Информационные процессы, Том 12, № 1, 2012, стр. 84–97.

ТЕОРИЯ И МЕТОДЫ ОБРАБОТКИ ИНФОРМАЦИИ

Оценка экспоненты вероятности ошибки декодирования обобщенного МПП-кода специальной конструкции

В. В. Зяблов, П. С. Рыбин

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

Поступила в редколлегию 22.03.2012

Аннотация—В работе предложена специальная конструкция обобщенного кода с малой плотностью проверок (МПП-кода) и алгоритм декодирования данного кода с малой сложностью. Для рассматриваемого кода и алгоритма декодирования была получена нижняя оценка на экспоненту вероятности ошибочного декодирования. Полученная оценка позволяет заключить, что в ансамбле рассматриваемых МПП-кодов существуют коды со скоростью до пропускной способности, у которых экспонента вероятности ошибки больше нуля.

1. ВВЕДЕНИЕ

Код с малой плотностью проверок (МПП-код) был предложен Р. Галлагером в [1]. В работе [2] впервые было показано, что в ансамбле МПП-кодов Галлагера существуют коды, гарантированно исправляющие линейную долю ошибок со сложностью декодирования $\mathcal{O}(n \log n)$, где n - длина кода. Затем в работе [3] эта оценка была улучшена и применена для обобщенного МПП-кода.

В работах [4] и [5] были получены верхняя и нижняя границы на экспоненту вероятности ошибочного декодирования МПП-кода по максимуму правдоподобия. При этом сложность декодирования составляет $\mathcal{O}(2^n)$.

В данной работе построен обощенный МПП-код со специальной конструкцией и разработан оригинальный алгоритм декодирования. Показано, что сложность предложенного алоритма декодирования составляет $\mathcal{O}(n \log n)$. Впервые получена нижняя оценка на экспоненту вероятности ошибочного декодирования МПП-кода по алгоитму со сложностью $\mathcal{O}(n \log n)$, которая больше нуля для всех скоростей до пропускной способности.

2. МПП-КОД

2.1. Описание

Код с малой плотностью проверок (МПП-код) с компонентным кодом с проверкой на четность (МПП-код Галлагера) был предложен Галлагером в [1].

Для построения МПП-кода Галлагера рассмотрим блочную диагональную матрицу $\mathbf{H}_b$ на главной диагонали, которой стоят b проверочных матриц $\mathbf{H}_0$ компонентного кода с проверкой

на четность:

$$\mathbf{H}_b = \begin{pmatrix} \mathbf{H}_0 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathrm{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \underbrace{\mathbf{0}}_{b} & \mathbf{0} & \dots & \mathbf{H}_0 \end{pmatrix},$$

где b очень велико. Если длина кода с проверкой на четность равна n_0, тогда размер матрицы $\mathbf{H}_b$ – $b \times bn_0$. Обозначим $\pi(\mathbf{H}_b)$ случайную перестановку столбцов матрицы $\mathbf{H}_b$. Тогда матрица, составленная из $\ell > 2$ таких перестановок в качестве слоев,

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \\ \vdots \\ \mathbf{H}_\ell \end{pmatrix} = \begin{pmatrix} \pi_1(\mathbf{H}_b) \\ \pi_2(\mathbf{H}_b) \\ \vdots \\ \pi_\ell(\mathbf{H}_b) \end{pmatrix}$$

является разреженной проверочной матрицей $\mathbf{H}$ размера $\ell b \times bn_0$, которая определяет ансамбль МПП-кода Галлагера длины $n = bn_0$, где $n \gg n_0$. Обозначим этот ансамбль $\mathscr{E}_G(n_0, \ell, b)$.

Определение. Для заданного компонентного кода с проверкой на четность $\mathbf{H}_0$ независимо и равновероятно выбирая случайные перестановки π_l , $l = 1, 2, ..., \ell$, определим ансамбль МПП-кодов Галлагера $\mathscr{E}_G(n_0, \ell, b)$.

Замечание. Понятно, что построение МПП-кода Галлагера легко обобщить, просто заменив проверочную матрицу $\mathbf{H}_0$ кода с проверкой на четность на какой-либо другой линейный блочный код с длиной n_0 и соответствующей скоростью R_0. В данном случае мы получим обобщенный МПП-код.

Нижняя оценка на скорость R кода $\mathbf{H}$ определяется формулой:

$$R \geqslant 1 - \ell(1 - R_0),$$

где R_0 – скорость кода-компонента. Равенство достигается только в случае, когда $\mathbf{H}$ имеет полный ранг.

2.2. Мажоритарный алгоритм декодирования

Идея мажоритарного алгоритма декодирования заключается в уменьшении количества невыполненных проверок на каждой итерации декодирования. Результатом работы алгоритма является “исправленная” последовательность и флаг, информирующий об успешном декодировании или об отказе от декодирования.

