Информационные процессы, Том 15, № 4, 2015, стр. 447–459

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ ИНФОРМАЦИИ

Корректирующая способность двоичного нерегулярного МПП-кода при декодирования по итеративному алгоритму с малой сложностью[1]

П. С. Рыбин

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

Поступила в редколлегию 18.12.2015

Аннотация—В работе рассматривается нерегулярный код с малой плотностью проверок (МПП-код) и два итеративных алгоритма декодирования с малой сложностью. В качестве первого алгоритма декодирования рассматривается мажоритарный алгоритм исправления ошибок, а в качестве второго – итеративный алгоритм исправления стираний. В работе приведены нижние оценки на корректирующую способность (долю гарантированно исправимых ошибок и стираний соответственно) при декодировании нерегулярного МПП-кода по алгоритмам с малой сложностью (исправления ошибок и стираний соответственно). Новые оценки получены в результате анализа представления нерегулярного МПП-кода в виде графа Таннера. В работе представлены численные результаты, полученные по новым оценкам, и сравнение с лучшими известными оценками для различных параметров регулярного МПП-кода. Для нерегулярного МПП-кода численные значения получены впервые.

КЛЮЧЕВЫЕ СЛОВА: МПП-код, нерегулярный, двоичный, алгоритм декодирования, итеративный, с малой сложностью, ошибки, стирания.

1. ВВЕДЕНИЕ

Асимптотические корректирующие свойства кодов с малой плотностью проверок (МПП) Галлагера [1] при передаче по двоичному стирающему каналу были впервые исследованы в работе [2], где было показано, что существует такой МПП-код Галлагера, который гарантированно исправляет линейную долю стираний при декодировании по алгоритму со сложностью $O(n \log n)$, где n – длина МПП-кода. Затем в работе [3] были разработаны методы, основанные на производящих функциях, для оценки доли гарантированно исправимых ошибок при декодировании МПП-кода по алгоритму с малой сложностью. В работе [4] был получен результат, аналогичный [2], для МПП-кода, проверочная матрица которого составлена из перестановочных матриц. А в работе [5] комбинаторными методами была получена более простая для вычисления аналитическая оценка корректирующей способности МПП-кода в канале с ошибками, но численные результаты оказались в большинстве случаев не лучше результатов, полученных по старой оценке [3]. При этом стоит отметить, что в работе [5] рассматривался алгоритм отличный от алгоритма из [3]. В данной работе мы рассматриваем несколько модифицированные для нерегулярных МПП-кодов алгоритмы из работ [2, 3].

МПП-код с компонентным кодом Хэмминга (Х-МПП-код) был рассмотрены в работе [7]. Затем кодовое расстояние и "мягкое" декодирование Х-МПП-кодов было исследовано в работах [8] и [9]. В работе [10] было показано, что ансамбль Х-МПП-кодов содержит коды с минимальным кодовым расстоянием, почти достигающим границу Варшамова–Гилберта. Затем

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 13-01-12458 офи_м2, № 14-07-31197 мол_а, № 14-01-93108 НЦНИЛ_а.

путем обобщения методов, разработанных в [3], в работах [6, 11] и [12] были получены результаты для X-МПП-кодов и q-ичных МПП-кодов, аналогичные результату из [3]. В работе [13] были обобщены методы из [3] для двоичного стирающего канала. Затем в работе [15] были разработаны методы оценки в графе Таннера числа ребер с заданными свойствами, что позволило получить новую оценку на долю гарантированно исправимых ошибок, которая немного улучшает оценку из [3] и значительно улучшает оценку из [6, 11].

В отличие от предыдущих работ в работе [14] был рассмотрен ансамбль нерегулярный МПП-кодов и предложен новый алгоритм декодирования. Было показано, что для любой скорости кода $0 < R < 1$, любого $0 < \epsilon < 1$ и достаточно большого n существует линейный код и алгоритм декодирования, который с вероятностью $1-\mathcal{O}\left(n^{-3/4}\right)$ исправляют любую случайную комбинацию стираний кратности $(1-R)(1-\epsilon)$ за время пропорциональное $n \ln 1/\epsilon$.

В данной работе частично используются идеи, методы и подходы, разработанные в работах [13, 15, 16]. В работе рассматривается нерегулярный МПП-код и итеративные алгоритмы исправления ошибок и стираний с малой сложностью, аналогичные алгоритмам из [2, 3]. Впервые получены оценки как на долю ошибок, так и на долю стираний, гарантированно исправимых нерегулярным МПП-кодом. Численные результаты, полученные по предложенное оценке для различных параметров регулярного МПП-кода, достигают аналогичных значений известных ранее лучших оценок [13, 15]. Численные результаты для нерегулярных МПП-кодов представлены впервые.

