Асимптотическая оценка доли ошибок, исправляемых q-ми МПП-кодами

А. А. Фролов
email: alexey.frolov@iitp.ru
Институт проблем передачи информации,
Российская академия наук,
Москва, Россия

В. В. Зяблов
email: zyablov@iitp.ru
Институт проблем передачи информации,
Российская академия наук,
Москва, Россия

Аннотация

Рассматривается ансамбль случайных q-ичных кодов с малой плотностью проверок. В качестве кода-компонента используются коды с q-ичной проверкой на четность с $d = 2$ и коды Рида-Соломона с $d = 3$. Предложен итеративный алгоритм декодирования с жестким решением, требующий числа итераций порядка логарифма от длины кода. Показано, что при таком алгоритме декодирования в ансамбле существуют коды, способные исправить линейно растущее с длиной кода число ошибок. Ослаблено условие на коэффициент вершинного расширения графа Таннера, соответствующего коду.

1 Введение

Коды с малой плотностью проверок (МПП-коды) были предложены Галлагером в [1], и характеризуются разреженной проверочной матрицей. Если проверочная матрица содержит j единиц в каждом столбце и k единиц в каждой строке, то такой код называется регулярным (j, k)-МПП-кодом. Графически код можно представить в виде двудольного

графа, в котором символьные вершины соответствуют столбцам проверочной матрицы (имеют степень j), а кодовые вершины соответствуют строкам и имеют степень k. Этот метод был предложен Таннером в [2]. Пример двудольного графа Таннера приведен на Рис. 1:

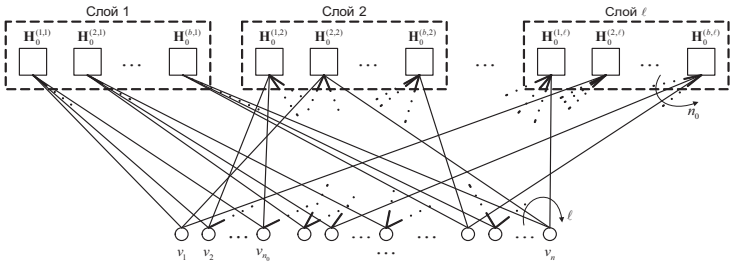

Рис. 1: Граф Таннера

Конструкция МПП-кодов Галлагера является частным случаем конструкции Таннера и получается из нее, если использовать код с двоичной проверкой на четность в качестве компонентного кода. Альтернативные конструкции МПП-кодов могут быть получены путем замены кодов с проверкой на четность другими блочными кодами с длинами, равными степеням вершин. В качестве компонентных кодов можно использовать коды Хэмминга [3, 4], БЧХ-коды или коды Рида-Соломона [5].

Впервые корректирующая способность МПП-кодов Галлагера для двоичносимметричного канала (ДСК) была рассмотрена в [6], где было доказано существование МПП-кодов, способных исправить линейно растущее с длиной кода число ошибок при сложности декодирования $O\left(n\log_2(n)\right)$, где n – длина кода. Здесь и далее под сложностью мы понимаем определение, данное в [7], т.е. минимальное число функциональных элементов в схеме, реализующей декодирование. Аналогичные результаты имеются для МПП-кодов с кодом Хэмминга в качестве компонентного [3].

В данной работе мы, развивая идеи работ [3] и [6], докажем , что среди случайных q-ичных кодов с кодом-компонентом с q-ичной проверкой на четность или с кодом компонентом Рида-Соломона с минимальным кодовым расстоянием $d = 3$ существуют коды, декодирование которых алгоритмом, имеющим малую сложность $(\mathcal{O}\left(n\log_2(n)\right))$, позволяет исправить линейно растущее с длиной кода число ошибок. То есть мы обобщим результаты, полученные в [6] для двоичных кодов с $d = 2$ и в [3] для двоичных кодов с $d = 3$ на случай q-ичных кодов. В этом и состоит наша основная задача.

Помимо этого, в данной работе предложено обобщение алгоритма, использовавшегося в [6], на случай q-ичных кодов.

По сравнению с работами [3, 6] ослаблено условие на коэффициент вершинного расширения графа Таннера, соответствующего МПП-коду.

Статья организована следующим образом: в §2 рассмотрена структура q-ичных МПП-кодов. В §3 предложен обобщенный алгоритм декодирования. В §4 сформулирован основной результат статьи. В §5 дается доказательство основного результата, которое разделено на три части. В §6 приведены полученные численные результаты.

2 Структура q-ичных МПП-кодов

Для построения проверочной матрицы q-ичного МПП-кода рассмотрим блочную диагональную матрицу $\mathbf{H}_b$, на главной диагонали которой находятся b проверочных матриц $\mathbf{H}_0$ кода-компонента.

$$\mathbf{H}_b = \begin{pmatrix} \mathbf{H}_0 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0 \end{pmatrix}_{bm \times bn_0}$$

где m – избыточность кода-компонента ($m = n_0 - k_0$).

В данной работе изучаются МПП-коды с кодом-компонентом с q-ичной проверкой на четность и с кодом компонентом Рида-Соломона ($d = 3$).

В первом случае $\mathbf{H}_0$ состоит из ненулевых элементов поля $GF(q)$:

$$\mathbf{H}_0 = \underbrace{\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{n_0}} \end{pmatrix}}_{n_0}$$

Во втором случае $\mathbf{H}_0$ – это просто проверочная матрица кода Рида-Соломона размерности $2 \times n_0,\ n_0 = q$.

Пусть $\phi(\mathbf{H}_b)$ обозначает матрицу, полученную из матрицы $\mathbf{H}_b$ произвольной перестановкой столбцов и умножением их на произвольные ненулевые элементы поля $GF(q)$. Тогда матрица размерности $lbm \times bn_0$, составленная из ℓ таких матриц, как слоев,

$$\mathbf{H} = \begin{pmatrix} \phi_1(\mathbf{H}_b) \\ \phi_2(\mathbf{H}_b) \\ \vdots \\ \phi_l(\mathbf{H}_b) \end{pmatrix}_{\ell bm \times bn_0}$$

является разреженной проверочной матрицей q-ного МПП-кода.
Определим ансамбль q-ичных МПП-кодов следующим образом:

О п р е д е л е н и е 1. Элементы ансамбля $\mathscr{E}(n_0, \ell, b)$ получаются путем независимого выбора перестановок $\pi_i, i = 1, 2, \ldots, \ell$ и ненулевых констант $c_{i,j},\ i = 1, 2, \ldots, \ell; j = 1, 2, \ldots, n$, на которые умножаются столбцы получившихся в результате перестановок проверочных матриц слоев.

З а м е ч а н и е 1. Отметим, что в отличие от определения ансамбля для двоичных кодов здесь добавляется умножение на константы, не равные нулю.

З а м е ч а н и е 2. Из определения ансамбля $\mathscr{E}(n_0, \ell, b)$ ясно, что длина кода $n = bn_0$. Дальше мы будем устремлять n к бесконечности, и это следует понимать следующим образом: $b \to \infty$, а параметр n_0 фиксирован.

Нижняя оценка скорости кода $C \in \mathscr{E}(n_0, \ell, b)$ получена в [2].

$$R \geqslant 1 - \frac{\ell b\,(n_0 - k_0)}{bn_0} = 1 - \ell\,(1 - R_0) \tag{1}$$

Равенство достигается в случае полного ранга матрицы $\mathbf{H}$. Из соотношения (1) получим ограничение для скорости кода-компонента:

$$R_0 > 1 - \frac{1}{\ell}$$

то есть чем больше количество слоев, тем выше должна быть скорость кода-компонента.