Сформулируем мажоритарный алгоритм декодирования $\mathscr{A}_M$, каждая i-я итерация, $i = 1, 2, ..., i_{\max}$, которого состоит из следующих шагов:

1. Вычисляем проверки кодов-компонентов и количество невыполненных проверок для декодируемой последовательности $\mathbf{r}^{(i)}$, где $\mathbf{r}^{(1)}$ это принятая последовательность $\mathbf{r}$.
2. Последовательно рассматриваем символы декодируемой последовательности $\mathbf{r}^{(i)}$:

– если найдем символ, замена которого уменьшит количество невыполненных проверок, то данный символ инвертируется (заменяется), и выполнение алгоритма переходит к следующему шагу.
– если достигнут конец последовательности, то выполнение алгоритма переходит к следующему шагу.

3. Рассматриваем обновленную последовательность $\mathbf{r}^{(i)}$, полученную на предыдущем шаге:
   – если синдром МПП-кода Галлагера для обновленной последовательности стал нулевым (т.е. нет ни одного компонентного кода с невыполненной проверкой), алгоритм возвращает обновленную ("исправленную") последовательность $\mathbf{r}^{(i)}$, устанавливает флаг успешного декодирования и прекращает выполнение;
   – в противном случае если количество невыполненных проверок уменьшилось, то алгоритм переходит к следующей итерации $i+1$ с последовательностью $\mathbf{r}^{(i+1)}$, которая в точности совпадает с обновленной последовательностью $\mathbf{r}^{(i)}$;
   – иначе алгоритм устанавливает флаг отказа от декодирования и завершает выполнение.

2.3. Доля гарантированно исправимых ошибок

В работе [3] была получена оценка доли гарантированно исправимых ошибок ω_t обобщенным МПП-кодом при декодировании по алгоритму $\mathscr{A}_M$. В данной работе нас будет интересовать формулировка теоремы только для случая МПП-кода Галлагера из $\mathscr{E}_G(n_0, \ell, b)$. Введем следующие обозначения для случая МПП-кода Галлагера:

– $g_0(s, n_0)$ – весовая функция кода с проверкой на четность:

$$g_0(s, n_0) = \frac{(1+s)^{n_0} + (1-s)^{n_0}}{2},$$

– $g_1(s, n_0)$ – производящая функция комбинаций ошибок, обнаруживаемых кодом с проверкой на четность:

$$g_1(s, n_0) = \frac{(1+s)^{n_0} - (1-s)^{n_0}}{2}.$$

– $g_e(s, v, n_0)$ – специальная дважды производящая функция:

$$g_e(s, v, n_0) = g_1\left(sv^2, n_0\right).$$

– $h(\omega)$ – функция двоичной энтропии:

$$h(\omega) = -\omega \log_2 \omega - (1-\omega)\log_2(1-\omega).$$

Теорема 1. *Пусть существует корень ω_0 следующего уравнения:*

$$h(\omega) - \ell F_e(\omega, n_0) = 0,$$

где $F_e(\omega, n_0)$ определяется выражением:

$$F_e(\omega, n_0) \triangleq h(\omega) + \max_{s>0, 0<v<1} \left\{ \omega \log_2 sv - \frac{1}{n_0} \log_2 \left(g_e(s, v, n_0) + g_0(s, n_0) \right) \right\}.$$

Пусть также для найденного значения ω_0 существует корень уравнения α_0 следующего уравнения:

$$h(\omega_0) - \ell F_{\mathbf{s}}(\alpha, \omega_0, n_0, \ell) = 0,$$

где $F_{\mathbf{s}}(\alpha, \omega_0, n_0, \ell)$ определяется выражением:

$$F_{\mathbf{s}}(\alpha, \omega_0, n_0, \ell) \triangleq h(\omega_0) + \max_{s>0, 0<v<1} \{\omega_0 \left(\log_2 s + \frac{\ell - \frac{1-\alpha}{\alpha}}{\ell} \log_2 v \right) -$$

$$- \frac{1}{n_0} \log_2 (g_1(s, n_0)\, v + g_0(s, n_0))\}.$$

Тогда в ансамбле $\mathscr{E}_G(n_0, \ell, b)$ существует код (с вероятностью p такой, что $\lim\limits_{n\to\infty} p = 1$), который может исправить любую комбинацию ошибок кратности до $\lfloor \omega_t n \rfloor$, где $\omega_t = \alpha_0 \omega_0$, со сложностью декодирования по алгоритму $\mathscr{A}_M$ порядка $\mathcal{O}(n \log n)$.