2. МПП-КОД

Удобно определять МПП-код, используя его представление в виде графа Таннера [17]. Граф Таннера представляет собой двудольный граф, где вершины на левой стороне соответствуют битовым символам кодового слова (вершины-символы), а вершины на правой стороне соответствуют проверочным соотношениям (вершины-проверки). В данной работе рассматривается ансамбль нерегулярных МПП-кодов. Он определяется двумя следующими векторами:

$$\tilde{\lambda} = \left(\tilde{\lambda}_2, \ldots, \tilde{\lambda}_c\right),$$

$$\tilde{\rho} = \left(\tilde{\rho}_1, \ldots, \tilde{\rho}_d\right),$$

где $\tilde{\lambda}_l$ – доля вершин-символов со степенью l и $\tilde{\rho}_l$ – доля вершин-проверок со степенью l. Для удобства введем также следующие полиномы:

$$\tilde{\lambda}(x) = \sum_{l=2}^{c} \tilde{\lambda}_l x^{l-1},$$

$$\tilde{\rho}(x) = \sum_{l=2}^{d} \tilde{\rho}_l x^{l-1}.$$

Пусть E обозначает общее количество ребер в рассматриваемом графе, n обозначает количество вершин-символов (длина кода), а m – количество вершин-проверок (общее количество проверочных соотношений). Тогда $n\tilde{\lambda}_l l$ равно количеству ребер, исходящих из вершин-символов со степенью l, а $m\tilde{\rho}_l l$ – количеству ребер, исходящих из вершин-проверок со степенью l. Следовательно,

$$n = \frac{E}{\sum\limits_{l=2}^{c} \tilde{\lambda}_l l} = \frac{E}{1 + \tilde{\lambda}'(1)},$$

$$m = \frac{E}{\sum\limits_{l=2}^{d} \tilde{\rho}_l l} = \frac{E}{1 + \tilde{\rho}'(1)},$$

где $\tilde{\lambda}'(1)$ и $\tilde{\rho}'(1)$ – значения производных функций $\tilde{\lambda}(x)$ и $\tilde{\rho}(x)$ по переменной x, вычисленные в точке $x = 1$.

Каждой вершине-символу со степенью i ставим в соответствие i гнезд-символов (мест подсоединения ребер к данной вершине-символу). Аналогично, каждой вершине-проверке со степенью i ставим в соответствие i гнезд-проверок. Общее количество гнезд-символов равно общему количеству гнезд-проверок и равно общему количеству ребер E. Ансамбль двудольных графов определяется равновероятным выбором перестановки π длины E. Для каждого $1 \le i \le E$ мы соединяем вершину-символ, соответствующую iому гнезду-символу, с вершинной-проверкой, соответствующей π_iому гнезду-проверке. Следует отметить, что при таком построение две вершины может соединять более чем одно ребро. Тогда проверочная матрица $\mathbf{H}$, соответствующая полученному двудольному графу, строится следующим образом. Элемент $\mathbf{H}_{i,j}$ матрицы, соответствующий iой вершине-символу и jой вершине-проверке, равен “1”, если нечетное число ребер соединяет эти две вершины, иначе равен “0”.

Скорость R' каждого кода в ансамбле удовлетворяет неравенству $R' \ge R$, где

$$R = 1 - \frac{m}{n} = 1 - \frac{\sum\limits_{l=2}^{c} \tilde{\lambda}_l l}{\sum\limits_{l=2}^{d} \tilde{\rho}_l l} = 1 - \frac{1 + \tilde{\lambda}(1)}{1 + \tilde{\rho}'(1)}$$

конструктивная скорость кода (равенство достигается только тогда, когда проверочная матрица имеет полный ранг, а соответствующий двудольный граф не имеет ребер кратности большей чем один).

Частный случай ансамбля нерегулярных МПП-кодов, описанного выше, получается, если все вершины-символы имеют одинаковую степень c, а вершины-проверки имеют одинаковую степень d. В таком случае ансамбль называется ансамблем регулярных МПП-кодов и $R = 1 - c/d$, т.к. $nc = md$.

3. ИСПРАВЛЕНИЕ ОШИБОК

3.1. Алгоритм декодирования

В данной работе мы рассматриваем мажоритарный алгоритм декодирования МПП-кода, аналогичный алгоритму из в [3, 15], основная идея которого заключается в уменьшении веса синдрома МПП-кода на каждой итерации алгоритма декодирования. На каждой итерации мы последовательно инвертируем символы, каждый из которых соответствует вершине-символу со степенью l, которая соединена с более чем $l/2$ вершинами-проверками (компонентными кодами), соответствующими невыполненным проверками на четность. Ясно, что при инвертировании такого символа вес синдрома уменьшится, т.к. более чем $l/2$ проверок станут выполненными.

Рассмотрим теперь мажоритарный алгоритм декодирования $\mathcal{A}$ нерегулярного МПП-кода, каждая итерация i, $i = 1, 2, \ldots, i_{max}$ состоит из следующих двух шагов:

1. последовательно рассматриваем каждый символ декодируемой последовательности $\mathbf{r}^{(i)}$, где $\mathbf{r}^{(1)}$ – принятая последовательность:
   – определяем количество невыполненных проверок, соответствующих вершинам-проверкам, соединенным с вершиной-символом, соответствующей рассматриваемому символу;

- инвертируем текущий символ, если вершина-символ со степенью l, соответствующая данному символу, соединена с более чем $l/2$ вершинами-проверками, соответствующими невыполненным проверкам;
- переходим к следующему символу;

2. рассматриваем обновленную последовательность $\mathbf{r}^{(i)}$, полученную на предыдущем шаге:
   - если синдром МПП-кода для обновленной последовательности стал нулевым (т.е. коды-компоненты с невыполненными проверками отсутствуют), то возвращаем обновленную (исправленную) последовательность $\mathbf{r}^{(i)}$, устанавливаем флаг успешного декодирования и завершаем выполнение алгоритма;
   - иначе, если вес синдрома для обновленной последовательности уменьшился, переходим к следующей $i+1$ итерации с последовательностью $\mathbf{r}^{(i+1)}$, которая полностью совпадает с обновленной последовательностью $\mathbf{r}^{(i)}$;
   - иначе устанавливаем флаг отказа от декодирования и завершаем выполнение алгоритма декодирования.