Для дальнейшего изложения нам также потребуется понятие обобщенного синдрома. Напомним, что синдром принятого вектора вычисляется следующим образом:

$$\mathbf{S} = \mathbf{r}\mathbf{H}^T$$

где $\mathbf{r}$ – это принятый вектор. $\mathbf{S}$ имеет размерность $1 \times \ell bm$.

Обобщенный синдром состоит из синдромов кодов компонентов (размерность синдрома кода-компонента – $1 \times m$).

$$\mathbf{S}_{generalized} = \begin{pmatrix} \mathbf{s}_1 & \mathbf{s}_2 & \ldots & \mathbf{s}_{lb} \end{pmatrix}$$

$$\mathbf{s}_i = \left(s_{(i,1)} s_{(i,2)} \ldots s_{(i,m)}\right)$$

$\mathbf{S}_{generalized}$ имеет размерность $1 \times \ell b$.

Так как в данной работе будет использоваться только обобщенный синдром, то в дальнейшем будем обозначать его $\mathbf{S}$.

3 Алгоритм декодирования

Приведем описание итеративного алгоритма декодирования с жестким решением, обобщенного на случай q-ичных кодов. До начала работы алгоритма вычисляется обобщенный синдром принятого вектора.

Алгоритм $\mathscr{A}$

Каждая итерация состоит из следующих двух шагов:

1. Проходим по всем символам из вектора $r(i)$, где $r(1)$ – это принятый вектор, и для каждого из них выполняем следующее:
   - **Вычисляем решения**
     Рассматриваются синдромы ℓ кодов-компонентов, в которые входит данный символ. Если синдром кода-компонента ненулевой, то есть этот код-компонент обнаружил ошибку, то вычисляем *решение*. *Решением* назовем значение, которое нужно добавить к данному символу, чтобы синдром кода-компонента стал нулевым. Кодам-компонентам с нулевыми синдромами соответствуют нулевые *решения*.
   - **Критерий замены**
     Выбирается подмножество одинаковых ненулевых *решений* максимальной мощности ℓ' (если таких подмножеств несколько, то выбирается любое из них). Если ℓ' больше числа нулевых *решений*, то к символу добавляется значение *решения*, синдром пересчитывается. Переходим к следующему символу.
2. Если вес синдрома равен нулю, то выдается исправленный вектор. Иначе сравниваются веса синдрома до и после итерации. Если вес уменьшился, то переходим к следующей итерации, иначе – отказ от декодирования.

З а м е ч а н и е 3. После каждой замены символа вес обобщенного синдрома уменьшается, так как количество синдромов кодов-компонентов, ставших нулевыми (ℓ'), больше количества синдромов кодов-компонентов, ставших ненулевыми (их число совпадает с числом нулевых решений).

З а м е ч а н и е 4. Отметим, что в случае $d = 2$ *решение* можно вычислить при любом ненулевом значении синдрома кода-компонента. В случае $d = 3$ *решение* существует не всегда.

З а м е ч а н и е 5. Важно отметить, что алгоритм $\mathscr{A}$ работает с символами последовательно. То есть синдром пересчитывается после каждой замены символа. Это понадобится нам в дальнейшем при доказательстве корректности алгоритма.

4 Формулировка основного результата

Т е о р е м а 1. *Если существует по крайней мере один положительный корень (относительно переменной ω) уравнения (2), то в ансамбле $\mathscr{E}(n_0, \ell, b)$ МПП-кодов существуют коды (с вероятностью $p : \lim\limits_{n\to\infty} p = 1$), которые могут исправить любую комбинацию ошибок веса не более $\lfloor \frac{\omega_\alpha n}{2} \rfloor$ при сложности декодирования $\mathcal{O}(n \log_2 n)$.*

$$\omega_\alpha = \omega_0 - \varepsilon_1$$

где
ω_0 *– наименьший положительный корень уравнения (2)*
ε_1 *– сколь угодно малая положительная величина*

$$h(\omega) + \omega \log_2 (q-1) - \ell F(\alpha, \omega, n_0) = 0 \tag{2}$$

где $h(\omega)$ – бинарная энтропия: $h(\omega) = -\omega \log_2 \omega - (1-\omega)\log_2(1-\omega)$, а функция $F(\alpha, \omega, n_0)$ определяется следующим образом:

$$\begin{aligned} F(\alpha, \omega, n_0) &= h(\omega) + \omega \log_2 (q-1) - \tfrac{1}{n_0} h(\alpha\omega n_0) + \\ &+ \max_{s>0} \left\{ \omega \log_2 (s) - \tfrac{1}{n_0} \log_2 (g_0(s, n_0)) - \alpha\omega \log_2 \left(\tfrac{g_1(s,n_0)}{g_0(s,n_0)} \right) \right\} \end{aligned} \tag{3}$$

$\alpha > \frac{1}{2} + \varepsilon_2$, ε_2 – сколь угодно малая положительная величина.
Поиск максимума ведется по всем положительным s таким, что

$$\frac{\alpha\omega n_0}{1 - \alpha\omega n_0} \leqslant \frac{g_1(s, n_0)}{g_0(s, n_0)} \tag{4}$$

$g_0(s, n_0)$ – производящая функция весов кодовых слов компонентного кода.
$g_1(s, n_0)$ – производящая функция весов всех остальных слов.

З а м е ч а н и е 6. Отметим, что

$$g_0(s, n_0) + g_1(s, n_0) = (1 + (q-1)s)^{n_0}$$

так как $(1+(q-1)\,s)^{n_0} = \sum\limits_{W=0}^{n_0} \begin{pmatrix} n_0 \\ W \end{pmatrix} (q-1)^W\, s^W$ – производящая функция весов всех возможных слов.

5 Доказательство основного результата

5.1 Существование МПП-кодов с хорошим коэффициентом расширения

Л е м м а 1. *Для любой фиксированной комбинации из W ошибок вероятность того, что вес обобщенного синдрома кода из ансамбля $\mathscr{E}\,(n_0, \ell, b)$ не превысит величины $\alpha W \ell$, ограничена сверху величиной $2^{-n\ell F(\alpha,\omega,n_0)}$:*

$$P_W(|\mathbf{S}| \leqslant \alpha W \ell) \leqslant 2^{-n\ell F(\alpha,\omega,n_0)},\ \ \omega = \frac{W}{n}$$

Д о к а з а т е л ь с т в о. Рассмотрим l-тый слой. Введем следующую производящую функцию:

$$Q_W^l(t) = \sum_{j=0}^{b} P_W\left(|\mathbf{S}_l| = j\right) t^j \tag{5}$$

где $P_W\left(|\mathbf{S}_l| = j\right)$ обозначает вероятность того, что при заданном W число кодов в слое l, обнаруживших ошибку, в точности равно j.

Для того, чтобы вычислить $P_W\left(|\mathbf{S}_l| = j\right)$, поступим следующим образом: зафиксируем перестановку π_l , а перестановки и умножения на константы будем производить с элементами вектора, а не со столбцами проверочной матрицы. Очевидно, что данные задачи эквивалентны, и так как от выбранной перестановки π_l ничего не зависит, пусть она будет тождественной.

$$P_W\left(|\mathbf{S}_l| = j\right) = \frac{N_j\left(W, n_0, b\right)\binom{b}{j}}{\binom{n}{W}\left(q-1\right)^W} \tag{6}$$

где $N_j\left(W, n_0, b\right)$ - число векторов ошибок веса W, при которых синдром l-го слоя выглядит следующим образом:

$$\mathbf{S}_l = \left(\underbrace{\alpha_1 \ldots \alpha_j}_{j} \underbrace{0 \ldots 0}_{b-j}\right)$$

где α_i могут принимать любые ненулевые значения.