3. ЛИНЕЙНЫЙ КОД

3.1. Описание

В самом общем случае линейным кодом (n, k) называется подпространство размерности k линейного векторного пространства размерности n над полем GF(q). В данной работе мы будем рассматривать линейные коды только над GF(2).

3.2. Алгоритм декодирования по максимуму правдоподобия

Пусть заданы вероятности перехода символа 1 в 0 и обратно. Имея список всех кодовых слов (размера $2^k = 2^{(Rn)}$), можно расчитать вероятность перехода принятой последовательности $\mathbf{r}$ в любое другое кодовое слово из списка. Результатом декодирования по максимуму правдоподобия является кодовое слово, вероятность перехода в которое является наименьшим. Понятно, что в случае двоично-симметричного канала (ДСК) наименьшая вероятность перехода достигается на ближайшем слове, т.е. алгоритм декодировани по максимуму правдоподобия совпадает с алгоритмом по минимуму расстояния.

3.3. Экспонента вероятности ошибочного декодирования

Следующая теорема, доказанная в общем виде в [6] и сформулированная в данном виде в [7], позволяет получить оценку на экспоненту вероятности ошибки при декодировании по максимуму правдоподобия линейного кода:

Теорема 2. *Существуют двоичные линейные блочные коды, для которых экспонента вероятности ошибочного декодирования по максимуму правдоподобия в ДСК без памяти при любой скорости передачи не превосходящей пропускной способности канала C, оценивается снизу величиной $E_0(R, p)$, определяемой равенствами*

при $0 \le R \le R_0 \left(R_0 = 1 - h\left(\frac{2\sqrt{p(1-p)}}{1+2\sqrt{p(1-p)}} \right) \right)$

$$E_0(R, p) = -\delta_{VG}(R) \ln \left(2\sqrt{p(1-p)} \right);$$

при $R_0 \le R \le R_* \left(R_* = 1 - h\left(\frac{\sqrt{p}}{\sqrt{p}+\sqrt{1-p}} \right) \right)$

$$E_0(R, p) = (1-R) \ln 2 - \ln \left(1 + 2\sqrt{p(1-p)} \right);$$

при $R_* \le R \le C$ $(C = 1 - h(p))$

$$\left.\begin{array}{c} E_0(R,p) = \frac{s}{1-s}(1-R)\ln 2 - \frac{1}{1-s}\ln\left(p^{1-s} + (1-p)^{1-s}\right) \\ R = 1 - h\left(\frac{p^{1-s}}{p^{1-s}+(1-p)^{1-s}}\right) \end{array}\right\} 0 \le s \le \frac{1}{2}.$$

Замечание. В дальнейшем под линейным кодом мы будем понимать коды, удовлетворяющие теореме 2.

4. ОСНОВНОЙ РЕЗУЛЬТАТ

4.1. Описание конструкции

Пусть даны проверочная матрица $\mathbf{H}_0$ кода с проверкой на четность с длиной n_0 и скоростью R_0 и проверочная матрица $\mathbf{H}_1$ случайного линейного кода с длиной n_1 и скоростью R_1. Тогда построим следующие две блочные матрицы:

$$\mathbf{H}_{b_0} = \begin{pmatrix} \mathbf{H}_0 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \underbrace{\mathbf{0} \quad \mathbf{0} \quad \dots \mathbf{H}_0}_{b_0} \end{pmatrix}$$

и

$$\mathbf{H}_{b_1} = \begin{pmatrix} \mathbf{H}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_1 & \dots & \mathbf{0} \\ \dots & \dots & \ddots & \dots \\ \underbrace{\mathbf{0} \quad \mathbf{0} \quad \dots \mathbf{H}_1}_{b_1} \end{pmatrix},$$

где b_0 и b_1 такие, что $n_0 b_0 = n_1 b_1$.

Теперь построим проверочную матрицу $\mathbf{H}$ обобщенного МПП-кода специального типа следующим образом:

$$\mathbf{H} = \begin{pmatrix} \pi_1(\mathbf{H}_{b_0}) \\ \pi_2(\mathbf{H}_{b_0}) \\ \vdots \\ \pi_\ell(\mathbf{H}_{b_0}) \\ \pi_{\ell+1}(\mathbf{H}_{b_1}) \end{pmatrix},$$

где, как и ранее, π_i, $i = \overline{1, \ell+1}$ - случайная перестановка столбцов матрицы.

Легко заметить, что первые ℓ слоев проверочной матрицы $\mathbf{H}$ представляют собой ничто иное, как проверочную матрицу МПП-кода Галлагера, которую мы обозначим как $\mathbf{H}_2$. Тогда проверочную матрицу $\mathbf{H}$ можно записать в следующему виде:

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_2 \\ \pi_{\ell+1}(\mathbf{H}_{b_1}) \end{pmatrix}.$$

Определение. Построенную конструкцию обобщенного МПП-кода будем называть МПП-кодом Галлагера с добавленным одним слоем, составленным из случайных линейных кодов (СЛ-Г-МПП-кодом).

