На правах рукописи

Рыбин Павел Сергеевич

Асимптотические оценки корректирующих свойств и сложности декодирования двоичных кодов с малой плотностью проверок

05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2012

Работа выполнена в Федеральном государственном бюджетном учреждении науки Институте проблем передачи информации им. А. А. Харкевича Российской академии наук (ИППИ РАН).

Научный руководитель:	*доктор технических наук,* **Зяблов Виктор Васильевич**
Официальные оппоненты:	**Зиновьев Виктор Александрович**, *доктор физико-математических наук, профессор, ИППИ РАН, ведущий научный сотрудник лаборатории №1* **Федоренко Сергей Валентинович**, *доктор технических наук, доцент, ФГАОУ ВПО Санкт-Петербургский государственный университет аэрокосмического приборостроения, профессор кафедры комплексной защиты информации*
Ведущая организация:	*ФГБОУ ВПО «Московский физико-технический институт (государственный университет)»*

Защита состоится «____» _____ 2012 г. в ____ часов на заседании диссертационного совета *Д 002.077.01* на базе *ИППИ РАН*, расположенном по адресу: *127994, г. Москва, ГСП-4, Большой Каретный переулок, д. 19, стр. 1.*

С диссертацией можно ознакомиться в библиотеке *ИППИ РАН.*

Автореферат разослан «____» _____ 2012 г.

Ученый секретарь
диссертационного совета Д 002.077.01
доктор физико-математических наук И. И. Цитович

Общая характеристика работы

Актуальность работы. Широкое распространение и активное развитие систем передачи и хранения информации привело к резкому увеличению требований как к скорости, так и к достоверности передачи данных по каналам связи. Согласно фундаментальным результатам теории кодирования для достижения всё меньшей вероятности ошибки необходимо использовать всё более длинные коды. При увеличении длины кода остро встают вопросы как асимптотических корректирующих свойств, так и сложности декодирования рассматриваемого кода. Таким образом, возникает задача построения и исследования эффективных кодов, имеющих алгоритмы кодирования и декодирования, реализация которых может быть осуществлена с помощью современных или предвидимых в будущем технических средств. К таким алгоритмам принято относить алгоритмы кодирования и декодирования с неэкспоненциальной сложностью.

Одним из подходов к решению данной задачи является использование кодов с малой плотностью проверок (Г-МПП кодов), предложенных Р. Г. Галлагером в 1960 г. Данные коды позволяют строить кодовые блоки большой длины. При этом они являются асимптотически "хорошими"[1] и имеют наименьшую из известных сложность декодирования. Исследованию этих кодов посвящено большое количество работ. Достаточно детально были исследованы как потенциальные, так и реализуемые асимптотические корректирующие свойства Г-МПП-кодов. К потенциальным корректирующим относят такие свойства, которые на данный момент реализуются только при использовании алгоритмов декодирования с экспоненциальной сложностью. Кодовое расстояние Г-МПП-кодов было оценено Р. Г. Галлагером в его диссертационной работе 1960 г. В работах Д. Бурштейна и О. Барака 2006 г. и 2007 г. получены верхние и нижние оценки на экспоненту вероятности ошибочного декодирования Г-МПП-кода по максимуму правдоподобия, сложность которого является экспоненциальной. Реализуемые корректирующие свойства Г-МПП-кодов исследовались в работах В. В. Зяблова и М. С. Пинксера 1974 г. и 1975 г., К. Ш. Зигангирова и Д. К. Зигангирова 2006 г., а также в работе К. Ш. Зигангирова, А. Е. Пусане, Д. К. Зигангирова и Д. Дж. Костелло 2008 г. При этом рассматривались алгоритмы декодирования с неэкспоненциальной сложностью для различных каналов связи.

В 1981 г. Р. Таннер предложил обобщеную конструкцию кода с малой плотностью проверок (МПП-кода[2]). В настоящее время обобщенные конструкции МПП-кодов вызывают всё больший интрес. Из них детально были иссле-

[1] Под асимптотически "хорошими" кодами будем понимать коды, у которых минимальное кодовое расстояние растет линейно с длиной кода.

[2] Здесь и далее под МПП-кодом будем понимать код с малой плотностью проверок с некоторым заданным компонентным кодом, в том числе и кодом с проверкой на четность.