Замечание 1. Важно отметить, что в соответствии с описанием алгоритма $\mathcal{A}$ новые дополнительные ошибки могут быть добавлены к последовательности во время декодирования. Другими словами, алгоритм $\mathcal{A}$ не гарантирует, что только ошибочные символы будут инвертированы (исправлены), что может привести к добавлению новых ошибок.

Обозначим l_i степень iой вершины-символа и e_i количество вершин-проверок, соответствующих невыполненным проверкам и соединенных с iой вершиной-символом. Тогда условие инвертирования символа может быть записано следующим образом:

$$e_i > l_i/2. \tag{1}$$

Получим следующее условие, при котором гарантируется, что для заданного МПП-кода и заданной комбинации ошибок кратности W гарантированно найдется такой символ, замена (инвертирование) которого уменьшит количество невыполненных проверок (вес синдрома).

Лемма 1. *Для существования по крайней мере одного символа, который будет заменен алгоритмом $\mathcal{A}$ в течение одной итерации декодирования заданного МПП-кода, достаточно выполнения условия*

$$E_W = \sum_{j=1}^{W} e_{i_j} > \frac{1}{2}\sum_{j=1}^{W} l_{i_j}, \tag{2}$$

где W – количество ошибок в принятой последовательности, а i_1, i_2, …, i_W – номера позиций ошибочных символов.

Доказательство. Условие (2) гарантирует только, что условие (1) выполняется хотя бы для одного символа. Предположим, что условие (1) не выполняется ни для одного из W ошибочных символов, т.е.

$$e_i < l_i/2, \forall j = 1, W.$$

Тогда

$$\sum_{j=1}^{W} e_{i_j} < \frac{1}{2}\sum_{j=1}^{W} l_{i_j}.$$

Противоречие.

Замечание 2. Заметим, что условие (2) гарантирует лишь то, что среди всех n символов последовательности найдется символ, удовлетворяющий условию (1). При этом не гарантируется, что найденный символ будет непременно ошибочным. При замене (инвертировании) правильного (не ошибочного) символа алгоритмом $\mathcal{A}$ будет внесена ошибка, но при этом количество невыполненных проверок будет уменьшено.

Замечание 3. Именно путем оценки вероятности выполнения условия (2) мы получим оценку на долю гарантированно исправимых ошибок, представленную в следующей разделе.

3.2. Оценка доли гарантированно исправимых ошибок

Введем основное уравнение, необходимое для формулировки последующих теорем:

$$\max_{0\le\beta\le\gamma}\left\{\tau\left(\omega,\beta\right)+\theta\left(\alpha,\beta,\gamma\right)-\gamma h\left(\frac{\beta}{\gamma}\right)\right\}=0, \tag{3}$$

где $h\left(\frac{\beta}{\gamma}\right)=-\frac{\beta}{\gamma}\log_2\frac{\beta}{\gamma}-\left(1-\frac{\beta}{\gamma}\right)\log_2\left(1-\frac{\beta}{\gamma}\right)$ – функция двоичной энтропии, $\gamma=\sum_i i\tilde{\lambda}$ – средняя степень вершин-символов, $\tau\left(\omega,\beta\right)$ определяется следующим образом

$$\tau\left(\omega,\beta\right)=\min_{\substack{x>0\\y>0}}\left\{\log_2\left(1+xy\tilde{\lambda}\left(y\right)\right)-\omega\log_2 x-\beta\log_2 y\right\}$$

и $\theta\left(\alpha,\beta,\gamma\right)$ имеет следующий вид

$$\theta\left(\alpha,\beta,\gamma\right)=\min_{\substack{x>0\\0<y<1}}\left\{(1-R)\log_2\psi\left(\gamma,x,y\right)-\beta\log_2 x-\alpha\beta\log_2 y\right\},$$

где α и $\psi\left(\gamma,x,y\right)$ определяются для каждой теоремы отдельно.

Сформулируем следующую теорему.

Теорема 1. *Пусть ω_t минимальный положительный корень уравнения* (3)*, для которого $\alpha=1/2$ (в соответствии с условием* (2)*), а $\psi\left(\gamma,x,y\right)$ имеет следующий вид:*

$$\begin{aligned}\psi\left(\gamma,x,y\right)=\psi\left(x,y\right)=\frac{1}{2}\left(\left(1+xy\right)\tilde{\rho}\left(1+xy\right)-\left(1-xy\right)\tilde{\rho}\left(1-xy\right)\right.\\ \left.+\left(1+x\right)\tilde{\rho}\left(1+x\right)+\left(1-x\right)\tilde{\rho}\left(1-x\right)\right).\end{aligned}$$

Тогда существует (с вероятностью $p_n:\lim\limits_{n\to\infty}p_n=1$) такой нерегулярный МПП-код, заданный полиномами $\tilde{\lambda}\left(x\right)=\sum_{l=2}^{c}\tilde{\lambda}_l x^{l-1}$ и $\tilde{\rho}\left(x\right)=\sum_{l=2}^{d}\tilde{\rho}_l x^{l-1}$, который может исправить любую комбинацию ошибок кратности менее $\lfloor\omega_t n/2\rfloor$ при декодировании по алгоритму $\mathcal{A}$ со сложностью $\mathcal{O}\left(n\log n\right)$.

3.3. Численные результаты

В данном разделе представлены численные результаты, полученные по предложенной выше оценке для некоторых параметров нерегулярных МПП-кодов.