Отметим, что длина получившегося кода равна $n = b_0 n_0 = b_1 n_1$, а скорость R можно найти следующим образом:

$$R \geq R_1 - \ell\,(1 - R_0)\,.$$

– или если положить скорость МПП-кода Галлагера равной R_2:

$$R \geq R_1 + R_2 - 1.$$

Определение. Равновероятно выбирая случайные перестановки π_i, $i = \overline{1, \ell+1}$, определим ансамбль $\mathscr{E}_{GL}\,(n_0, \ell, b, n_1, 1, b_1)$ СЛ-Г-МПП-кодов.

4.2. Алгоритм декодирования

Декодировать построенный СЛ-Г-МПП-код будем как каскадный код, т. е. на первом шаге декодируем принятую последовательность, используя линейные блоковые коды с проверочной матрицей $\mathbf{H}_1$ из $\ell + 1$ слоя матрицы $\mathbf{H}$. Затем полученную на предыдущем шаге последовательность декодируем, используя проверочную матрицу $\mathbf{H}_2$ МПП-кода Галлагера.

В данной работе будем рассматривать алгоритм декодирования $\mathscr{A}_C$, состоящий из следующих двух шагов:

1. последовательно декодируем по максимуму правдоподобия каждый из b_1 линейных блоковых кодов $\mathbf{H}_1$ из $\ell + 1$ слоя проверочной матрицы $\mathbf{H}$;
2. затем полученную на предыдущем шаге последовательность декодируем по мажоритарному алгоритму $\mathscr{A}_M$, используя проверочную матрицу Г-МПП-кода $\mathbf{H_2}$.

Таким образом, каждую принятую последовательность декодируем один раз сначала по максимуму прадоподобия, используя линейный коды $\mathbf{H}_1$, затем полученную последовательность декодируем по мажоритарному алгоритму, используя Г-МПП-код $\mathbf{H}_2$.

4.3. Экспонента вероятности ошибочного декодирования

При рассмотрении вероятности ошибочного декодирования P ограничемся только случаем двоично симметричного канала (ДСК) без памяти с вероятностью ошибки при передаче каждого символа p.

Оценку вероятности будем представлять ввиде:

$$P \leq \exp\left\{-nE\,(R_1, n_1, \omega_t, p)\right\},$$

где $E\,(R_1, n_1, \omega_t, p)$ – искомая экспонента вероятности ошибочного декодирования.

Теперь сформулируем следующую теорему, которая утверждает, что в ансамбле $\mathscr{E}_{GL}\,(n_0, \ell, b, n_1, 1, b_1)$ при $n \to \infty$ (т. е. $b_0 \to \infty$ и $b_1 \to \infty$) для любой скорости R меньше пропускной способности C ДСК без памяти существует СЛ-Г-МПП-код, который при декодировании по алгоритму $\mathscr{A}_C$ со сложностью $\mathcal{O}\,(n \log n)$ имеет экспоненциально малую вероятность ошибки:

Теорема 3. *Пусть в ансамбле $\mathscr{E}_G(n_0, \ell, b)$ существует МПП-код Галлагера со скростью R_2, который исправляет любую комбинацию ошибок кратности до $\lfloor \omega_t n \rfloor$ при декодировании по мажоритарному алгоритму $\mathscr{A}_M$.*

Пусть также существует линейный код с длиной n_1, скоростью R_1 и экспонентой вероятности ошибочного декодирвания по максимуму правдоподобия $E_0(R_1, p)$.

Тогда в ансамбле $\mathscr{E}_{GL}(n_0, \ell, b, n_1, 1, b_1)$ существует СЛ-Г-МПП-код с длиной n:

$$n = n_0 b_0 = n_1 b_1$$

и скоростью R:

$$R \geq R_1 + R_2 - 1$$

такой, что при передаче по ДСК без памяти с вероятностью ошибки p экспонента ошибочного декодирования со сложностью $\mathcal{O}(n \log n)$ ограничена снизу E:

$$E(R_1, n_1, \omega_t, p) = \min_{\omega_t \leq \beta \leq \beta_0} \left\{ \beta E_0(R_1, p) + E_2(\beta, \omega_t, p) - \frac{1}{n_1} H(\beta) \right\},$$

