_{s_3>0} s_3^{-W+y} g_1^i(s_3) g_0^{b-i}(s_3)}{\binom{n}{W-y}}$$

Вынесем независимые множители за скобки:

$$\sum_{\mathbf{S}_j} P_2(\mathbf{S}_j|y)P_3(\mathbf{S}_j|W-y) =$$

$$\frac{\min\limits_{s_2>0}\min\limits_{s_3>0} s_2^{-y\ell_2} s_3^{-(W-y)\ell_3}}{\binom{n}{y}^{\ell_2}\binom{n}{W-y}^{\ell_3}} \prod_{\ell_{23}}\sum_i \binom{b}{i} g_1^i(s_2) g_0^{b-i}(s_2) g_1^i(s_3) g_0^{b-i}(s_3).$$

$$\sum_{\mathbf{S}_j} P_2(\mathbf{S}_j|y)P_3(\mathbf{S}_j|W-y) = \frac{\min\limits_{s_2>0}\min\limits_{s_3>0} s_2^{-y\ell_2} s_3^{-(W-y)\ell_3} \left(g_0(s_2)g_0(s_3)+g_1(s_2)g_1(s_3)\right)^{b\ell}}{\binom{n}{y}^{\ell_2}\binom{n}{W-y}^{\ell_3}}. \qquad (9)$$

Оценим (9) сверху. Заметим, что знаменатель не зависит от $s_i$. Для отыскания минимума по $s_i$ исследуем частные производные числителя:

$$D_{s_2}\left[C s_2^{-y\ell_2}(g0(s_2)A + g1(s_2)B)^{\ell_2 b}\right] =$$

$$C2^{-b\ell_2}\ell_2 s_2^{-y\ell_2}\left[B\left((1+s_2)^{n_0}-(1-s_2)^{n_0}\right)+A\left((1-s_2)^{n_0}+(1+s_2)^{n_0}\right)\right]^{b\ell_2}\times$$

$$\times\left(\frac{bn_0\left[A\left((1+s_2)^{n_0-1}-(1-s_2)^{n_0-1}\right)+B\left((1-s_2)^{n_0-1}+(1+s_2)^{n_0-1}\right)\right]}{B\left((1+s_2)^{n_0}-(1-s_2)^{n_0}\right)+A\left((1-s_2)^{n_0}+(1+s_2)^{n_0}\right)} - \frac{y}{s_2}\right),$$

где A, B, C - константы, зависящие от $s_3$. $A = g_0(s_3)$, $B = g_1(s_3)$. Заметим, что произведение

$$C2^{-b\ell_2}\ell_2 s_2^{-y\ell_2}\left[B\left((1+s_2)^{n_0}-(1-s_2)^{n_0}\right)+A\left((1-s_2)^{n_0}+(1+s_2)^{n_0}\right)\right]^{b\ell_2}$$

всегда положительно, так как $A,\ B > 0$, $s_2 \in (0,1)$. Ноль производной может дать только правый сомножитель

$$\left(\frac{bn_0\left[A\left((1+s_2)^{n_0-1}-(1-s_2)^{n_0-1}\right)+B\left((1-s_2)^{n_0-1}+(1+s_2)^{n_0-1}\right)\right]}{B\left((1+s_2)^{n_0}-(1-s_2)^{n_0}\right)+A\left((1-s_2)^{n_0}+(1+s_2)^{n_0}\right)} - \frac{y}{s_2}\right).$$

После приведения к общему знаменателю решим уравнение

$$bn_0 s_2 \left[A\left((1+s_2)^{n_0-1}-(1-s_2)^{n_0-1}\right)+B\left((1-s_2)^{n_0-1}+(1+s_2)^{n_0-1}\right)\right]- \\ y\left[B\left((1+s_2)^{n_0}-(1-s_2)^{n_0}\right)+A\left((1-s_2)^{n_0}+(1+s_2)^{n_0}\right)\right]=0.$$

Сгруппировав коэффициенты при $(1-s_2)^{n_0-1}$ и $(1+s_2)^{n_0-1}$, получим:

$$(A-B)(1-s_2)^{n_0-1}\left(bn_0 s_2+y(1-s_2)\right)=(A+B)(1+s_2)^{n_0-1}\left(y(1+s_2)-bn_0 s_2\right).$$