Введем еще одну производящую функцию:

$$E_j(s) = \sum_{i=0}^{n} N_j(i, n_0, b) s^i$$

Очевидно что,

$$E_j(s) = \sum_{i=0}^{n} N_j(i, n_0, b) s^i \geqslant N_j(W, n_0, b) s^W$$

следовательно,

$$N_j(W, n_0, b) \leqslant \frac{E_j(s)}{s^W}$$

Неравенство верно для любого $s > 0$. Наиболее точным значением является минимальный элемент множества $\left\{ \frac{E_j(s)}{s^W} \right\}$:

$$N_j(W, n_0, b) \leqslant \min_{s>0} \left\{ \frac{E_j(s)}{s^W} \right\} \tag{7}$$

Заметим, что в каждом слое множества позиций, занятых кодовыми символами компонентных кодов, не пересекаются. В то же время все позиции покрыты, следовательно, мы можем записать:

$$E_j(s) = (g_1(s, n_0))^j (g_0(s, n_0))^{b-j} \tag{8}$$

$g_0(s, n_0)$ и $g_1(s, n_0)$ определены в условии теоремы 1.

Подставив равенство (8) в (7) получим

$$N_j(W, n_0, b) \leqslant \min_{s>0} \left\{ \frac{(g_1(s, n_0))^j (g_0(s, n_0))^{b-j}}{s^W} \right\}$$

Полученное выражение подставим в (6)

$$P_W(|\mathbf{S}_l| = j) \leqslant \frac{\binom{b}{j}}{\binom{n}{W} (q-1)^W} \min_{s>0} \left\{ \frac{(g_1(s, n_0))^j (g_0(s, n_0))^{b-j}}{s^W} \right\}$$

Объединяя с (5) получим

$$
\begin{aligned}
&Q_W^l(t) \leqslant \sum_{j=0}^{b} \left(\frac{\binom{b}{j}}{\binom{n}{W}(q-1)^W} \min_{s>0} \left\{ \frac{(g_1(s,n_0))^j (g_0(s,n_0))^{b-j}}{s^W} \right\} t^j \right) \leqslant \\
&\leqslant \binom{n}{W}^{-1} (q-1)^{-W} \min_{s>0} \left\{ s^{-W} \sum_{j=0}^{b} \binom{b}{j} t^j (g_1(s,n_0))^j (g_0(s,n_0))^{b-j} \right\} = \\
&= \binom{n}{W}^{-1} (q-1)^{-W} \min_{s>0} \left\{ s^{-W} (g_0(s,n_0) + t g_1(s,n_0))^b \right\}
\end{aligned} \tag{9}
$$

Согласно определению ансамбля $\mathscr{E}(n_0, \ell, b)$ перестановка π_i и константы $c_{i,j}, j = 1, 2, \ldots, n$ для каждого слоя i выбираются независимо, поэтому вес обобщенного синдрома $|\mathbf{S}|$ есть сумма независимых случайных переменных $|\mathbf{S}_i|$, $i = 1, 2 \ldots \ell$. Производящая функция для обобщенного синдрома выглядит следующим образом:

$$
Q_W(t) = \sum_{j=0}^{b\ell} P_W(|\mathbf{S}| = j)\, t^j = \prod_{l=1}^{\ell} Q_W^l(t) = \left(Q_W^l(t)\right)^{\ell} \tag{10}
$$

Из (9) и (10) получим

$$
Q_W(t) \leqslant \binom{n}{W}^{-\ell} (q-1)^{-W\ell} \min_{s>0} \left\{ s^{-W\ell} (g_0(s,n_0) + t g_1(s,n_0))^{b\ell} \right\} \tag{11}
$$

Вероятность того, что вес обобщенного синдрома будет не больше $\alpha W \ell$ равна

$$
P_W(|\mathbf{S}| \leqslant \alpha W \ell) = \sum_{j=0}^{\alpha W \ell} P_W(|\mathbf{S}| = j)
$$

$$
Q_W(t) \geqslant \sum_{j=0}^{\alpha W \ell} P_W(|\mathbf{S}| = j)\, t^j = t^{\alpha W \ell} \sum_{j=0}^{\alpha W \ell} P_W(|\mathbf{S}| = j)\, t^{j - \alpha W \ell}
$$

Пусть $0 < t \leqslant 1$, тогда $Q_W(t) \geqslant t^{\alpha W \ell} \sum\limits_{j=0}^{\alpha W \ell} P_W(|\mathbf{S}| = j)$

В итоге

$$
P_W(|\mathbf{S}| \leqslant \alpha W \ell) = \sum_{j=0}^{\alpha W \ell} P_W(|\mathbf{S}| = j) \leqslant \frac{Q_W(t)}{t^{\alpha W \ell}} \tag{12}
$$

После подстановки (11) в (12) и минимизации по t получим

$$P_W\left(|\mathbf{S}| \leqslant \alpha W\ell\right) \leqslant \binom{n}{W}^{-\ell}(q-1)^{-W\ell} \min_{0<t\leqslant 1} \min_{s>0} \left\{(t^{\alpha}s)^{-W\ell}(g_0(s,n_0)+tg_1(s,n_0))^{b\ell}\right\}$$

Неравенство может быть переписано в виде:

$$P_W(|\mathbf{S}| \leqslant \alpha W\ell) \leqslant \binom{n}{W}^{-\ell}(q-1)^{-W\ell} \min_{0<t\leqslant 1} \min_{s>0} \left\{s^{-W\ell}(g_0(s,n_0))^{b\ell}(f(t,s))^{b\ell}\right\} \tag{13}$$

где

$$f(t,s) \triangleq \frac{1+t\frac{g_1(s,n_0)}{g_0(s,n_0)}}{t^{\alpha\omega n_0}}$$

Положив $\frac{df}{dt}$ равным нулю, найдем t_0, при котором достигается минимум

$$t_0 = \frac{\alpha\omega n_0}{1-\alpha\omega n_0}\left(\frac{g_0(s,n_0)}{g_1(s,n_0)}\right)$$

s выбирается таким, что $t_0 \leqslant 1$

$$f(t_0,s) = 2^{h(\alpha\omega n_0)}\left(\frac{g_1(s,n_0)}{g_0(s,n_0)}\right)^{\alpha\omega n_0} \tag{14}$$

где $h\left(p\right)$ – функция энтропии, которая может быть записана как $h(p) = \log_2 \frac{p^{-p}}{(1-p)^{(1-p)}}$

Подставив (14) в (13) получим:

$$P_W\left(|\mathbf{S}| \leqslant \alpha W\ell\right) \leqslant \binom{n}{W}^{-\ell}(q-1)^{-W\ell} 2^{\frac{h(\alpha\omega n_0)n\ell}{n_0}} \times$$
$$\times \min_{s>0}\left\{s^{-\omega n\ell}(g_0(s,n_0))^{\frac{n\ell}{n_0}}\left(\frac{g_1(s,n_0)}{g_0(s,n_0)}\right)^{\alpha\omega n\ell}\right\}$$

Воспользовавшись неравенством $\binom{n}{\omega n} \leqslant 2^{nh(\omega)}$, придем к требуемому результату:

$$P_W(|\mathbf{S}| \leqslant \alpha W\ell) \leqslant 2^{-n\ell F(\alpha,\omega,n_0)}$$

▲

Рассмотрим вероятность найти код, вес обобщенного синдрома которого меньше либо равен $\alpha W\ell$ хотя бы для одной комбинации ошибок веса W. Если эта вероятность меньше единицы, значит, существует код,

вес обобщенного синдрома которого превосходит $\alpha W\ell$ для любой комбинации ошибок веса W:

$$\binom{n}{W}(q-1)^W P_W(|\mathbf{S}| \leqslant \alpha W\ell) < 1 \tag{15}$$

Для того, чтобы найти максимальную кратность ошибок, для которой выполняется условие (15) нужно решить уравнение:

$$\binom{n}{W}(q-1)^W P_W(|\mathbf{S}| \leqslant \alpha W\ell) = 1$$

Будем искать W в виде $W = \omega n$. Прологарифмировав и воспользовавшись соотношением $\begin{pmatrix} n \\ \omega n \end{pmatrix} \leqslant 2^{nh(\omega)}$, получим

$$\ell F(\alpha, \omega, n_0) - h(\omega) - \omega \log_2(q-1) = 0$$

З а м е ч а н и е 7. Заметим, что условие (15) не гарантирует нам существование кода, "хорошего" при всех W вплоть до максимального значения. Вообще говоря "хорошие" коды при разных W могут быть различными. Это условие используется только для поиска максимального значения W.