где $\beta_0 = \min\left(\frac{\omega_t}{2p}, 1\right)$, $H(\beta) = -\beta \ln \beta - (1-\beta)\ln(1-\beta)$ – функция энтропии, а $E_2(\beta, \omega_t, p)$ имеет следующий вид:

$$E_2(\beta, \omega_t, p) = \frac{1}{2}\left(\omega_t \ln \frac{\omega_t}{p} + (2\beta - \omega_t) \ln \frac{2\beta - \omega_t}{1-p}\right) - \beta \ln(2\beta),$$

при этом n_1 удовлетворяет следующим условиям:

$$\frac{-\ln \beta_0}{E_0(R_1, p)} \leq n_1 \leq \frac{1}{R_1} \log_2 \log_2(n).$$

5. ДОКАЗАТЕЛЬСТВО ОСНОВНОГО РЕЗУЛЬТАТА

Рассмотрим сначала сложность алгоритма декодирования $\mathscr{A}_C$ СЛ-Г-МПП-кода.

Лемма 1. *Сложность алгоритма $\mathscr{A}_C$ декодирования СЛ-Г-МПП-кода длины n составляет порядка $\mathcal{O}(n \log n)$, если длина линейного кода $n_1 \leq \frac{1}{R_1} log_2 log_2(n)$.*

Доказательство. Поскольку длина линейного кода равна n_1, а скорость R_1, то сложность декодирования одного кода по максимуму правдоподобия составляет порядка $\mathcal{O}\left(2^{R_1 n_1}\right)$. Всего кодов b_1, что пропорционально n, тогда сложность декодирования всех кодов пропорциональна $\mathcal{O}\left(n 2^{R_1 n_1}\right)$.

В работе [3] было показано, что сложность алгоритма декодирования $\mathscr{A}_M$ МПП-кода Галлагера составляет $\mathcal{O}(n \log n)$.

Следовательно, для того, чтобы сложность алгоритма декодирования $\mathscr{A}_C$ составляла $\mathcal{O}(n \log_2 n)$, необходимо, чтобы выполнялось следующее условие:

$$2^{R_1 n_1} \leq n \log_2(n).$$

Откуда находим условие на n_1:

$$n_1 \leq \frac{1}{R_1}\log_2\log_2(n). \tag{1}$$

Теперь докажем теорему 3.

Доказательство. Пусть на первом шаге декодирования СЛ-Г-МПП-кода по алгоритму $\mathscr{A}_C$ ровно в i линейных кодах произошла ошибка декодирования. Поскольку в каждом коде не может быть более n_1 ошибок, то количество ошибок W после первого шага декодирования будет не более in_1. Пусть $i = \beta b_1$, где β – доля линейных кодов, при декодировании которых произошла ошибка, тогда:

$$W \leq \beta b_1 n_1 = \beta n.$$

Согласно теореме 1 МПП-код Галлагера гарантированно исправляет любую комбинацию ошибок кратности:

$$W < W_0 = \lfloor \omega_t n \rfloor.$$

Следовательно, при $\beta < \omega_t$ вероятность P ошибочного декодирования СЛ-Г-МПП-кода по алгоритму $\mathscr{A}_C$ равна 0:

$$P = 0, \beta < \omega_t.$$

При $\beta > \omega_t$ вероятность ошибочного декодирования определяется следующим образом:

$$P = \sum_{i=\lfloor \omega_t b_1 \rfloor}^{b_1} \binom{b_1}{i} P_2(W \geq W_0|i) P_1^i(n_1, R_1, p)(1 - P_1(n_1, R_1, p))^{b_1 - i}, \tag{2}$$

где $P_1(n_1, R_1, p)$ – вероятность ошибочного декодирования линейного кода:

$$P_1 \leq \exp\{-n_1 E_0(R_1, p)\},$$

а $P_2(W \geq W_0|i)$ – вероятность того, что количество ошибок после первого шага алгоритма декодирования $\mathscr{A}_C$ будет не менее W_0 при условии, что ровно i линейных кодов декодировались с ошибками.

Поскольку в случае ошибочного декодирования линейного кода по максимуму правдоподобия количество ошибок в блоке не может более чем удвоиться, то для того, чтобы после первого шага декодирования по алгоритму $\mathscr{A}_C$ количество ошибок было более W_0, необходимо, чтобы изначально в i ошибочных блоках в сумме было не менее $\frac{W_0}{2}$ ошибок. Тогда $P_2(W \geq W_0|i)$ можно записать следующим образом:

$$P_2(W \geq W_0|i) = \sum_{j=\lfloor \frac{\omega_t n}{2} \rfloor}^{in_1} \binom{in_1}{j} p^j (1-p)^{in_1 - j}.$$

Используя границу Чернова, $P_2\left(W \geq W_0|i\right)$ можно оценить как:

$$P_2\left(W \geq W_0|i\right) \leq \exp\left\{-nE_2\left(\beta, \omega_t, p\right)\right\},$$

где $E_2\left(\beta, \omega_t, p\right)$:

$$E_2\left(\beta, \omega_t, p\right) = \begin{cases} \frac{1}{2}\left(\omega_t \ln\frac{\omega_t}{p} + (2\beta - \omega_t)\ln\frac{2\beta-\omega_t}{1-p}\right) - \beta\ln 2\beta,\ \beta < \beta_0 \\ 0,\ \beta \geq \beta_0 \end{cases}, \tag{3}$$

где $\beta = \frac{i}{b_1}$, а β_0:

$$\beta_0 = \min\left(\frac{\omega_t}{2p}, 1\right),$$

т.к. $\beta > 1$ не имеет смысла.