В Табл. 1 приведены численные результаты для нерегулярного МПП-кода со скоростью $R=1/2$ и для различных полиномов $\tilde{\lambda}\left(x\right)$ и $\tilde{\rho}\left(x\right)$. Видно, что предложенная нижняя граница достигает значений лучших ранее известных оценок для регулярных МПП-кодов [15]. Также можно заметить, что в нерегулярно случае полученные значения не превосходят значений,

Таблица 1. Доля гарантированно исправимых ошибок нерегулярным МПП-кодом со скоростью $R = 1/2$ и заданными полиномами $\tilde{\lambda}(x)$ и $\tilde{\rho}(x)$

$\tilde{\lambda}_5$	0	0.25	0	0	0	0
$\tilde{\lambda}_{10}$	1	0.5	0	0	0	0
$\tilde{\lambda}_{15}$	0	0.25	0	0.25	0	0
$\tilde{\lambda}_{20}$	0	0	1	0.5	0	0
$\tilde{\lambda}_{25}$	0	0	0	0.25	0	0.25
$\tilde{\lambda}_{30}$	0	0	0	0	1	0.5
$\tilde{\lambda}_{35}$	0	0	0	0	0	0.25
$\tilde{\rho}_{20}$	1	1	0	0	0	0
$\tilde{\rho}_{40}$	0	0	1	1	0	0
$\tilde{\rho}_{60}$	0	0	0	0	1	1
$\omega_t/2$	3.2e-4	9e-7	1.2e-3	1.1e-3	1.4e-3	1.4e-3

полученных для регулярного случая, но с ростом средней степени вершины-символа различие между регулярным и нерегулярным случаем уменьшается.

В Табл. 2 представлены численные результаты для случая нерегулярного МПП-кода со средней степенью вершины-символа равной 10. Можно заметить, что добавление вершин-символов с малой степенью приводи к уменьшению доли гарантированно исправимых стираний.

Таблица 2. Доля гарантированно исправимых ошибок нерегулярным МПП-кодом со скоростью $R = 1/2$ и фиксированными $\tilde{\lambda}_{30} = 0.5$ и $\tilde{\rho}_{60} = 1$

$\tilde{\lambda}_5$	0	0	0	0	0.0833	0.2727
$\tilde{\lambda}_{10}$	0	0	0	0.1667	0	0
$\tilde{\lambda}_{15}$	0	0	0.25	0	0	0
$\tilde{\lambda}_{20}$	0	0.3333	0	0	0	0
$\tilde{\lambda}_{25}$	0.4167	0	0	0	0	0
$\tilde{\lambda}_{30}$	0.5	0.5	0.5	0.5	0.5	0.5
$\tilde{\lambda}_{35}$	0	0	0	0	0.4167	0
$\tilde{\lambda}_{40}$	0	0	0	0.3333	0	0
$\tilde{\lambda}_{45}$	0	0	0.25	0	0	0
$\tilde{\lambda}_{50}$	0	0.1667	0	0	0	0
$\tilde{\lambda}_{55}$	0.0833	0	0	0	0	0
$\tilde{\lambda}_{60}$	0	0	0	0	0	0.2273
$\omega_0/2$	1.4e-3	1.4e-3	1.3e-3	1.1e-3	1.1e-5	8e-7

4. ИСПРАВЛЕНИЕ СТИРАНИЙ

4.1. Алгоритм декодирования

Рассмотрим передачу кода с проверкой на четность по двоичному стирающему каналу. Известно, что кодовое расстояние кода с проверкой на четность равно $\Delta_0 = 2$. Следовательно, код с проверкой на четность гарантированно исправляет любое одно стирание ($\Delta_0 - 1 = 1$). Ясно, что переданное двоичное значение стертого символа равно сумме по модулю два не стертых символов.

Теперь рассмотрим алгоритм декодирования $\mathcal{B}$ МПП-кода с компонентным кодом с проверкой на четность. Данный алгоритм аналогичен алгоритмам из работ [2] и [13]. Основная идея алгоритма заключается в том, чтобы на каждой итерации алгоритма найти хотя бы один компонентный код (код с проверкой на четность) с исправимой комбинацией стираний (с одним стиранием). В таком случае количество стираний в декодируемой последовательности будет уменьшаться с каждой итерацией. И в силу конечности количества стираний в принятой последовательности все они будут исправлены за конечное число шагов.

Каждая итерация декодирования i, $i = 1, 2, \ldots, i_{\max}$, итеративного алгоритма $\mathcal{B}$ состоит из следующих двух шагов:

1. последовательно рассматриваем стертые символы декодируемой последовательности $\mathbf{r}^{(i)}$, где $\mathbf{r}^{(1)}$ – принятая последовательность $\mathbf{r}$:
   - определяем компонентные коды, содержащие текущий стертый символ (вершины-проверки, соединенные с текущей вершиной-символом);
   - заменяем стирание восстановленным двоичным значением, если хотя бы одна проверка, полученная на предыдущем шаге, содержит исправимую комбинацию стираний (одно текущее стираний);
   - переходим к следующему стертому символу в декодируемой последовательности;
2. рассматриваем обновленную последовательность $\mathbf{r}^{(i)}$, полученную на предыдущем шаге:
   - если обновленная последовательность $\mathbf{r}^{(i)}$ не содержит стираний, алгоритм возвращает обновленную (исправленную) последовательность $\mathbf{r}^{(i)}$, устанавливает флаг успешного декодирования и останавливает исполнение;
   - в противном случае если количество стираний в обновленной последовательности уменьшилось (некоторые из стираний были исправлены), то алгоритм переходит к следующей итерации $i + 1$ с декодируемой последовательностью $\mathbf{r}^{(i+1)}$, которая совпадает с обновленной последовательностью $\mathbf{r}^{(i)}$;
   - иначе алгоритм устанавливает флаг отказа от декодирования и останавливает выполнение.