Теперь докажем существование кода, "хорошего" при всех W вплоть до максимального значения. Пусть $G(\omega) = lF(\alpha, \omega, n_0) - h(\omega) - \omega \log_2(q-1)$. Если существует ω_0 удовлетворющее следующим условиям:

$$\begin{cases} G(\omega_0) = 0 \\ G(\omega) > 0 \ \forall \omega \in (0, \omega_0) \end{cases} \tag{16}$$

то верна следующая теорема:

Т е о р е м а 2. *В ансамбле $\mathscr{E}(n_0, \ell, b)$ МПП-кодов существуют коды (с вероятностью $p : \lim\limits_{n\to\infty} p = 1$), такие что $|\mathbf{S}| > \alpha W\ell$ для любой комбинации ошибок веса $W \leqslant \lfloor \omega_\alpha n \rfloor$, $\omega_\alpha = \omega_0 - \varepsilon$. ω_0 удовлетворяет условиям (16), ε – сколь угодно малая положительная величина.*

Д о к а з а т е л ь с т в о. Рассмотрим следующее условие:

$$\sum_{W=1}^{\lfloor \omega_\alpha n \rfloor} \binom{n}{W}(q-1)^W P_W(|\mathbf{S}| \leqslant \alpha W\ell) < 1 \tag{17}$$

В левой части стоит не что иное, как оценка сверху для вероятности "плохих" кодов, то есть кодов, дающих на каком-либо векторе синдром с неподходящим весом.

Перепишем это условие в виде

$$\lim_{n\to\infty}\sum_{W=1}^{\lfloor\omega_\alpha n\rfloor}2^{-n\left(\ell F(\alpha,\frac{W}{n},n_0)-h(\frac{W}{n})-\frac{W}{n}\log_2(q-1)\right)}<1$$

Выберем сколь угодно малую величину ε' и рассмотрим следующие два предела:

$$\lim_{n\to\infty}\sum_{W=1}^{\lfloor\varepsilon' n\rfloor}2^{-n\left(\ell F(\alpha,\frac{W}{n},n_0)-h(\frac{W}{n})-\frac{W}{n}\log_2(q-1)\right)} \tag{18}$$

$$\lim_{n\to\infty}\sum_{W=\lceil\varepsilon' n\rceil}^{\lfloor\omega_\alpha n\rfloor}2^{-n\left(\ell F(\alpha,\frac{W}{n},n_0)-h(\frac{W}{n})-\frac{W}{n}\log_2(q-1)\right)} \tag{19}$$

Сначала рассмотрим предел (19):

Можно показать, что существует $G_0>0 : G(\omega)\geqslant G_0 \quad \forall\omega\in[\varepsilon',\omega_\alpha]$. Полностью доказательство приводить не будем, ограничимся лишь идеей:

Рассмотрим функцию $G'(\omega)$, получающуюся из функции $G(\omega)$ заменой s на $f(\omega)=c_1\omega+c_2$, причем

$$\begin{cases} f(\varepsilon')=s_{\varepsilon'} \\ f(\omega_\alpha)=s_{\omega_\alpha}\end{cases}$$

где $s_{\varepsilon'}$ и s_{ω_α} – это значения s, при которых достигается максимум $G(\omega)$ при $\omega=\varepsilon'$ и $\omega=\omega_\alpha$ соответственно.

Ясно, что

$$\begin{cases} G'(\varepsilon')=G(\varepsilon')>0 \\ G'(\omega_\alpha)=G(\omega_\alpha)>0\end{cases}$$

Функция $G'(\omega)$ непрерывна на отрезке $[\varepsilon',\omega_\alpha]$, следовательно, существует $\min\limits_{\omega\in[\varepsilon',\omega_\alpha]}G'(\omega)=G_0$. $G_0>0$ (эту часть доказательства мы опустим).

Теперь, так как $G(\omega)\geqslant G'(\omega) \quad \forall\omega\in[\varepsilon',\omega_\alpha]$, то $G(\omega)\geqslant G_0 \quad \forall\omega\in[\varepsilon',\omega_\alpha]$.

$$0\leqslant\lim_{n\to\infty}\sum_{W=\lceil\varepsilon' n\rceil}^{\lfloor\omega_\alpha n\rfloor}2^{-n\left(\ell F(\alpha,\frac{W}{n},n_0)-h(\frac{W}{n})-\frac{W}{n}\log_2(q-1)\right)}\leqslant\lim_{n\to\infty}\sum_{W=\lceil\varepsilon' n\rceil}^{\lfloor\omega_\alpha n\rfloor}2^{-nG_0}=$$
$$=\lim_{n\to\infty}\left((\lfloor\omega_\alpha n\rfloor-\lceil\varepsilon' n\rceil+1)\cdot 2^{-nG_0}\right)=0$$

Таким образом,

$$\lim_{n\to\infty}\sum_{W=\lceil\varepsilon' n\rceil}^{\lfloor\omega_\alpha n\rfloor} 2^{-n\left(lF(\alpha,\frac{W}{n},n_0)-h(\frac{W}{n})-\frac{W}{n}\log_2(q-1)\right)}=0$$

Теперь вернемся к пределу (18)

$$G(\omega)=\tfrac{\ell-1}{\ell}h(\omega)+\tfrac{\ell-1}{\ell}\omega\log_2(q-1)-\tfrac{1}{n_0}h(\alpha\omega n_0)+$$
$$+\max_{s>0}\left\{\omega\log_2(s)-\tfrac{1}{n_0}\log_2(g_0(s,n_0))-\alpha\omega\log_2\left(\tfrac{g_1(s,n_0)}{g_0(s,n_0)}\right)\right\}$$

Поступим следующим образом:
Введем функцию $G^*(\omega)$:

$$G^*(\omega)=\tfrac{\ell-1}{\ell}h(\omega)+\tfrac{\ell-1}{\ell}\omega\log_2(q-1)-\tfrac{1}{n_0}h(\alpha\omega n_0)+$$
$$+\tfrac{1}{2}\omega\log_2\left(\omega^{\frac{1}{2}}\right)-\tfrac{1}{n_0}\log_2\left(g_0\left(\omega^{\frac{1}{2}},n_0\right)\right)-\alpha\omega\log_2\left(\frac{g_1\left(\omega^{\frac{1}{2}},n_0\right)}{g_0\left(\omega^{\frac{1}{2}},n_0\right)}\right)$$