В соответствии с (3) сумму (2) можно записать следующим образом:

$$P = \sum_{i=\lfloor\omega_t b_1\rfloor}^{\lfloor\beta_0 b_1\rfloor} \binom{b_1}{i} P_2\left(W \geq W_0|i\right) P_1^i\left(n_1, R_1, p\right)\left(1 - P_1\left(n_1, R_1, p\right)\right)^{b_1-i} + \sum_{i=\lceil\beta_0 b_1\rceil}^{b_1} \binom{b_1}{i} P_1^i\left(n_1, R_1, p\right)\left(1 - P_1\left(n_1, R_1, p\right)\right)^{b_1-i}$$

Рассмотрим каждую сумму отдельно:

$$P' = \sum_{i=\lfloor\omega_t b_1\rfloor}^{\lfloor\beta_0 b_1\rfloor} \binom{b_1}{i} P_2\left(W \geq W_0|i\right) P_1^i\left(n_1, R_1, p\right)\left(1 - P_1\left(n_1, R_1, p\right)\right)^{b_1-i},$$

$$P'' = \sum_{i=\lceil\beta_0 b_1\rceil}^{b_1} \binom{b_1}{i} P_1^i\left(n_1, R_1, p\right)\left(1 - P_1\left(n_1, R_1, p\right)\right)^{b_1-i}.$$

Сумму P'' легко оценить как "хвост" биномиального распределения с вероятнстью P_1, используя границу Чернова:

$$P'' \leq \exp\left\{-nE''\left(R_1, n_1, \omega_t, p\right)\right\},$$

где $E''\left(R_1, n_1, p\right)$ можно записать как:

$$E''\left(R_1, n_1, p\right) = \beta_0 E_0\left(R_1, p\right) - \frac{1}{n_1} H\left(\beta_0\right),$$

при этом P_1 удовлетворяет условию:

$$P_1(n_1, R_1, p) \le \beta_0 \Rightarrow n_1 \ge \frac{-\ln \beta_0}{E_0(R_1, p)}. \tag{4}$$

Теперь оценим сумму P':

$$P' \le \lceil (\beta_0 - \omega_t) b_1 \rceil \max_{\omega_t \le \beta \le \beta_0} \left\{ \binom{b_1}{\beta b_1} P_2(W \ge W_0 | \beta b_1) P_1^{\beta b_1} (1 - P_1)^{(1-\beta) b_1} \right\}.$$

Откуда при $n \to \infty$ ($b_1 \to \infty$ и $b_0 \to \infty$) получаем $E'(R_1, n_1, \omega_t, p)$:

$$E'(R_1, n_1, \omega_t, p) = \min_{\omega_t \le \beta \le \beta_0} \left\{ E_2(\beta, \omega_t, p) + \beta E_0(R_1, p) - \frac{1}{n_1} H(\beta) \right\}. \tag{5}$$

Заметим, что если в правой части (5) минимум достигается при β_0, то в соотвествии с (3) $E' = E''$. Следовательно, $E' \le E''$.

Легко убедиться, что при $n \to \infty$ верно следующее;

$$P \le \exp\{-nE(R_1, n_1, \omega_t, p)\},$$

где $E(R_1, n_1, \omega_t, p) = \min\{E'(R_1, n_1, \omega_t, p), E''(R_1, n_1, p)\} = E'(R_1, n_1, \omega_t, p)$.

Согласно лемме 1 сложность алгоритма декодирования $\mathscr{A}_C$ составляет порядка $\mathcal{O}(n \log n)$, если выполняется условие (1), но для выполнения полученной оценки необходимо выполнение условия (4). Следовательно,

$$\frac{-\ln \beta_0}{E_0(R_1, p)} \le n_1 \le \frac{1}{R_1} \log_2 \log_2 n,$$

что завершает доказательство.