Важно отметить, что в отличие от исправление ошибок исправление стираний не вносит новые стирание в декодируемую последовательность и позиции всех стираний известны. Следовательно, чтобы исправить все стираний проверочные соотношения с исправимыми комбинациями стираний должны существовать на каждой итерации алгоритма. Обозначим e_i количество вершин-проверок, соответствующих проверочным соотношениям с исправимой комбинацией стираний и соединенных с iой вершиной-символом. Тогда текущий стертый iый символ будет исправлен, если $e_i > 0$. Обозначим l_i степень iой вершины-символа и сформулируем следующее условие, при котором для заданного МПП-кода и комбинации стираний кратности W найдется компонентный код с исправимой комбинацией стираний.

Лемма 2. *Для существования по крайней мере одного компонентного кода с исправимой комбинацией стираний в течение одной итерации алгоритмом $\mathcal{B}$ заданного МПП-кода, достаточно выполнения условия*

$$E_W = \sum_{j=1}^{W} e_{i_j} > \alpha \sum_{j=1}^{W} l_{i_j}, \tag{4}$$

где W – количество стираний в декодируемой последовательности, i_1, i_2, …, i_W – позиции стертых символов и α – некоторая маленькая положительная константа, $0 \le \alpha \le 1$.

Замечание 4. Константа α имеет смысл линейной доли проверочных соотношений с исправимыми комбинациями стираний. Эта константа влияет на оценку сложности декодирования.

Если $\alpha > 0$, то аналогично [2, 13] можно показать, что сложность алгоритма $\mathcal{B}$ составляет $\mathcal{O}(n \log n)$.

Замечание 5. Оценивая вероятность выполнения условия (4), мы получим нижнюю оценку на долю гарантированно исправимых стираний, представленную в следующей секции.

4.2. Оценка доли гарантированно исправимых стираний

Теорема 2. *Пусть ω_τ минимальный положительный корень уравнения* (3)*, для которого $\alpha > 0$ – произвольная малая константа (в соответствии с условием* (4)*, линейная доля проверочных соотношений ровно с одним стиранием), а $\psi(\gamma, x, y)$ имеет следующий вид:*

$$\psi(\gamma, x, y) = \gamma x (y - 1) + (1 + x)\,\tilde{\rho}(1 + x).$$

Тогда существует (с вероятностью $p_n : \lim\limits_{n\to\infty} p_n = 1$) такой нерегулярный МПП-код, заданный полиномами $\tilde{\lambda}(x) = \sum_{l=2}^{c} \tilde{\lambda}_l x^{l-1}$ и $\tilde{\rho}(x) = \sum_{l=2}^{d} \tilde{\rho}_l x^{l-1}$, который может исправить любую комбинацию стираний кратности менее $\lfloor \omega_\tau n \rfloor$ при декодировании по алгоритму $\mathcal{B}$ со сложностью $\mathcal{O}(n \log n)$.

4.3. Численные результаты

В данной секции представлены численные результаты, полученные по предложенной выше оценке для некоторых параметров нерегулярных МПП-кодов.

В Табл. 3 приведены численные результаты для нерегулярного МПП-кода со скоростью $R = 1/2$ и для различных полиномов $\tilde{\lambda}(x)$ и $\tilde{\rho}(x)$. Видно, что предложенная нижняя граница достигает значений лучших ранее известных оценок для регулярных МПП-кодов [13]. Также можно заметить, что в нерегулярно случае полученные значения не превосходят значений, полученных для регулярного случая, но с ростом средней степени вершины-символа различие между регулярным и нерегулярным случаем уменьшается.

Таблица 3. Доля гарантированно исправимых стираний нерегулярным МПП-кодом со скоростью $R = 1/2$ и заданными полиномами $\tilde{\lambda}(x)$ и $\tilde{\rho}(x)$

$\tilde{\lambda}_5$	0	0.25	0	0	0	0
$\tilde{\lambda}_{10}$	1	0.5	0	0	0	0
$\tilde{\lambda}_{15}$	0	0.25	0	0.25	0	0
$\tilde{\lambda}_{20}$	0	0	1	0.5	0	0
$\tilde{\lambda}_{25}$	0	0	0	0.25	0	0.25
$\tilde{\lambda}_{30}$	0	0	0	0	1	0.5
$\tilde{\lambda}_{35}$	0	0	0	0	0	0.25
$\tilde{\rho}_{20}$	1	1	0	0	0	0
$\tilde{\rho}_{40}$	0	0	1	1	0	0
$\tilde{\rho}_{60}$	0	0	0	0	1	1
ω_τ	6.2e-2	6.1e-2	4.6e-2	4.5e-2	3.6e-2	3.6e-2

В Табл. 4 представлены численные результаты для случая нерегулярного МПП-кода со средней степенью вершины-символа равной 10. Можно заметить, что добавление вершин-символов с малой степенью приводи к уменьшению доли гарантированно исправимых стираний.