Она получается из функции $G(\omega)$ заменой s на $\omega^{\frac{1}{2}}$. Очевидно, что

$$G(\omega)\geqslant G^*(\omega)$$

Найдем значения ω при которых выполняется условие (4):

$$\frac{\alpha\omega n_0}{1-\alpha\omega n_0}\leqslant\frac{g_1\left(\omega^{\frac{1}{2}},n_0\right)}{g_0\left(\omega^{\frac{1}{2}},n_0\right)}$$

$$\frac{g_0\left(\omega^{\frac{1}{2}},n_0\right)+g_1\left(\omega^{\frac{1}{2}},n_0\right)}{g_1\left(\omega^{\frac{1}{2}},n_0\right)}\leqslant\frac{1}{\alpha\omega n_0}$$

Но $g_0\left(\omega^{\frac{1}{2}},n_0\right)+g_1\left(\omega^{\frac{1}{2}},n_0\right)=\left(1+(q-1)\,\omega^{\frac{1}{2}}\right)^{n_0}$, следовательно,

$$\frac{\left(1+(q-1)\,\omega^{\frac{1}{2}}\right)^{n_0}}{g_1\left(\omega^{\frac{1}{2}},n_0\right)}\leqslant\frac{1}{\alpha\omega n_0}$$

Заметим, что $g_1\left(\omega^{\frac{1}{2}},n_0\right)\geqslant n_0(q-1)\omega^{\frac{1}{2}}$, так как все слова веса 1 не кодовые. В то же время $\left(1+(q-1)\,\omega^{\frac{1}{2}}\right)^{n_0}\leqslant(1+(q-1))^{n_0}=q^{n_0}$, так как $\omega\leqslant 1$. В итоге

$$\alpha\omega n_0 \leqslant \frac{n_0(q-1)\omega^{\frac{1}{2}}}{q^{n_0}}$$

И окончательно получим

$$\omega \leqslant \left(\frac{q-1}{\alpha q^{n_0}}\right)^2$$

Мы получили ограничение на ε'

$$\varepsilon' \leqslant \left(\frac{q-1}{\alpha q^{n_0}}\right)^2 \tag{20}$$

Вернемся к вычислению предела

$$G(\omega) \geqslant G^*(\omega) \Rightarrow \lim_{n\to\infty} \sum_{W=1}^{\lfloor \varepsilon' n \rfloor} 2^{-n\cdot G\left(\frac{W}{n}\right)} \leqslant \lim_{n\to\infty} \sum_{W=1}^{\lfloor \varepsilon' n \rfloor} 2^{-n\cdot G^*\left(\frac{W}{n}\right)}$$

Преобразуем функцию $G^*(\omega)$

$$\begin{aligned} &G^*(\omega) = \tfrac{\ell-1}{\ell} h(\omega) + \tfrac{\ell-1}{\ell}\omega\log_2(q-1) - \tfrac{1}{n_0}h(\alpha\omega n_0) + \\ &+\tfrac{1}{2}\omega\log_2(\omega) - \tfrac{1}{n_0}\log_2\left(g_0\left(\omega^{\frac{1}{2}}, n_0\right)\right) - \alpha\omega\log_2\left(\frac{g_1\left(\omega^{\frac{1}{2}}, n_0\right)}{g_0\left(\omega^{\frac{1}{2}}, n_0\right)}\right) \end{aligned} \tag{21}$$

Так как $g_0(s, n_0)$ – производящая функция весов кодовых слов кода компонента, то она имеет следующий вид:

$$g_0(s, n_0) = 1 + N_d s^d + \ldots$$

то есть имеет свободный член (линейный код всегда содержит нулевое слово) и не содержит слагаемого с s (слова веса 1 не кодовые).

$$\frac{g_1(s, n_0)}{g_0(s, n_0)} = \frac{(1+(q-1)s)^{n_0}}{g_0(s, n_0)} - 1 \leqslant (1+(q-1)s)^{n_0} - 1$$

так как $g_0(s, n_0) \geqslant 1 \ \ \forall\omega \geqslant 0$.

В итоге

$$\begin{aligned} &G^*(\omega) \geq \tfrac{\ell-1}{\ell} h(\omega) + \tfrac{\ell-1}{\ell}\omega\log_2(q-1) - \tfrac{1}{n_0}h(\alpha\omega n_0) + \tfrac{1}{2}\omega\log_2(\omega) - \\ &-\tfrac{1}{n_0}\log_2\left(1 + g_0\left(\omega^{\frac{1}{2}}, n_0\right) - 1\right) - \alpha\omega\log_2\left(\left(1+(q-1)\omega^{\frac{1}{2}}\right)^{n_0} - 1\right) \end{aligned}$$

После преобразований получим следующую оценку для функции $G(\omega)$

$$G(\omega) \geqslant G^*(\omega) = -\left(\tfrac{\ell-1}{\ell} - \tfrac{1}{2} - \tfrac{\alpha}{2}\right)\omega \log_2 \omega + \mathcal{O}(\omega)$$

Выберем $\alpha < \frac{2(\ell-1)}{\ell} - 1 = 1 - \frac{2}{\ell}$, тогда

$$G(\omega) \geqslant -c_1 \omega \log_2 \omega + c_2 \omega + o(\omega), \quad c_1 > 0$$

$$\lim_{n\to\infty} \sum_{W=1}^{\lfloor \varepsilon' n \rfloor} 2^{-n \cdot G\left(\frac{W}{n}\right)} \leqslant \lim_{n\to\infty} \sum_{W=1}^{\lfloor \varepsilon' n \rfloor} 2^{n \cdot c_1 \cdot \frac{W}{n} \log_2 \frac{W}{n} - n \cdot c_2 \cdot \frac{W}{n}} =$$
$$= \lim_{n\to\infty} \sum_{W=1}^{\lfloor \varepsilon' n \rfloor} \left(\frac{W}{n}\right)^{c_1 \cdot W} 2^{-c_2 \cdot W} = \lim_{n\to\infty} \sum_{W=1}^{\lfloor \varepsilon' n \rfloor} \left((\varepsilon')^{c_1} \cdot 2^{-c_2}\right)^W =$$
$$= \frac{(\varepsilon')^{c_1} \cdot 2^{-c_2}}{1 - (\varepsilon')^{c_1} \cdot 2^{-c_2}} = \varepsilon''$$

Заметим, что знак c_2 не важен, так как мы всегда можем сделать получившееся значение сколь угодно малым, правильно подобрав ε'. При выборе ε' также необходимо помнить об условии (20).

Так как оба предела существуют и конечны, то

$$\lim_{n\to\infty} \sum_{W=1}^{\lfloor \omega_\alpha n \rfloor} 2^{-n\left(lF(\alpha, \frac{W}{n}, n_0) - h(\frac{W}{n}) - \frac{W}{n}\log_2(q-1)\right)} \leqslant \varepsilon'' < 1 \qquad (22)$$

▲

Таким образом, мы доказали, что почти все коды из ансамбля $\mathscr{E}(n_0, \ell, b)$ имеют хороший коэффициент вершинного расширения.

5.2 Выбор α

Рассмотрим подграф графа Таннера, содержащий вершины-символы с ошибками (кратность ошибок равна W) и вершины-коды, в которые входят ребра, исходящие из выбранных вершин-символов. Далее мы будет работать только с этим подграфом.

Введем следующие обозначения:

A – множество кодов, обнаруживших ошибку ($a = |A|$).

A_i $(i = 1 \ldots n_0)$ – подмножество A, содержащее только те коды, в которые входят в точности i ребер ($a_i = |A_i|$)

$A_{\geqslant 2} = A \setminus A_1$ – подмножество A, содержащее только те коды, в которые входят не менее 2-х ребер ($a_{\geqslant 2} = |A_{\geqslant 2}|$)

C – множество кодов, содержащих ошибки, но не обнаруживших их ($c = |C|$).