Левая часть уравнения (4) положительна при любых $y>0$, $s_{2,3}\in(0,1)$, а правая только при $s_2>\frac{y}{bn_0-y}$. Возьмем граничные значения $s_2=\frac{y}{bn_0-y}$, $s_3=\frac{W-y}{bn_0-W+y}$. При подстановке этих значений в (9), максимальное значение (9) по $y$ наблюдается при $y=\frac{W}{2}$. Аналогичное наблюдение выполняется и для сомножителя $N_1(y)N_4(W-y)$ из (8). Покажем это.

$$N_1(y)N_4(W-y)=\frac{\min\limits_{s_1>0}\left\{\frac{g_0^b(s_1)}{{s_1}^y}\right\}^{\ell_1}}{\binom{n}{y}^{\ell_1-1}}\frac{\min\limits_{s_4>0}\left\{\frac{g_0^b(s_4)}{{s_4}^{W-y}}\right\}^{\ell_4}}{\binom{n}{W-y}^{\ell_4-1}}. \tag{10}$$

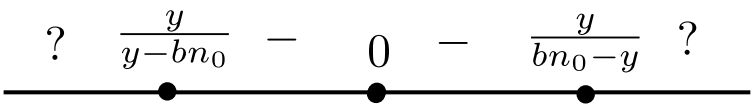
Возьмем частную производную по $s_1$.

$$D_{s_1}\left[s_1^{-y\ell_1}g_0\left(s_1\right)^{\ell_1 b}C\right]= \\ 2^{-\ell_1 b}C\ell_1 s_1^{-\ell_1 y}\left((1-s_1)^{n_0}+(1+s_1)^{n_0}\right)^{\ell_1 b}\times \\ \times\left[\frac{bn_0\left((1+s_1)^{n_0-1}-(1-s_1)^{n_0-1}\right)}{(1-s_1)^{n_0}+(1+s_1)^{n_0}}-\frac{y}{s_1}\right].$$

После приведения к общему знаменателю, получим условие экстремума:

$$(1+s_1)^{n_0-1}\left[s_1(bn_0-y)-y\right]+(1-s_1)^{n_0-1}\left[s_1(y-bn_0)-y\right]=0. \tag{11}$$

В зависимости от $s_1$, функция в левой части (11) имеет различный знак: Пусть $s_0$ – поло-




жительный корень уравнения (11), тогда $s_0>\frac{y}{bn_0-y}$. В соответствии со знаком производной, минимум выражения (10) по $s_i$ достигается при $s_i>\frac{y}{bn_0-y}$.

Получаем следующую оценку сверху на слагаемые в выражении (8).

$$N_1(y)N_4(W-y)\sum_{\mathbf{S}_j}P_2(\mathbf{S}_j|y)P_3(\mathbf{S}_j|W-y)= \\ \frac{\min\limits_{s_1,\ s_2,\ s_3,\ s_4>0}s_1^{-y\ell_1}s_2^{-y\ell_2}s_3^{-(W-y)\ell_3}s_4^{-(W-y)\ell_4}g_0^{\ell_1 b}(s_1)g_0^{\ell_4 b}(s_4)\left(g_0(s_2)g_0(s_3)+g_1(s_2)g_1(s_3)\right)^{\ell_2 b}}{\binom{n}{y}^{\ell_1+\ell_2-1}\binom{n}{W-y}^{\ell_3+\ell_4-1}}\le \\ \left.\frac{s_1^{-y\ell_1}s_2^{-y\ell_2}s_3^{-(W-y)\ell_3}s_4^{-(W-y)\ell_4}g_0^{\ell_1 b}(s_1)g_0^{\ell_4 b}(s_4)\left(g_0(s_2)g_0(s_3)+g_1(s_2)g_1(s_3)\right)^{\ell_2 b}}{\binom{n}{y}^{\ell_1+\ell_2-1}\binom{n}{W-y}^{\ell_3+\ell_4-1}}\right|_{s_{1,2}=\frac{y}{bn_0-y},\ s_{3,4}=\frac{W-y}{bn_0-W+y}}. \tag{12}$$

Обозначим $\ell_3+\ell_4=\ell$. При выборе $\ell_1=\ell_4$, (12) преобразуется в

$$\frac{y}{(bn_0-y)}^{-y\ell}\frac{(W-y)}{(bn_0-W+y)}^{-(W-y)\ell}\frac{g_0^{\ell_1 b}(s_1)g_0^{\ell_4 b}(s_4)\left(g_0(s_2)g_0(s_3)+g_1(s_2)g_1(s_3)\right)^{\ell_2 b}}{\binom{n}{y}^{\ell-1}\binom{n}{W-y}^{\ell-1}}. \qquad (13)$$

Найдем максимальное слагаемое в зависимости от $y$. Анализируя производную, можно показать, что при выборе $s_1=s_2=\frac{y}{bn_0-y}$, $s_3=s_4=\frac{W-y}{bn_0-W+y}$ максимальное значение выражения (13) достигается в точке $y=\frac{W}{2}$. Утверждение 1 доказано.