Таблица 4. Доля гарантированно исправимых стираний нерегулярным МПП-кодом со скорость $R = 1/2$ и фиксированными $\tilde{\lambda}_{10} = 0.5$ и $\tilde{\rho}_{20} = 1$

$\tilde{\lambda}_5$	0.25	0.3333	0.375	0.4	0.4167	0.4286
$\tilde{\lambda}_{10}$	0.5	0.5	0.5	0.5	0.5	0.5
$\tilde{\lambda}_{15}$	0.25	0	0	0	0	0
$\tilde{\lambda}_{20}$	0	0.1667	0	0	0	0
$\tilde{\lambda}_{25}$	0	0	0.125	0	0	0
$\tilde{\lambda}_{30}$	0	0	0	0.1	0.5	0.5
$\tilde{\lambda}_{35}$	0	0	0	0	0.0833	0
$\tilde{\lambda}_{40}$	0	0	0	0	0	0.0714
ω_τ	6.1e-2	5.9e-2	5.4e-2	4.9e-2	4.6e-2	4.2e-2

5. ДОКАЗАТЕЛЬСТВО ОСНОВНЫХ РЕЗУЛЬТАТОВ

Для простоты изложения и понимания рассмотрим сначала доказательство Теоремы 2.

Доказательство. Пусть $\lfloor p(x) \rfloor_i$ означает коэффициент при x^i в полиноме $p(x)$:

$$p(x) = \sum_i \lfloor p(x) \rfloor_i x^i.$$

Теперь обозначим $t(W, j)$ количество способов выбрать W вершин-символов так, чтобы из них выходило ровно j ребер. Мы может записать это следующим образом:

$$t(W, j) = \left\lfloor \prod_k \left(1 + xy^k\right)^{\tilde{\lambda}_k n} \right\rfloor_{W,j}.$$

Далее обозначим $q(j, i)$ количество способов выбрать j гнезд-проверок так, чтобы точно i из них принадлежали проверочным соотношениям с исправимой комбинацией стираний (с один стиранием), а все остальные – проверочным соотношениям с неисправимой комбинацией стираний (с двумя и более стираниями) или без стираний. Запишем это следующим образом:

$$q(j, i) = \left\lfloor \prod_k \left(g_1(xy, k) + g_0(x, k)\right)^{\tilde{\rho}_k m} \right\rfloor_{j,i},$$

где $g_1(xy, k)$ и $g_0(x, k)$ – производящие функции количества исправимых комбинаций стираний и неисправимых комбинаций стираний для кода с проверкой на четность соответственно:

$$g_1(xy, k) = kxy, g_0(x, k) = (1 + x)^k - kx.$$

Тогда вероятность выбрать W вершин-символов так, чтобы точно j ребер выходило из них и выбрать j гнезд-проверок так, чтобы точно i из них принадлежали вершинам-проверками, соответствующим проверочным соотношениям с исправимой комбинацией стираний, в нерегулярном МПП-коде, заданном соответствующими полиномами, может быть записана следующим образом:

$$P(E_W = i, j) = \frac{t(W, j)}{\binom{n}{W}} \frac{q(j, i)}{\binom{E}{j}}.$$

Следовательно, мы можем записать

$$P\left(E_W \le \alpha j, j\right) = \sum_{i=0}^{\alpha j} P\left(E_W = i, j\right) = \frac{t\left(W, j\right)}{\binom{n}{W}} \frac{\sum\limits_{i=0}^{\alpha j} q\left(j, i\right)}{\binom{E}{j}}$$

Откуда вероятность выбрать W вершин-символов так, чтобы условие (4) не выполнялось, определяется выражением:

$$P\left(E_W \le \alpha \sum_{j=1}^{W} l_{i_j}\right) = \sum_{j} \frac{t\left(W, j\right)}{\binom{n}{w}} \frac{\sum\limits_{i=0}^{\alpha j} q\left(j, i\right)}{\binom{E}{j}}$$

Рассмотрим вероятность найти код, для которого условие (4) не выполняется хотя бы для одной комбинации стираний кратности W. Если эта вероятность меньше 1, то существует код, для которого условие (4) выполняется для любой комбинации стираний кратности W:

$$\binom{n}{W} P\left(E_W \le \alpha \sum_{j=1}^{W} l_{i_j}\right) \le 1.$$

Для того, чтобы найти максимальную кратность комбинации стираний, мы должны решить уравнение:

$$\binom{n}{W} P\left(E_W \le \alpha \sum_{j=1}^{W} l_{i_j}\right) = 1. \tag{5}$$

Рассмотрим следующую оценку сверху:

$$P\left(E_W \le \alpha \sum_{j=1}^{W} l_{i_j}\right) \le E \max_{0 \le j \le E} \left\{ \frac{t\left(W, j\right)}{\binom{n}{W}} \frac{\sum\limits_{i=0}^{\alpha j} q\left(j, i\right)}{\binom{E}{j}} \right\}$$

Также легко получить следующие оценки:

$$t\left(W, j\right) \le \min_{\substack{x>0 \\ y>0}} \left\{ \frac{\prod\limits_{k} \left(1 + xy^k\right)^{\tilde{\lambda}_k n}}{x^W y^j} \right\},$$

$$\sum_{i=0}^{\alpha j} q\left(j, i\right) \le \min_{\substack{x>0 \\ 0<y<1}} \left\{ \frac{\prod\limits_{k} \left(g_1\left(xy, k\right) + g_0\left(x, k\right)\right)^{\tilde{\rho}_k m}}{x^j y^{\alpha j}} \right\}.$$