6. ЧИСЛЕННЫЕ РЕЗУЛЬТАТЫ

Рассмотрим зависимость минимально необходимой длины линейного кода n_1, при которой выполняется условие (4), от скорости R СЛ-Г-МПП-кода при фиксированном значении вероятности ошибки на символ $p = 0,001$. При этом полученное значение n_1 будем максимизировать по таким скоростям R_1 линейного кода и R_2 МПП-кода Галлагера, что $R = R_1 + R_2 - 1$. Данная зависимость приведена на рис. 1:

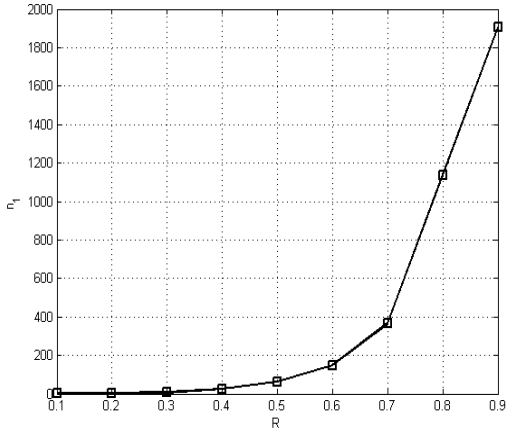

Рис. 1. Зависимость минимально необходимой длины n_1 при фиксированной вероятности ошибки $p = 0,001$ от скорости R СЛ-Г-МПП-кода

В соответствии с рис. 1 выберем длину $n_1 = 2000$ и получим зависимость экспоненты вероятности ошибки $E(R_1, n_1, \omega_t, p)$ от скорости R_1 линейного кода при фиксированной скорости $R = 0,5$ СЛ-Г-МПП-кода и вероятности ошибки $p = 0,001$. Данная зависимость приведена на рис. 2.

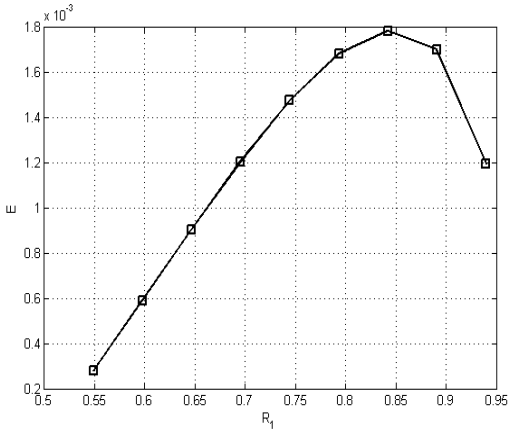

Рис. 2. Зависимость $E(R_1, n_1, \omega_t, p)$ от скорости R_1 при фиксированной скорости $R = 0,5$, длине линейного кода $n_1 = 2000$ и вероятности ошибки на бит $p = 0,001$

Как видно на рис. 2 значение $E(R_1, n_1, \omega_t, p)$ достигает максимум при скоростях $R_1 \approx 0,85$ и $R_2 = R + 1 - R_1 \approx 0,65$.

Теперь значение экспоненты будем максимизировать по таким скоростям R_1 линейного кода и R_2 МПП-кода Галлагера, что $R = R_1 + R_2 - 1$. Обозначим полученное значение следующим образом:

$$E(R,p) = \max_{R_1,R_2:R_1+R_2-1=R} E(R_1, n_1, \omega_t, p).$$

На рис. 3 представлен график зависимости $E(R,p)$ от вероятности ошибки p при фиксированной $n_1 = 2000$ и $R = 0,5$.

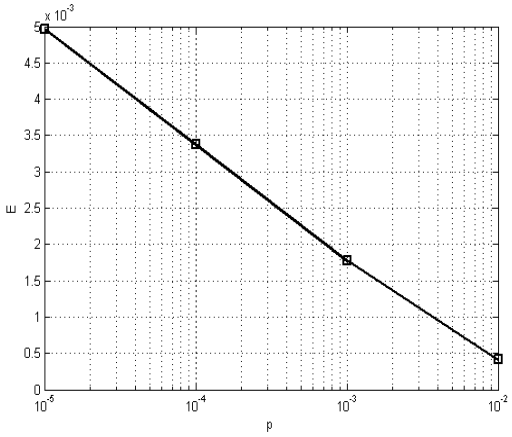

Рис. 3. Зависимость $E(R,p)$ от скорости p при фиксированной $n_1 = 2000$ и $R = 0,5$

Сравним значения $E(R,p)$ и $E_0(R,p)$ в зависимости от вероятности ошибки в канале p. Для лучшего восприятия графиков отобразим зависимости в логарифмических координатах (см. рис. 4)