$e_{A_1}^{(i)}$ – число ребер, выходящих из вершины-символа i и входящих в множество A_1

$e_C^{(i)}$ – число ребер, выходящих из вершины-символа i и входящих в множество C

На Рис. 2 приведен пример подграфа графа Таннера, и графически проиллюстрированы введенные обозначения.

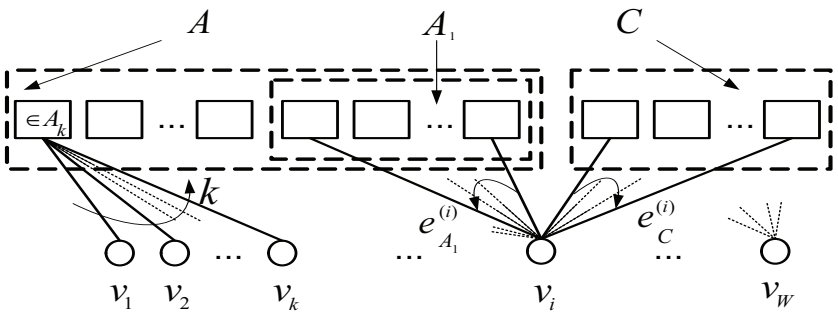

Рис. 2: Подграф графа Таннера

Сформулируем и докажем достаточное условие того, что найдется символ, который будет заменен нашим алгоритмом (согласно описанию алгоритма это приведет к уменьшению веса обобщенного синдрома).

Нам потребуются следующие леммы:

Л е м м а 2. *Если для ошибочного символа i выполнено условие $e_{A_1}^{(i)} > e_C^{(i)}$, то он непременно будет заменен нашим алгоритмом.*

Д о к а з а т е л ь с т в о. Очевидно, что все коды с одной ошибкой дадут одинаковые решения. Число нулевых решений есть $e_C^{(i)}$, так как ошибочный символ не может входить в коды не содержащие ошибок. Возможны два случая:

1. Множество полученных решений имеет наибольшую мощность среди множеств одинаковых по величине решений

2. Для данного символа существует подмножество решений мощности большей, чем $e_{A_1}^{(i)}$.

В любом из этих случаев символ будет заменен, и это приведет к уменьшению веса обобщенного синдрома. ▲

З а м е ч а н и е 8. В лемме не утверждается, что символ будет исправлен.

Л е м м а 3. *Если* $a_1 > \sum_{i=1}^{W} e_C^{(i)}$, *то найдется ошибочный символ* i, *для которого* $e_{A_1}^{(i)} > e_C^{(i)}$

Д о к а з а т е л ь с т в о. От обратного. Пусть такого символа не существует, тогда $e_{A_1}^{(i)} \leqslant e_C^{(i)}\ \forall i \in [1, W]$. Отсюда немедленно следует, что

$$\sum_{i=1}^{W} e_{A_1}^{(i)} \leqslant \sum_{i=1}^{W} e_C^{(i)}$$

но

$$\sum_{i=1}^{W} e_{A_1}^{(i)} = a_1$$

что противоречит условию. Лемма доказана. ▲

Теперь мы готовы доказать теорему.

Т е о р е м а 3. *Для существования по крайней мере одного символа, который будет заменен нашим алгоритмом в пределах итерации, достаточно выполнения следующего условия:*

$$a > \frac{Wl}{2}$$

Д о к а з а т е л ь с т в о. Число ребер, выходящих из W вершин с ошибочными символами равно $W\ell$. Эти ребра могут входить в коды обнаружившие ошибку ($A = A_1 \bigsqcup A_{\geqslant 2}$) или в коды не обнаружившие ошибку, но содержащие их (C).

Оценим число ребер, входящих в каждое из трех множеств кодов (имеются в виду только ребра, выходящие из ошибочных символов):

- Число ребер, входящих в коды из множества A_1 равно $\sum_{i=1}^{W} e_{A_1}^{(i)} = a_1$
- Число ребер, входящих в коды из множества $A_{\geqslant 2}$ не меньше $2\,(a - a_1)$ (использовано то, что в каждый из кодов входит как минимум два ребра)
- Число ребер, входящих в коды из множества C равно $\sum_{i=1}^{W} e_C^{(i)}$

Получим следующее неравенство, верное для любого кода из ансамбля $\mathscr{E}(n_0, \ell, b)$ при любом W

$$W\ell \geqslant \sum_{i=1}^{W} e_C^{(i)} + a_1 + 2(a - a_1)$$

Немного преобразовав неравенство получим:

$$\sum_{i=1}^{W} e_C^{(i)} - a_1 \leqslant W\ell - 2a \tag{23}$$

Отсюда немедленно следует, что если $a > \frac{W\ell}{2}$, то $\sum\limits_{i=1}^{W} e_C^{(i)} - a_1 < 0$, что и завершает доказательство теоремы. ▲

Так как $a = |\mathbf{S}|$, то согласно предыдущей теореме и теореме о существовании кодов с хорошим коэффициентом расширения нужно выбрать $\alpha > \frac{1}{2}$.

К сожалению, в процессе декодирования мы можем вносить ошибки и из-за этого W_i (число ошибок после i-й итерации) может стать больше, чем $W_\alpha = \lfloor \omega_\alpha n \rfloor$. В этом случае мы уже не сможем утверждать, что $|\mathbf{S}| > \frac{W\ell}{2}$. С другой стороны, если $W_i < W_\alpha \ \forall i = 1, \ldots, i_{max}$, то все ошибки будут исправлены, так как синдром достигнет нуля.

Л е м м а 4. *Если $W_i < W_\alpha \ \forall i = 1, \ldots, i_{max}$, то все ошибки будут исправлены алгоритмом $\mathscr{A}$.*

Д о к а з а т е л ь с т в о. Так как $W_i < W_\alpha \ \forall i = 1, \ldots, i_{max}$, то

$$|\mathbf{S}_i| > \frac{W_i \ell}{2} \ \forall i = 1, \ldots, i_{max}$$

Так как синдром на каждой итерации уменьшается, то рано или поздно он станет нулевым. Докажем, что $W_{imax} = 0$. От обратного. Пусть $W_{imax} \neq 0$, тогда $|\mathbf{S}_{imax}| > \frac{W_{imax}\ell}{2} > 0$. Противоречие.

▲

Иными словами теперь вопрос состоит в том, какова максимальная начальная кратность ошибок, для которой число ошибок $W_i < W_\alpha \ \forall i = 1, \ldots, i_{max}$. Следующая теорема дает ответ на этот вопрос.

Т е о р е м а 4. *Пусть в коде из ансамбля $\mathscr{E}(n_0, \ell, b)$ $|\mathbf{S}| > \frac{W\ell}{2} \ \forall W \leqslant \lfloor \omega_\alpha n \rfloor$, тогда если начальная кратность ошибок $W_0 \leqslant \lfloor \frac{\omega_\alpha n}{2} \rfloor$, то $W_i < \lfloor \omega_\alpha n \rfloor \ \forall i = 1, \ldots, i_{max}$.*

Д о к а з а т е л ь с т в о. Заметим, что $|\mathbf{S}_i| \leqslant \lfloor \frac{\omega_\alpha n}{2} \rfloor \ell$, так как синдром с каждой заменой символа может только уменьшаться. Алгоритм $\mathscr{A}$ работает с символами последовательно (синдром пересчитывается после

каждой замены символа), следовательно, в один момент времени может быть внесена только одна ошибка. Из этого немедленно следует, что если для некоторого момента времени j $W_j > \lfloor \omega_\alpha n \rfloor$, то в некоторый момент времени k кратность ошибок $W_k = \lfloor \omega_\alpha n \rfloor$. Тогда $|\mathbf{S}_k| > \lfloor \frac{\omega_\alpha n}{2} \rfloor \ell$. Противоречие. ▲

5.3 Сложность декодирования

В предыдущем разделе мы доказали, что при $\alpha > \frac{1}{2}$ и начальном количестве ошибок $W_0 \leqslant \lfloor \frac{\omega_\alpha n}{2} \rfloor$ алгоритм исправит все ошибки. Этот раздел посвящен вопросу о сложности декодирования, который с помощью следующей леммы сводится к вопросу о числе итераций. Пусть начальный вес синдрома $|\mathbf{S}| = \sigma W_0 \ell$, $\alpha < \sigma \leqslant 1$ $(W_0 = \lfloor \frac{\omega_\alpha n}{2} \rfloor)$.