Пусть $W = \omega n$, $1 \le \omega \le 1$, и $j = \beta n$, $0 \le \beta \le \gamma$. Тогда предел отношения логарифма полученных оценок к длине кода n, когда $n \to \infty$, может быть записан следующим образом:

$$\tau\left(\omega, \beta\right) = \lim_{n \to \infty} \frac{\log_2 t\left(\omega n, \beta n\right)}{n} \le \min_{\substack{x>0 \\ y>0}} \left\{ \log_2 \left(\prod_{k} \left(1 + xy^k\right)^{\tilde{\lambda}_k} \right) - \omega \log_2 x - \beta \log_2 y \right\}$$

$$= \min_{\substack{x>0 \\ y>0}} \left\{ \sum_{k} \tilde{\lambda}_k \log_2 \left(1 + xy^k\right) - \omega \log_2 x - \beta \log_2 y \right\}$$

Поскольку $\sum\limits_k \tilde{\lambda}_k = 1$ по условию, а логарифм – выпуклая функция, то

$$\sum_k \tilde{\lambda}_k \log_2\left(1+xy^k\right) \le \log_2\left(\sum_k \tilde{\lambda}_k\left(1+xy^k\right)\right).$$

Следовательно,

$$\tau(\omega,\beta) \le \min_{\substack{x>0\\y>0}}\left\{\log_2\left(1+xy\tilde{\lambda}(y)\right) - \omega\log_2 x - \beta\log_2 y\right\}.$$

Аналогично,

$$\theta(\gamma,\alpha,\beta) = \lim_{n\to\infty}\frac{\log_2\sum\limits_{i=0}^{\alpha\beta n} q(\beta n, i)}{n} \le \min_{\substack{x>0\\0<y<1}}\left\{(1-R)\log_2\psi(\gamma,x,y) - \beta\log_2 x - \alpha\beta\log_2 y\right\},$$

где $\psi(\gamma,x,y) = \gamma x(y-1) + (1+x)\,\tilde{\rho}(1+x)$.

Также следует отметить, что

$$\binom{E}{j} \sim 2^{\gamma n h\left(\frac{\beta}{\gamma}\right)}.$$

Подставляя найденные оценки в (5) и устремляя $n\to\infty$, мы получим

$$\max_{0\le\beta\le\gamma}\left\{\tau(\omega,\beta) + \theta(\alpha,\beta,\gamma) - \gamma h\left(\frac{\beta}{\gamma}\right)\right\} = 0,$$

что завершает доказательство.

Замечание 6. Для доказательства Теоремы 1 достаточно положить $\alpha = 1/2$ в соответствии с условием (2), а в качестве производящих функций $g_1(xy,k)$ и $g_0(x,k)$ рассмотреть производящие функции комбинаций ошибок, обнаруживаемых (нечетное количество ошибок) и не обнаруживаемых (кодовые слова) двоичным кодом с проверкой на четность соответственно:

$$g_1(xy,k) = \frac{(1+xy)^k - (1-xy)^k}{2}, g_0(x,k) = \frac{(1+x)^k + (1-x)^k}{2}.$$

Как отмечалось выше при декодировании по алгоритму $\mathcal{A}$ новые ошибки могут быть добавлены в последовательность. Следовательно, в процессе декодирования количество ошибок может превысить $\lfloor\omega_t n\rfloor$. В этом случае нельзя гарантировать, что условие (2) выполняется, а значит комбинация ошибок может быть неисправимой. Можно показать аналогично работе [3], что достаточно взять комбинацию ошибок с начальной кратностью не превосходящей $\lfloor\omega_t n/2\rfloor$ для того, чтобы в процессе декодирования кратность ошибок в декодируемой последовательности не превысило $\lfloor\omega_t n\rfloor$.

Замечание 7. Все последующие рассуждения и доказательства, необходимые для полного доказательства Теоремы 1 и Теоремы 2 полностью аналогичны [13, 15].

6. ЗАКЛЮЧЕНИЕ

В работе рассмотрены нерегулярные МПП-коды и алгоритмы декодирования как для исправления ошибок, так и для исправления стираний. Для каждого алгоритма декодирования получена оценка снизу на долю гарантированной исправимых ошибок и стираний соответственно. Показано, что полученные оценки достигают значения лучших известных оценок для регулярных МПП-кодов. Для нерегулярных МПП-кодов оценки получены впервые, показано что для нерегулярных МПП-кодов значения оценки не превосходят значения оценки для регулярных МПП-кодов с той же скоростью, при этом значения оценки для нерегулярных МПП-кодов уменьшаются с увеличением доли вершин-символов с малой степенью и приближаются к значениям оценки для регулярных МПП-кодов с ростом средней степени вершины-символа. Представленные в данной работе оценки могут быть обобщены на случай нерегулярных qичных МПП-кодов [18, 19], а также могут быть использованы для выбора, оптимизации и оценки корректирующей способности кодовых конструкций, основанных на нерегулярных МПП-кодах, для построения систем связи будущих поколений [20–22].

СПИСОК ЛИТЕРАТУРЫ

1. Галлагер Р. Дж. *Коды с малой плотностью проверок на четность*. М.: Мир, 1966. (Gallager R. G. *Low-Density Parity-Check Codes.* Cambridge, MA: MIT Press, 1963.)

2. Зяблов В. В., Пискер М. С. Сложность декодирования низкоплотностных кодов при передаче по каналу со стираниями. *Пробл. передачи информ.*, 1974, т. 10, № 1, стр. 15–28.