дованы МПП-коды с компонентым кодом Хэмминга (Х-МПП-коды). Потенциальные корректирующие свойства рассматривались в работе К. Ш. Зигангирова и М. Лентмайера 1999 г. и в работе В. В. Зяблова и С. Стиглмайера 2007 г. А реализуемые корректирующие свойства Х-МПП-кода исследовались в работе В. В. Зяблова, Р. Йоханнессона и М. Лончар 2009 г., а также в работе А. Барга и А. Мазумдара 2011 г. Однако, в предыдущих работах при исследовании алгоритмов декодирования обобщенных конструкций МПП-кодов особенности декодирования компонентных кодов учитывались не в полной мере.

Таким образом, на данный момент особый теоретический интерес имеет исследование свойств различных конструкций обобщенных МПП-кодов. При этом как теоретическое, так и практическое значение имеет исследование алгоритмов декодирования МПП-кодов с неэкспоненциальной сложностью. Следовательно, возникает задача исследования реализуемых корректирующих свойств обобщенных МПП-кодов.

Цель диссертационной работы состоит в исследовании асимптотических корректирующих свойств двоичных МПП-кодов при использовании алгоритмов декодирования, имеющих наименьшую из известных сложность и при этом экспоненциально убывающую вероятность ошибочного декодирования.

В качестве основных реализуемых корректирующих свойств были выбраны следующие:

- доля гарантированно исправимых стираний;
- доля гарантированно исправимых ошибок;
- экспонента вероятности ошибочного декодирования,

для которых необходимо получить оценки снизу при декодировании двоичного МПП-кода по алгоритму с наименьшей из известных сложностью.

Научная новизна состоит в следующем:

- Разработан новый метод оценки доли гарантированно исправимых стираний при декодировании МПП-кода по алгоритму с наименьшей из известных сложностью, основанный на учете особенностей декодирования компонетных кодов. Данный метод позволил улучшить ранее известные лучшие оценки для Г-МПП-кода и впервые получить оценку для Х-МПП-кода.
- Разработан новый метод оценки доли гарантированно исправимых ошибок при декодировании МПП-кода по алгоритму с наименьшей из известных сложностью, основанный на учете особенностей декодирования компонентных кодов. Данный метод позволил улучшить ранее известные лучшие оценки для Г-МПП-кода и Х-МПП-кода.

- Предложена новая конструкция МПП-кода и алгоритм его декодирования;

- Впервые показано, что существуют МПП-коды с предложенной конструкцией, для которых вероятность ошибки эспоненциально убывает для всех скоростей меньше пропускной способности при декодировании с наименьшей из известных сложностью.

Практическая значимость. Работа носит теоретический характер. Результаты, изложенные в диссертации, могут быть использованы для оценки корректирующих свойств и выбора оптимальных параметров различных конструкций МПП-кодов при разработке новых систем связи и стандартов передачи данных.

На защиту выносятся следующие положения:

- получена асимптотическая оценка как доли стираний, так и доли ошибок, гарантированно исправимых обобщенным МПП-кодом с заданным компонентным кодом, при декодировании по алгоритму с наименьшей из известных сложностью, учитывающему особенности декодирования компонентых кодов;

- предложена конструкция МПП-кода и алгоритм его декодирования;

- получена асимптотическая оценка экспоненты вероятности ошибочного декодирования предложенного МПП-кода по алгоритму с наименьшей из известных сложностью;

- показано, что для всех кодовых скоростей меньше пропускной способности существует МПП-код с предложенной конструкцией, при декодировании которого по алгоритму с наименьшей из известных сложностью вероятность ошибки убывает экспоненциально.

Апробация работы. Основные результаты диссертации докладывались на следующих конференциях: IEEE International Symposium on Information Theory (2011), 5th International Symposium on Turbo Codes and Related Topics (2008), International Workshop on Algebraic and Combinatorial Coding Theory (2008, 2010), XII Symposium on Problems of redundancy in information and control systems (2009), конференциях молодых ученных и специалистов ИППИ РАН "Информационные технологии и системы" (2008, 2010, 2011), всероссийских научно-технических конференциях "Актуальные проблемы ракетно-космического приборостроения и информационных технологий" (2010, 2011). Кроме того, основные результаты докладывались на семинарах по теории кодирования в ИППИ РАН, а также в Математическом институте им. А. Реньи Венгерской академии наук.