**Теорема 1.** *Если существует положительный корень $\delta_0$ уравнения*

$$\frac{\ell_2}{n_0}\log\left(\frac{\left(1-\frac{\delta}{2-\delta}\right)^{2n_0}+\left(1+\frac{\delta}{2-\delta}\right)^{2n_0}}{2}\right)-\delta\ell\log\left(\frac{\delta}{2-\delta}\right)+\frac{\ell_1+\ell_4}{n_0}\log\left(g_0(\tfrac{\delta}{2-\delta})\right)-2H(\tfrac{\delta}{2})(\ell-1)=0$$

*относительно переменной $\delta$, то в ансамбле $\mathcal{E}_{ch}(\ell_1,\ell_2,n_0,b)$ существуют коды с относительным расстоянием больше $\delta_0$.*

Докажем теорему 1.

**Доказательство.** Подставив $y=\frac{W}{2}$ в (13), получим

$$\frac{2^{-b\ell_2}\left(\frac{W}{2bn_0-W}\right)^{-W\ell}\left(\left(1-\frac{W}{2bn_0-W}\right)^{2n_0}+\left(1+\frac{W}{2bn_0-W}\right)^{2n_0}\right)^{\ell_2 b}\left[g_0\left(\frac{W}{2bn_0-W}\right)\right]^{(\ell_1+\ell_4)b}}{\binom{n}{W/2}^{2\ell-2}}.$$

Таким образом,

$$P(W)\le\frac{2^{-b\ell_2}W\left(\frac{W}{2bn_0-W}\right)^{-W\ell}\left(\left(1-\frac{W}{2bn_0-W}\right)^{2n_0}+\left(1+\frac{W}{2bn_0-W}\right)^{2n_0}\right)^{\ell_2 b}\left[g_0\left(\frac{W}{2bn_0-W}\right)\right]^{(\ell_1+\ell_4)b}}{\binom{2n}{W}\binom{n}{W/2}^{2\ell-2}}$$

и среднее число кодовых слов $N_{ch}(W)=\binom{2n}{W}P(W)$ веса $W$ в ансамбле $\mathcal{E}_{ch}$ ограничено сверху:

$$N_{ch}(W)\le\frac{2^{-b\ell_2}W\left(\frac{W}{2bn_0-W}\right)^{-W\ell}\left(\left(1-\frac{W}{2bn_0-W}\right)^{2n_0}+\left(1+\frac{W}{2bn_0-W}\right)^{2n_0}\right)^{\ell_2 b}\left[g_0\left(\frac{W}{2bn_0-W}\right)\right]^{(\ell_1+\ell_4)b}}{\binom{n}{W/2}^{2\ell-2}}. \qquad (14)$$

До тех пор, пока $\sum\limits_{W=2}^{W=2n}N_{ch}(W)<1$, в ансамбле найдется хотя бы один код с минимальным расстоянием $d_{ch}>W$. Пусть $\delta$ - относительное расстояние, $\delta=\frac{W}{N}$, тогда асимптотическая оценка относительного кодового расстояния может быть получена из условия

$$\log\left(\frac{2^{-b\ell_2}(n_0b\delta)^2\left(\frac{\delta}{2-\delta}\right)^{-bn_0\delta\ell}\left(\left(1-\frac{\delta}{2-\delta}\right)^{2n_0}+\left(1+\frac{\delta}{2-\delta}\right)^{2n_0}\right)^{\ell_2 b}\left[g_0\left(\frac{\delta}{2-\delta}\right)\right]^{(\ell_1+\ell_4)b}}{2^{2nb_0H(\frac{\delta}{2})(\ell-1)}}\right)\le 0.$$

$$F(\delta)=\frac{\ell_2}{n_0}\log\left(\frac{\left(1-\frac{\delta}{2-\delta}\right)^{2n_0}+\left(1+\frac{\delta}{2-\delta}\right)^{2n_0}}{2}\right)-\delta\ell\log\left(\frac{\delta}{2-\delta}\right)+\frac{\ell_1+\ell_4}{n_0}\log\left(g_0(\tfrac{\delta}{2-\delta})\right)-2H(\tfrac{\delta}{2})(\ell-1).$$