3. Зяблов В. В., Пинскер М. С. Оценка сложности исправления ошибок низкоплотностными кодами Галлагера. *Пробл. передачи информ.*, 1975, т. 11. № 1. стр. 23–26.

4. Зигангиров Д. К., Зигангиров К. Ш. Декодирование низкоплотностных кодов с проверочными матрицами, составленными из перестановочных матриц, при передаче по каналу со стираниями. *Пробл. передачи информ.*, 2006, т. 42, № 2, стр. 44–52.

5. Зигангиров К. Ш., Пусане А. Е., Зигангиров Д. К., Костелло Д. Дж., О корректирующей способности кодов с малой плотностью проверок. *Пробл. передачи информ.*, 2008, т. 44, № 3, стр. 50–62.

6. Zyablov V., Loncar M., Johannesson R., Rybin P. On the Erasure-Correcting Capabilities of Low-Complexity Decoded LDPC Codes with Constituent Hamming Codes. *Proc. 11th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT08)*, 2008, pp. 338–347.

7. Lentmaier M., Zigangirov K. Iterative Decoding of Generalized Low-Density Parity-Check Codes. *Proc. IEEE Int. Symposium on Inform. Theory*, 1998, pp. 149.

8. Lentmaier M., Zigangirov K. On Generalized Low-Density Parity-Check Codes Based on Hamming Component Codes. *IEEE Commun. Lett.*, 1999, vol. 3, no. 8, pp. 248–250.

9. Boutros J., Pothier O., Zemor G. Generalized Low Density (Tanner) Codes. *Proc. IEEE Int. Conference on Communications*, 1999, pp. 441–445.

10. Stiglmayr S., Zyablov V. Asymptotically Good Low-Density Codes Based on Hamming Codes. *Proc. XI Int. Symposium on Problems of Redundancy in Information and Control Systems*, 2007, pp. 98–103.

11. Зяблов В. В., Йоханнессон Р., Лончар М. Просто декодируемые коды с малой плотностью проверок на основе кодов Хэмминга. *Пробл. передачи информ.*, 2009, т. 45, № 2, стр. 25–40.

12. Фролов А. А., Зяблов В. В. Асимптотическая оценка доли ошибок, исправляемых q-ичными МПП-кодами. *Пробл. передачи инфом.*, 2010, т. 46, № 2, стр. 47–65.

13. Зяблов В. В., Рыбин П. С. Исправление стираний кодами с малой плотностью проверок. *Пробл. передачи информ.*, 2009, т. 45, № 3, стр. 15–32.

14. Luby M. G., Mitzenmacher M., Shokrollahi M. A., Spielman D. A. Efficient Erasure Correcting Codes. *IEEE Trans. Inform. Theory*, 2001, vol. 47, no. 2, pp. 569–584.

15. Зяблов В. В., Рыбин П. С. Анализ связи свойств МПП-кодов и графа Таннера. *Пробл. передачи информ.*, 2012, т. 48, № 4, стр. 3–29.

16. Burshtein D., Miller G. Asymptotic Enumeration Methods for Analyzing LDPC Codes. *IEEE Trans. Inform. Theory*, 2004, vol. 50, no. 6, pp. 1115–1131.

17. Tanner R. A Recursive Approach to Low Complexity Codes. *IEEE Trans. Inform. Theory*, 1981, vol. 27, no. 5, pp. 533–547.

18. Frolov A. An Upper Bound on the Minimum Distance of LDPC Codes over GF(q). *Proc. IEEE Int. Symposium on Inform. Theory*, 2015, pp. 2885–2888.

19. Frolov A., Zyablov V. On the Multiple Threshold Decoding of LDPC codes over GF(q). *Proc. IEEE Int. Symposium on Inform. Theory*, 2015, pp. 2673–2677.

20. Иванов А. С., Ляхов А. И., Хоров Е. М. Аналитическая модель многошаговой передачи неординарного потока в беспроводных сетях с резервированиями канала, *Автомат. и телемех.*, 2015, № 7, стр. 52–68.

21. Каргин И. С., Хоров Е. М., Ляхов А. И. Математический метод оценки доли потерянных пакетов для многошагового маршрута в присутствии коррелированных помех. *Пробл. передачи информ.*, 2015, т. 51, № 3, стр. 105–111.

22. Кирьянов А., Куреев А., Ляхов А., Хоров Е. Анализ механизмов построения логической топологии в сетях MANET. *Информационные процессы*, 2015, т. 15, № 2, стр. 183–197.

Correcting capabilities of binary irregular LDPC code under low-complexity iterative decoding algorithm

Rybin P.S.

This paper deals with the irregular binary low-density parity-check (LDPC) codes and two iterative low-complexity decoding algorithms. The first one is the majority error-correcting decoding algorithm, and the second one is iterative erasure-correcting decoding algorithm. The lower bounds on correcting capabilities (the guaranteed corrected error and erasure fraction respectively) of irregular LDPC code under decoding (error and erasure correcting respectively) algorithms with low-complexity were represented. This lower bounds were obtained as a result of analysis of Tanner graph representation of irregular LDPC code. The numerical results, obtained at the end of the paper for proposed lower-bounds achieved similar results for the previously known best lower-bounds for regular LDPC codes and were represented for the first time for the irregular LDPC codes.

KEYWORDS: LDPC code, irregular, binary, decoding algorithm, iterative, low-complexity, errors, erasures.