Публикации. Материалы диссертации опубликованы в 15 печатных работах, из них 3 статьи в рецензируемых журналах [3, 5, 8], 10 статей в сборниках трудов конференций [1, 2, 4, 9–15] и тезисах 2 докладов [6, 7].

Личный вклад автора. Все основные научные положения и выводы, составляющие содержание диссертации, разработаны автором самостоятельно. Теоретические и практические исследования, а также вытекающие из них выводы и рекомендации проведены и получены автором лично.

Подготовка к публикации полученных результатов проводилась совместно с соавторами. Все теоретические результаты работ [2–5, 9, 11–14] получены автором самостоятельно. В работах [1, 6–8, 10, 15] автору принадлежит разработка алгоритмов декодирования двоичных МПП-кодов и проведение имитационного моделирования.

Структура и объем диссертации. Диссертация состоит из введения, обзора литературы, трех глав, заключения и библиографии. Общий объем диссертации 131 страница, включая 51 рисунок и 10 таблиц. Библиография включает 73 наименования на 10 страницах.

Содержание работы

Во Введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

В первой главе исследуются корректирующие свойства двоичного МПП-кода при передаче по симметричному стирающему каналу (ССК). Результаты опубликованы в работе [3].

В § 1.1 приведено введение к главе 1.

В § 1.2 описана струкртура двоичного МПП-кода. Рассмотрим построение проверочной матрицы $\mathbf{H}$ обобщенного МПП-кода, компонентный код которого имеет проверочную матрицу $\mathbf{H}_0$. Запишем диагональную блочную матрицу $\mathbf{H}_{b_0}$ с b_0 проверочными матрицами $\mathbf{H}_0$ на главной диагонали:

$$\mathbf{H}_{b_0} = \left(\underbrace{\begin{matrix} \mathbf{H}_0 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0 \end{matrix}}_{b_0} \right),$$

где b_0 очень велико. Если размер матрицы $\mathbf{H}_0$ равен $m_0 \times n_0$, тогда размер матрицы $\mathbf{H}_{b_0}$ – $b_0 m_0 \times b_0 n_0$. Обозначим $\pi\left(\mathbf{H}_{b_0}\right)$ случайную перестановку столб-

цов матрицы $\mathbf{H}_{b_0}$. Тогда матрица, составленная из $\ell > 2$ таких перестановок в качестве слоев,

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \\ \vdots \\ \mathbf{H}_\ell \end{pmatrix} = \begin{pmatrix} \pi_1(\mathbf{H}_{b_0}) \\ \pi_2(\mathbf{H}_{b_0}) \\ \vdots \\ \pi_\ell(\mathbf{H}_{b_0}) \end{pmatrix}$$

является разреженной проверочной матрицей $\mathbf{H}$ размера $\ell b_0 m_0 \times b_0 n_0$, которая определяет ансамбль обобщенного МПП-кода длины $n = b_0 n_0$, где $n \gg n_0$, с заданным кодом-компонентом с проверочной матрицей $\mathbf{H}_0$. Обозначим этот ансамбль $\mathscr{E}(n_0, \ell, b_0)$.

О п р е д е л е н и е 1.1. Для заданного компонентного кода с проверочной матрицей $\mathbf{H}_0$ независимо и равновероятно выбирая случайные перестановки π_l , $l = 1, 2, ..., \ell$, определим ансамбль обобщенных МПП-кодов $\mathscr{E}(n_0, \ell, b_0)$.

Таким образом, ансамбль МПП-кодов с компонентным кодом с проверкой на четность, т.е. ансамбль Г-МПП-кодов, будем обозначать $\mathscr{E}_G(n_0, \ell, b_0)$, а ансамбль МПП-кодов с компонетным кодом Хэмминга, т.е. ансамбль Х-МПП-кодов, будем обозначать $\mathscr{E}_H(n_0, \ell, b_0)$. А обозначение $\mathscr{E}(n_0, \ell, b_0)$ будем понимать как ансамбль МПП-кодов с заданным компонентным кодом (в том числе и с кодом с проверкой на четности и кодом Хэмминга). В случае необходимости компонентный код будет указываться явно, иначе ансамбль $\mathscr{E}(n_0, \ell, b_0)$ стоит рассматривать как ансамбль МПП-кодов с некоторым заданным компонентным кодом.