Л е м м а 5. *Сложность одной итерации декодирования есть* $\mathcal{O}(n)$

Д о к а з а т е л ь с т в о. Мы должны проверить все n символов, для проверки каждого из которых нам потребуется $\mathcal{O}(1)$ операций. ▲

К сожалению при $\alpha > \frac{1}{2}$ мы можем утверждать только то, что лишь один символ будет гарантированно заменен нашим алгоритмом в пределах итерации. Вес обобщенного синдрома при этом должен уменьшится как минимум на 1. В итоге нам потребуется $\mathcal{O}(n)$ итераций (Начальный вес синдрома $|\mathbf{S}| = \sigma W_0 \ell$ и каждую итерацию уменьшается на 1).

Для получения логарифмической оценки немного усилим условие на α и потребуем $\alpha > \frac{1}{2} + \varepsilon$ $(\varepsilon > 0)$.

Л е м м а 6. *Пусть* $\alpha > \frac{1}{2} + \varepsilon$ $(\varepsilon > 0)$, *тогда за одну итерацию алгоритма будут заменены по крайней мере* $\lceil \delta W \rceil$ *ошибочных символов, где*

$$\delta = \frac{2\varepsilon}{\ell(n_0 - 1) + 1}$$

Д о к а з а т е л ь с т в о.

$\alpha > \frac{1}{2} + \varepsilon$, следовательно, $a > \frac{W\ell}{2} + \varepsilon W \ell$. Отсюда, использовав условие (23) получим

$$a_1 - \sum_{i=1}^{W} e_C^{(i)} \geqslant 2\varepsilon W \ell$$

Или

$$\sum_{i=1}^{W} \left(e_{A_1}^{(i)} - e_C^{(i)} \right) \geqslant 2\varepsilon W \ell$$

Теперь найдем минимальное число символов, для которых выполнилось условие $e_{A_1}^{(i)} > e_C^{(i)}$

Очевидно, что
$0 < e_{A_1}^{(i)} - e_C^{(i)} \leqslant \ell$ для, тех символов, которые будут заменены
$-\ell < e_{A_1}^{(i)} - e_C^{(i)} \leqslant 0$ для, тех символов, которые не будут заменены
Тогда

$$W_1 \ell + (W - W_1)\, 0 \geqslant \sum_{i=1}^{W} \left(e_{A_1}^{(i)} - e_C^{(i)} \right) \geqslant 2\varepsilon W \ell$$

$$W_1 \geqslant 2\varepsilon W$$

$$\delta' = \frac{W_1}{W} \geqslant 2\varepsilon$$

Так как синдром пересчитывается после каждой замены символа, то любое изменение символа влияет на решения для оставшихся. Поступим следующим образом: пусть мы меняем символ i, оценим на какое количество символов мы можем повлиять. Символ i входит в ℓ кодов, которые могут содержать самое большое $\ell\,(n_0 - 1)$ символов кроме символа i
В итоге

$$\delta = \frac{\delta'}{\ell\,(n_0 - 1) + 1} \geqslant \frac{2\varepsilon}{\ell\,(n_0 - 1) + 1}$$

Лемма доказана.

▲

С л е д с т в и е 1. *Обозначим через* $|\mathbf{S}_{i-1}|$ *вес обобщенного синдрома до* i*-й итерации,* $|\mathbf{S}_i|$ *– после. Тогда*

$$|\mathbf{S}_i| \leqslant \left(1 - \frac{\delta}{\ell}\right) |\mathbf{S}_{i-1}|$$

Д о к а з а т е л ь с т в о. Так как замена каждого символа уменьшает вес обобщенного синдрома как минимум на 1, то согласно предыдущей теореме, за одну итерацию вес обобщенного синдрома уменьшится как минимум на δW. То есть

$$|\mathbf{S}_i| \leqslant |\mathbf{S}_{i-1}| - \delta W_{i-1}$$

Так как $W_{i-1} \geqslant \frac{|\mathbf{S}_{i-1}|}{\ell}$, то

$$|\mathbf{S}_i| \leqslant \left(1 - \frac{\delta}{\ell}\right) |\mathbf{S}_{i-1}|$$

▲

Т е о р е м а 5. *При* $\alpha > \frac{1}{2}+\varepsilon$ $(\varepsilon > 0)$ *и начальном количестве ошибок* $W_0 = \lfloor \frac{\omega_\alpha n}{2} \rfloor$ *алгоритм исправит все ошибки за* $\mathcal{O}(n \log_2 n)$ *операций.*

Д о к а з а т е л ь с т в о. Оценим число итераций:

$$\left(1 - \frac{\delta}{\ell}\right)^{i_{max}} |\mathbf{S}_0| < 1$$

Так как $|\mathbf{S}_0| = \sigma W_0 \ell$, то

$$i_{max} < \log_{\frac{1}{1-\frac{\delta}{\ell}}} (\sigma W_0 \ell)$$

▲

6 Численные результаты

На Рис. 3 и Рис. 4 представлены полученные зависимости доли исправляемых ошибок от скорости кода для $q = 64$ и $q = 16$. На каждом из этих рисунков показаны три зависимости:

- Зависимость $\omega_{d=3}(R)$ для кода-компонента Рида-Соломона с $d = 3$.
- Зависимость $\omega_{d=2}(R)$ для кода-компонента с q-ичной проверкой на четность $(n_0 = q)$.
- Зависимость $\omega_{max}(R)$ для кода-компонента с q-ичной проверкой на четность (n_0 подбирается таким образом, чтобы доля исправляемых ошибок была максимальна для данной скорости).

Таблица 1: Численные результаты, полученные при $q = 64$

R	0,125	0,25	0,375	0,5	0,625	0,75	0,875
$\omega_{max}(R)$	0,0156	0,0131	0,0104	0,0081	0,0058	0,0037	0,0017
$\omega_{d=2}(R)$	0,0117	0,0107	0,0095	0,0079	0,0058	0,0031	0,0001
$\omega_{d=3}(R)$	0,0078	0,0067	0,0054	0,0039	0,0022	0,0006	–

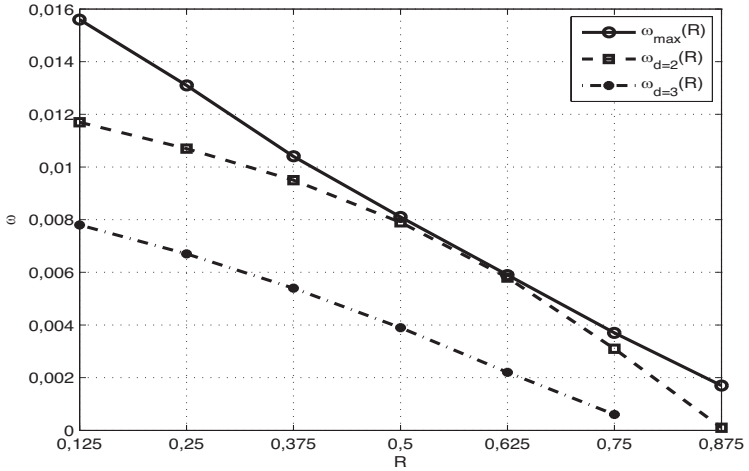

Рис. 3: Зависимости доли исправляемых ошибок от скорости кода для $q = 64$

Таблица 2: Численные результаты, полученные при $q = 16$

R	0,125	0,25	0,375	0,5	0,625	0,75	0,875
$\omega_{max}(R)$	0,0103	0,0095	0,0085	0,0072	0,0053	0,0033	0,0015
$\omega_{d=2}(R)$	0,0048	0,0036	0,0023	0,0010	–	–	–
$\omega_{d=3}(R)$	0,0008	0,0003	0,0001	10^{-7}	–	–	–