## 5. ЗАВИСИМОСТЬ ПАМЯТИ ОТ СКОРОСТИ

При скоростях $R \le 0.5$ коды из рассматриваемого ансамбля могут обладать полной памятью:

$$k \le 0.5n$$
$$\nu = k$$
$$\nu + k < n$$

В таком случае, при вычислении минимального веса блокового кода, составленного из первых двух кодовых блоков последовательности, параметры ансамбля $\mathcal{E}_{ch}(\ell_1, \ell_2, n_0, b)$ получают следующие значения: $\ell_1 = n_0(1-R)$, $\ell_2 = n_0 R$, где $R = k/n$. Преобразуем функцию (4):

$$F(\delta) = R \log\left(\frac{\left(1-\frac{\delta}{2-\delta}\right)^{2n_0}+\left(1+\frac{\delta}{2-\delta}\right)^{2n_0}}{2}\right) - \delta n_0 \log\left(\frac{\delta}{2-\delta}\right) + 2(1-R)\log\left(g_0\left(\frac{\delta}{2-\delta}\right)\right) - 2H\left(\frac{\delta}{2}\right)(n_0-1).$$

При скоростях $R > 0.5$ возможна только частичная память, так как кодовое ограничение должно удовлетворять следующему неравенству:

$$\nu < n - k.$$

Предельная память $\nu = n - k - \epsilon$, где $\epsilon$ – сколь угодно малая положительная величина. Тогда $\ell_1 = \ell_2 = n_0(1-R)$ и

$$F(\delta) = (1-R)\log\left(\frac{\left(1-\frac{\delta}{2-\delta}\right)^{2n_0}+\left(1+\frac{\delta}{2-\delta}\right)^{2n_0}}{2}\right) - 2\delta n_0(1-R)\log\left(\frac{\delta}{2-\delta}\right) + 2(1-R)\log\left(g_0\left(\frac{\delta}{2-\delta}\right)\right) - 2H\left(\frac{\delta}{2}\right)(2n_0(1-R)-1).$$

При помощи функции (4) и установленных в разделе 3 соотношений для активных расстояний получим нижние асимптотические границы кодовых расстояний. Известные границы кодовых расстояний вместе с полученной границей свободного расстояния (Ч)ЕП-МПП-кодов представлены на рис.1. При полной памяти при скоростях $R \leq 0.5$ граница свободного расстояния ЕП-МПП–кодов совпадает с границей Томмесена–Юстесена. При скоростях больше 0.5 память неполная и убывает с ростом скорости. Граница свободного расстояния ЕП-МПП–кодов оказывается ниже границы Томмесена–Юстесена, но выше границы Варшамова–Гилберта.

Уклон активных расстояний оценивается минимальным весом ненулевого кодового блока последовательности. Можно показать, что вес такого блока оценивается минимальным весом блочного кода со следующей проверочной матрицей:

$$\begin{bmatrix} \mathbf{H}_c(t-1) & \\ \mathbf{H}_f(t) & \mathbf{H}_p(t) \end{bmatrix}.$$

Верхняя граница уклона активных расстояний сверточных кодов исследовалась в работе [10]. Относительное значение уклона (Ч)ЕП-МПП-кодов $\delta_\alpha$ оказывается близко к оптимальному и лежит рядом с границей Варшамова-Гилберта $\delta_{GV}$, немного не доходя до нее. Например, при скорости $R = 0.5$ $\delta_\alpha = 0.10988$, в то время как $\delta_{GV} = 0.11002$.