В § 1.3 получена новая асимптотическая оценка доли гарантированно исправимых стираний при декодировании двоичного МПП-кода по алгоритму со сложностью $\mathcal{O}(n \log_2 n)$. Впервые оценка доли гарантированно исправимых стираний для Г-МПП-кода была получена В. В. Зябловым и М. С. Пинскером. Затем К.Ш. Зигангиров и Д.К. Зигангиров получили оценку доли гарантированно исправимых стираний для Г-МПП-кода с проверочной матрицей, составленной из перестановочных матриц. *В отличие от предыдущих оценок, полученных комбинаторными методами, новая оценка использует метод производящих функций. Это позволяет получить более точные результаты и унифицировать метод расчета доли гарантированно исправимых стираний для МПП-кода с любым компонентным кодом и любым алгоритмом декодирования этого кода-компонента, для которых известны производящие функции исправимых и неисправимых комбинаций стираний.*

Описание алгоритма декодирования $\mathscr{A}_\tau$ приводится в § 1.3.1. Идея алгоритма декодирования заключается в поиске исправимых комбинаций стираний кратности не более τ, вошедших в компонентные коды МПП-кода, и в последующем их исправлении.

В § 1.3.2 формулируется основной результат в виде следующей теоремы:

Т е о р е м а 1.1. *Пусть существует хотя бы один положительный*

корень и ω_τ *– минимальный из этих корней следующего уравнения:*

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

где $F(\alpha, \omega, n_0)$ *определяется выражением:*

$$F(\alpha, \omega, n_0) \stackrel{\Delta}{=} h(\omega) - \frac{1}{n_0} h(\alpha\omega n_0) +$$

$$+ \max\{\omega \log_2 s - \frac{1}{n_0} \log_2(g_0(s, n_0)) - \alpha\omega \log_2 \left(\frac{g_1(s, n_0)}{g_0(s, n_0)}\right)\},$$

где $\alpha > 0$ *- доля кодов с исправимыми стираниями (свободный параметр, определяющий константу перед оценкой сложности декодирования), и максимизация производиться по всем* s*, удовлетворяющим неравенству:*

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

Тогда в ансамбле $\mathscr{E}(n_0, \ell, b_0)$ *существует код, который может исправить любую комбинацию стираний кратности до* $\lfloor \omega_\tau n \rfloor$ *со сложностью декодирования порядка* $\mathcal{O}(n \log n)$.

В формулировке теоремы использовались следующие обозначения:

- $g_0(s, n_0) = \sum\limits_i G_0^{(i)} s^i$ – производящая функция количества $G_0^{(i)}$ неисправимых комбинаций стираний кратности i для заданного кода с длиной n_0;
- $g_1(s, n_0) = \sum\limits_i G_1^{(i)} s^i$ – производящая функция количества $G_1^{(i)}$ исправимых комбинаций стираний кратности i для заданного кода с длиной n_0;
- $h(\omega) = -\omega \log_2 \omega - (1 - \omega) \log_2 (1 - \omega)$ – функция двоичной энтропии.

Таким образом, *подставляя производящие функции* $g_0(s, n_0)$ *и* $g_1(s, n_0)$*, соответствующие компонентному коду и его алгоритму декодирования, получаем нижнюю оценку доли гарантированно исправимых стираний для МПП-кода с заданным компонентным кодом.* В дальнейшем рассматриваются только Г-МПП-коды и Х-МПП-коды.

В § 1.3.3 приводится доказательство теоремы 1.1.