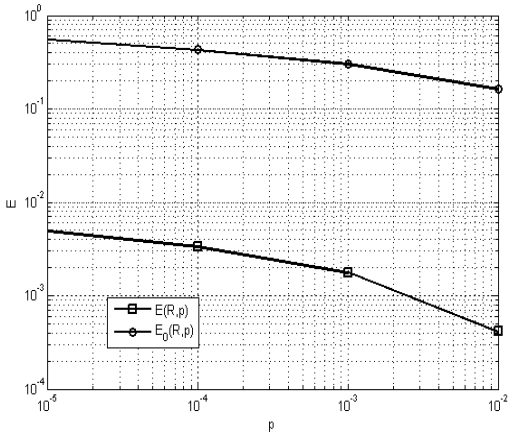

Рис. 4. Зависимость $E(R,p)$ при фиксированной $n_1 = 2000$ и $E_0(R,p)$ от вероятности p при скорости кода $R = 0,5$

Теперь найдем зависимость $E(R,p)$ от скорости R СЛ-Г-МПП-кода при заданных $n_1 = 2000$ и $p = 0,001$ (см. рис. 5). Сравним значения $E(R,p)$ и $E_0(R,p)$ в зависимости от скорости R. Для лучшего восприятия графиков отобразим зависимости в логарифмических координатах (см. рис. 6)

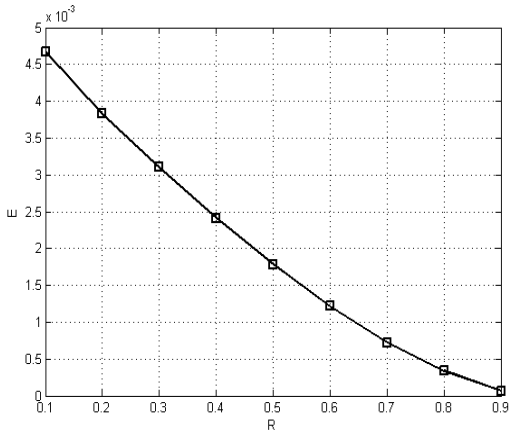

Рис. 5. Зависимость $E(R,p)$ от скорости R при фиксированной $n_1 = 2000$ и $p = 0,001$

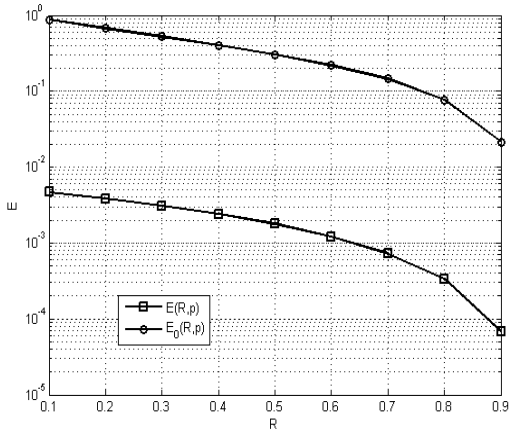

Рис. 6. Зависимость $E(R,p)$ при фиксированной $n_1 = 2000$ и $E_0(R,p)$ от скорости R при вероятности ошибки $p = 0,001$

Как видно из рис. 6 значение $E(R,p)$ меньше значения $E_0(R,p)$ примерно на два порядка. При этом стоит отметить, что сложность декодирования по алгоритму $\mathscr{A}_C$ пропорциональна $\mathcal{O}(n \log n)$, а сложность декодирования по максимуму правдоподобия – $\mathcal{O}\left(2^{Rn}\right)$. Таким образом, выбирая СЛ-Г-МПП-код в 100 раз длинее линейного кода, можно получить сравнимую вероятность ошибки декодирования при меньшей сложности декодера.

СПИСОК ЛИТЕРАТУРЫ

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

2. Зяблов В. В., Пинскер М. С. Оценка сложности исправления ошибок низкоплотностными кодами Галлагера. *Проблемы передачи информации*, 1975, том 11, № 1, стр. 23 – 26.

3. Rybin P. S., Zyablov V. V. Asymptotic estimation of error fraction corrected by binary LDPC code. *2011 IEEE International Symposium on Information Theory Proceedings (ISIT)*. 2011 , pp. 351 – 355.

4. Burshtein D., Barak O. Upper Bounds on the Error Exponents of LDPC Code Ensembles. *2006 IEEE International Symposium on Information Theory*, 2006, pp. 401 – 405.

5. Barak O., Burshtein D. Lower Bounds on the Error Rate of LDPC Code Ensembles. *IEEE Transactions on Information Theory*, 2007, vol. 53, no. 11, pp. 4225 – 4236.

6. Галлагер Р. Г. Теория информации и надежная связь. М: Сов. радио, 1974. (Gallager R. G. Information theory and reliable communication. Springer-Verlag, 1970.)

7. Блох Э. Л., Зяблов В. В. Линейные каскадные коды. М: Наука, 1982.