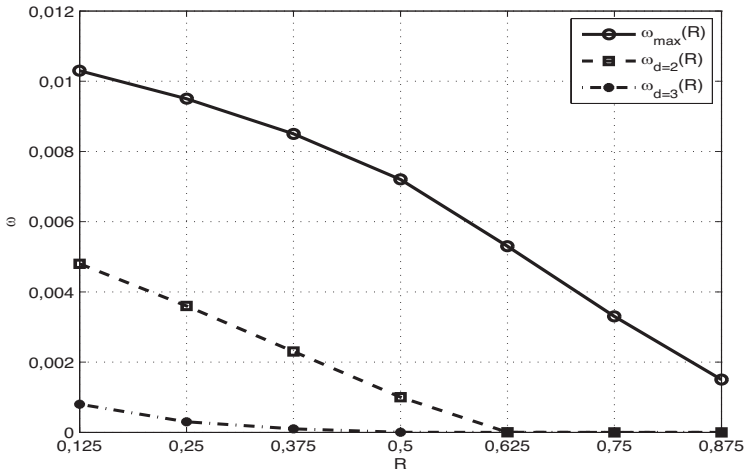

Рис. 4: Зависимости доли исправляемых ошибок от скорости кода для $q = 16$

На Рис. 5 и Рис. 6 проводится сравнение наших результатов и результатов, полученных в [8]. В [8] использовалось условие $\alpha > \frac{2}{3} + \varepsilon$. В этой работе нам удалось ослабить это условие до $\alpha > \frac{1}{2} + \varepsilon$, благодаря чему, результаты получились гораздо лучше. В качестве кода-компонента выбран код Рида-Соломона с $d = 3$.

Таблица 3: Численные результаты для $\omega(R)$ при $q = 128$

	R	0,125	0,25	0,375	0,5	0,625	0,75	0,875
Наши результаты	**1**	0,0057	0,0052	0,0046	0,0039	0,0028	0,0015	0,0001
Результаты, полученные в [8]	**2**	0,0018	0,0015	0,0013	0,0010	0,0006	0,0002	–

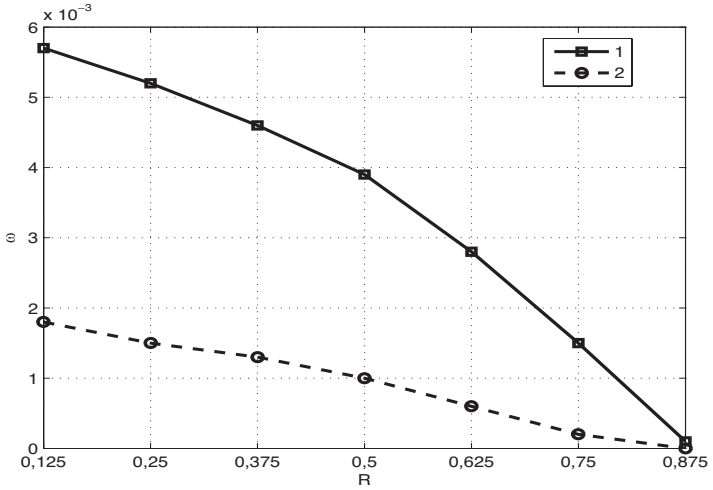

Рис. 5: Сравнение зависимостей доли гарантированно исправляемых ошибок от скорости кода при $q = 128$

Таблица 4: Численные результаты для $\omega(q)$ при $R = \frac{1}{2}$

	q	16	32	64	128	256	512	1024
Наши результаты	**1**	–	0,0017	0,0039	0,0039	0,0029	0,0018	0,0009
Результаты, полученные в [8]	**2**	–	$8 \cdot 10^{-5}$	0,0006	0,0011	0,0010	0,0008	0,0004

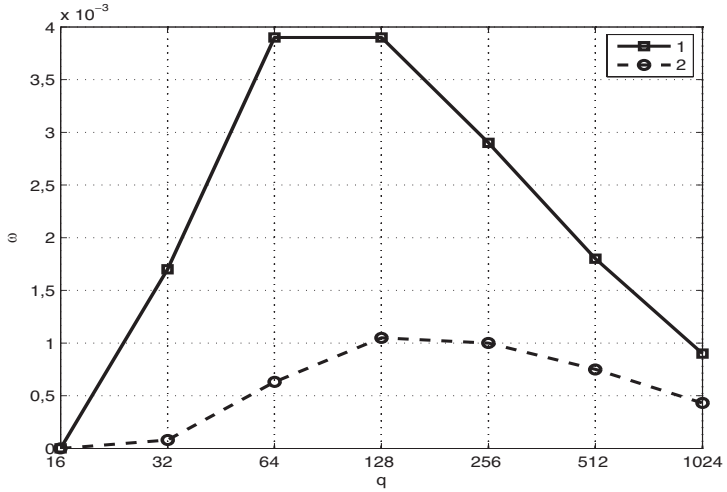

Рис. 6: Сравнение зависимостей доли гарантированно исправляемых ошибок от q при $R = \frac{1}{2}$

7 Заключение

В заключение отметим, что результаты полученные в данной работе для q-ичных кодов лучше, чем результаты, полученные для двоичных кодов в [3, 6]. Точно так же, как и для двоичных кодов, результаты, которые дает этот метод оценки, лучше для кода с кодом-компонентом с одним проверочным символом, чем для кода с кодом-компонентом с двумя проверочными символами.

Список литературы

[1] *Gallager R.G.* Low-Density Parity-Check Codes MIT Press, 1963.

[2] *Tanner M.* A Recursive Approach to Low Complexity Codes // IEEE Trans. Inform. Theory. 1981. V. 27. № 5. P. 533 – 547.

[3] *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 С. 25 – 40.

[4] *Zyablov V., Johannesson R., Loncar M., Rybin P.* On the Error-Correcting Capabilitiers of Low-Complexity Decoded LDPC Codes with Constituent Hamming Codes //Eleventh International Workshop on Algebraic and Combinatorial Coding Theory (ACCT2008), 2008.

[5] *Miladinovic N., Fossorier M.* Generalized LDPC Codes with Reed-Solomon and BCH Codes as Component Codes for Binary Channels // Proc. IEEE Global Conf. on Communication (GLOBECOM), St. Louis, USA, November. 2005.

[6] *Зяблов В.В., Пинскер М.С.* Оценка сложности исправления ошибок низкоплотностными кодами Галлагера // Пробл. передачи информ. 1975. Т. 11. №1 С. 23 – 36.

[7] *Бассалыго Л.А.* Формализация задачи о сложности задания кода // Пробл. передачи информ. 1976. Т. 12. №4 С. 105 – 106.

[8] *Zyablov V., Potapov V., Groshev F.* Low-complexity error correction in LDPC codes with constituent RS codes // Proc. 11th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'08). Pamporovo, Bulgaria. June 16-22, 2008. P. 348-353.