В § 1.3.4, § 1.3.5 и § 1.3.5 анализируются численные значени оценок доли гарантированно исправимых стираний для Г-МПП-кодов и Х-МПП-кодов. При этом для Г-МПП-кодов рассматривается алгоритм декодирования $\mathscr{A}_{\tau=1}$,

т.к. код с проверкой на четность гарантированно исправляет только одно стирание. А для Х-МПП-кодов рассматриваются два алгоритма декодирования $\mathscr{A}_{\tau=2}$ и $\mathscr{A}_{\tau=m_0}$, т.к. код Хэмминга гарантированно исправляет любую комбинацию из 2 и менее стираний, а также некоторые комбинации стираний кратности более 2 и менее m_0. На рис. 1 сравниваются максимальные значения новой оценки ($\omega_{\tau=1}$) и оценки (ω_0), полученной В. В. Зябловым и М. С. Пинскером в 1974 г., в зависимости от скорости R Г-МПП-кода при декодировании по алгоритму $\mathscr{A}_{\tau=1}$. Видно, что новая оценка превосходит оценку 1974 г. На рис. 2 приведены максимальные значения новой оценки ($\omega_{\tau=2}$ и $\omega_{\tau=m_0}$) при декодировании по алгоритмам $\mathscr{A}_{\tau=2}$ и $\mathscr{A}_{\tau=m_0}$ в зависимости от скорости R Х-МПП-кода. Видно, что использование алгоритма $\mathscr{A}_{\tau=m_0}$ дает значительный выигрыш по сравнению с алгоритмом $\mathscr{A}_{\tau=2}$.

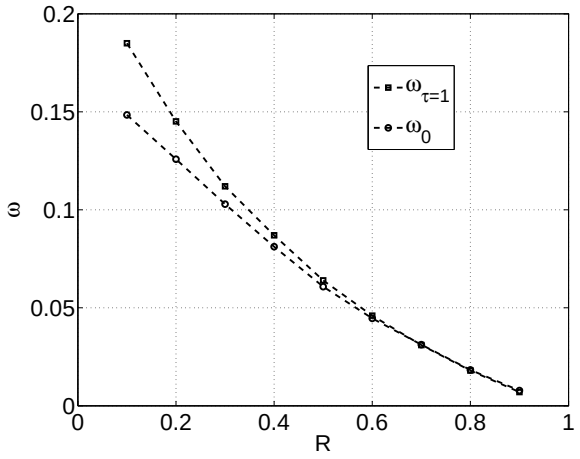

Рис. 1. Зависимость максимального значения доли $\omega_{\tau=1}$ и ω_0 от скорости R Г-МПП-кода

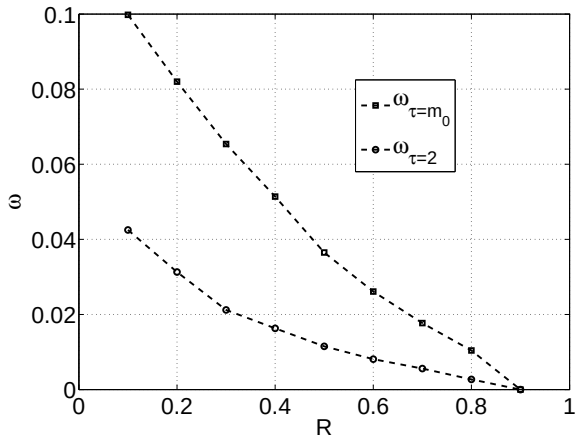

Рис. 2. Зависимость максимального значения доли $\omega_{\tau=2}$ и $\omega_{\tau=m_0}$ для алгоритмов $\mathscr{A}_{\tau=2}$ и $\mathscr{A}_{\tau=m_0}$ от скорости R Х-МПП-кода

В § 1.4 приведены результаты имитационного моделирования для ССК алгоритмов декодирования $\mathscr{A}_{\tau=1}$ для Г-МПП-кода и $\mathscr{A}_{\tau=m_0}$ для Х-МПП-кода. Рассматривались коды со скоростями R, примерно равными $0,25$, $0,5$ и $0,75$, длиной $n \approx 2000$, различным количеством слоев и соотвествующей длиной кода-компонента. Из полученных результатов следует, что для всех рассмотренных скоростей вероятность отказа на блок 10^{-5} для Г-МПП-кода достигается при больших значениях входной вероятности стирания, чем для Х-МПП-кода. Таким образом, в этом смысле Г-МПП-код имеет лучшие корректирующие свойства, чем Х-МПП-код. При этом стоит отметить, что оценка доли гарантированно исправимых стираний для Г-МПП-кода также превосходит аналогичную оценку для Х-МПП-кода.

В § 1.5 перечислены основные результаты главы.