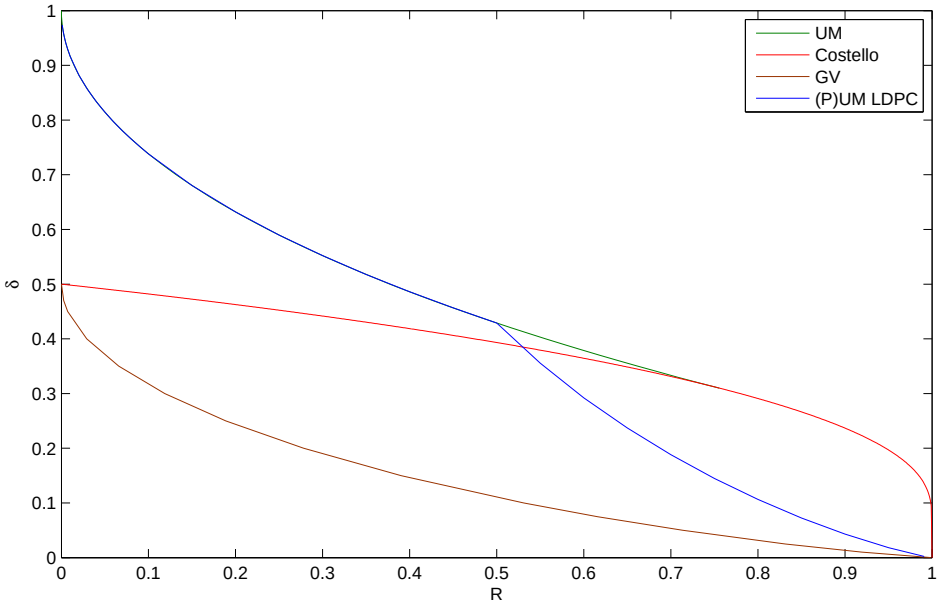



**Рис. 1.** Асимптотические границы относительного свободного расстояния. GV – граница Варшамова-Гилберта, Costello – граница Костелло, UM – граница Томмесена–Юстесена для кодов с полной единичной памятью, (P)UM LDPC – граница свободного расстояния для кодов с (частично)единичной памятью, полученных из блочных МПП–кодов.

## 6. ЗАКЛЮЧЕНИЕ

В данной работе представлен ансамбль двоичных сверточных кодов с (частично)единичной памятью, задаваемых проверочными матрицами вида (2), построенными на основе проверочных матриц блочных МПП-кодов. Для заданного ансамбля получена асимптотическая оценка свободного расстояния, при скоростях до 0.5 совпадающая с границей Томменсена и Юстенсена

для кодов с единичной памятью, построенных на основе лучших блочных кодов. При больших скоростях граница свободного расстояния ЧЕП-МПП-кодов хуже границы Томмесена–Юстесена, но лучше границы Варшамова–Гилберта. Получены аналитические границы активных строчных расстояний, показано, что коды по ансамблю имеют положительный уклон активных строчных расстояний, близкий к оптимальному. Сложность кодирования и декодирования таких кодов определяется сложностью кодирования и декодирования последовательности блочных МПП–кодов.

## СПИСОК ЛИТЕРАТУРЫ

1. Lee L.-N. Short Unit-Memory Byte-Oriented Binary Convolutional Codes Having Maximal Free Distance. *IEEE Transactions on Information Theory*. 1976, pp. 349–352.
2. Lauer G. S. Some Optimal Partial-Unit Memory Codes. *IEEE Transactions on Information Theory*. 1979, vol. 23, pp. 240–243.
3. Thommesen C., Justesen J. Bounds on distances and error exponents of unit memory codes. *IEEE Transactions on Information Theory*. 1983, vol. 29, pp. 637–649.
4. Zyablov V.V., Sidorenko V.R. On Periodic (Partial) Unit Memory Codes with Maximum Free Distance. *Lecture Notes in Computer Science*. 1994, vol. 829, pp. 74–79.
5. Dettmar U., Shavgulidze S. New Optimal Partial Unit Memory Codes. Electronic Letters. 1992, vol. 28, pp. 1748–1749.
6. Dettmar U., Sorger U. New optimal partial unit memory codes based on extended BCH codes. *Electronic Letters*. 1993, vol. 29, pp. 2024–2025.
7. Gallager R.G. Low-Density Parity-Check Codes The MIT Press: 1972.
8. Kondrashov K.A., Zyablov. V.V. On the lower bound of the free distance of partial unit memory codes based on LDPC Codes *Information Theory Proceedings (ISIT), IEEE International Symposium*. 2011, pp. 1831–1835.
9. Zyablov V.V., Hug F., Johannesson R. Chained Gallager codes. *International Symposium on Problems of Redundancy in Information and Control Systems*. 2009.
10. Jordan R., Pavlushkov V., Zyablov V.V. Maximum slope convolutional codes. *IEEE Transactions on Information Theory*. 2004, vol. 50, n. 10, pp. 2511 – 2526.

# Bounds on distances of partial unit memory codes based on LDPC Codes

**Kondrashov, K.; Zyablov, V.; Skopintsev, O.**

(Partial) Unit Memory codes provide a powerful possibility to construct convolutional codes based on block codes with resulting high correcting capabilities. In this contribution, an ensemble of (partial) unit memory codes based on LDPC block codes ((P)UM LDPC) is introduced. This ensemble is defined on set of semi-infinite parity check matrices with (partial) unit memory. Lower bounds for the free distance, active row distances and the slope of (P)UM LDPC codes are derived.

**KEYWORDS:** Convolutional codes, unit memory, LDPC, free distance, active row distances, slope.