Во второй главе исследуются корректирующие свойства двоичного МПП-кода при передаче по двоично-симметричному каналу (ДСК). Резуль-

таты опубликованы в работах [8, 11].

В § 2.1 приведено введение к главе 2.

В § 2.2 получена новая асимптотическая оценка доли гарантированно исправимых ошибок при декодировании двоичного МПП-кода по алгоритму со сложностью $\mathcal{O}(n \log_2 n)$. Впервые оценка доли гарантированно исправимых ошибок для Г-МПП-кода была получена В. В. Зябловым и М. С. Пинскером. Данная оценка является наилучшей из известных для Г-МПП-кодов. Наилучшую из известных оценок для Х-МПП-кодов получили А. Барг и А. Мазумдар. *В отличие от предыдущих работ в новой оценке учитываются особенности декодировани компонентных кодов, т. е. учитывается не только количество проверочных соотношений, которые станут выполненными после замены символа, но также и количество проверочных соотношений, которые останутся невыполненными после замены символа. Это позволяет смягчить условие на существование символа, замена которого уменьшит количество невыполненных проверочных соотношений, что приводит к значительному увеличению значений новой оценки.*

Описание итеративного мажоритарного алгоритма декодирования $\mathscr{A}_M$ приводится в § 2.2.1. Идея алгоритма декодирования заключается в уменьшении количества невыполненных проверочных соотношений на каждой итерации декодирования. Для данного алгоритма получено условие существования хотя бы одного символа, замена которого уменьшит количесто невыполненных проверочных соотношений, при входной комбинации ошибок кратности W:

$$E_{\sum}^{(W)} = 2\sum_{j=1}^{W} e_{A_{1\to 0}}^{(i_j)} + \sum_{j=1}^{W} e_{A_{1\to 1}}^{(i_j)} > W\ell, \tag{1}$$

где $e_{A_{1\to 0}}^{(i_j)}$ – количество проверок, которые станут выполненными после замены i_j-ого символа, а $e_{A_{1\to 1}}^{(i_j)}$ – количество проверок, которые останутся невыполненными после замены i_j-ого символа.

В § 2.2.2 формулируется основной результат в виде следующей теоремы:

Т е о р е м а 2.1. *Пусть существует хотя бы один положительный корень и ω_0 – минимальный из этих корней 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 хотя бы один положительный корень и α_0 – минимальный из этих корней следующего урав-

нения:

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

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 $\mathscr{E}(n_0, \ell, b_0)$ *существует код, который может исправить любую комбинацию ошибок кратности до* $\lfloor \omega_t n \rfloor$*, где* $\omega_t = \alpha_0 \omega_0$*, со сложностью декодирования порядка* $\mathcal{O}(n \log n)$*.*

В формулировки теоремы использовались следующие обозначения:

- $g_0(s, n_0) = \sum_i G_0^{(i)} s^i$ – производящая функция количества $G_0^{(i)}$ кодовых слов веса i заданного кода с длиной n_0;
- $g_1(s, n_0) = \sum_i G_1^{(i)} s^i$ – производящая функция количества $G_1^{(i)}$ комбинаций i ошибок, обнаруживаемых заданным кодом с длиной n_0;
- $g_e(s, v, n_0) = \sum_i \sum_j G_e^{(i,j)} s^j v^i$ – производящая функция количества таких $G_e^{(i,j)}$ комбинаций j ошибок, что $E_{\sum}^{(W)}$ (см. (1)) равна в точности i.

Таким образом, *подставляя производящие функции* $g_0(s, n_0)$, $g_1(s, n_0)$ *и* $g_e(s, v, n_0)$*, соответствующие компонентному коду, получаем нижнюю оценку доли гарантированной исправимых ошибок для МПП-кода с заданными компонентым кодом.* В дальнейшем рассматриваются только Г-МПП-коды и Х-МПП-коды.

В § 2.2.3 приводится доказательство теоремы 2.1.

В § 2.2.4, § 2.2.5 и § 2.2.6 анализируются численные значения оценок доли гарантированно исправимых ошибок для Г-МПП-кодов и Х-МПП-кодов. На рис. 3 сравниваются максимальные значения новой оценки (ω_t) и оценки ($\omega_\alpha/2$), полученной В. В. Зябловым и М. С. Пинскером в 1975 г., в зависимости от скорости R Г-МПП-кода. Видно, что новая оценка улучшает оценку 1975 г. для Г-МПП-кодов. На рис. 4 сравниваются значения новой оценки (ω_t) и оценки ($\gamma_0/2$), полученной А. Баргом и А. Мазумдаром 2011 г., в зависимости от длины кода-компонента n_0 Х-МПП-кода со скоростью $R = 0,5$. Видно, что предложенная оценка улучшает оценку 2011 г. для Х-МПП-кодов.

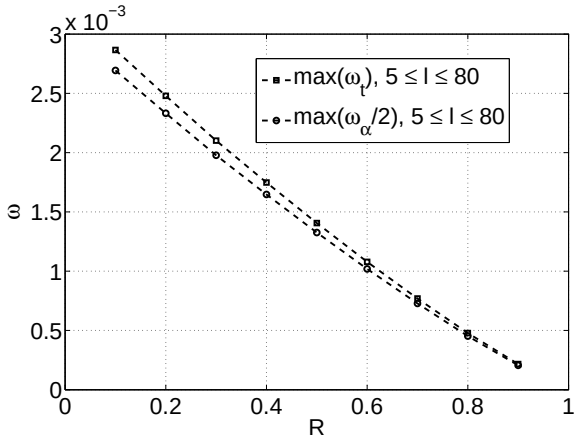

Рис. 3. Зависимость максимального значения доли ω_t и $\omega_\alpha/2$ от скорости R Г-МПП-кода

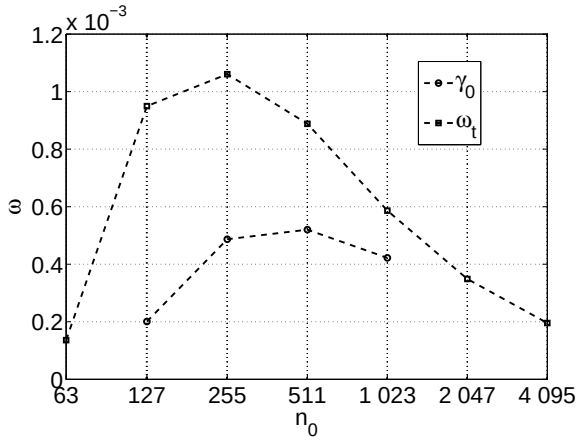

Рис. 4. Зависимость значения доли ω_t и $\gamma_0/2$ от длины кода-компонента n_0 Х-МПП-кода со скоростью $R = 0,5$

В § 2.3 приведены результаты имитационного моделирования для ДСК алгоритма декодирования $\mathscr{A}_M$ для Г-МПП-кода и Х-МПП-кода. Рассматривались коды со скоростями R, примерно равными $0,25$, $0,5$ и $0,75$, длиной $n \approx 2000$, различным количеством слоев и соотвествующей длиной кода-компонента. Из полученных результатов следует, что для всех рассмотренных скоростей вероятность отказа на блок 10^{-5} для Г-МПП-кода достигается при больших значения входной вероятности ошибки, чем для Х-МПП-кода. Таким образом, в таком смысле Г-МПП-код имеет лучшие корректирующие свойства, чем Х-МПП-код. При этом стоит отметить, что оценка доли гарантированно исправимых ошибок для Г-МПП-кода также превосходит аналогичную оценку для Х-МПП-кода.

Так же для Г-МПП-кода исследован новый алгоритм декодирования с введением стираний $\mathscr{A}_*$. Основная идея данного алгоритма заключается в том, что на позиции подозрительных символов (т.е. символов, удовлетворяющих критерию замены) устанавливаются стирания, а затем исправляются только стирания. По завершении каждой итерации на места стираний, если они не были исправлены, устанавливаются изначальные (принятые) значения. Из полученных результатов следует, что для всех рассматриваемых кодовых скоростей предложенный алгоритм $\mathscr{A}_*$ имеет лучшие корректирующие свойства, чем $\mathscr{A}_M$, т.е. при декодировании по алгоритму $\mathscr{A}_*$ вероятность отказа на блок 10^{-5} достигается при больших значениях входной вероятности ошибки, чем при декодировании по алгоритму $\mathscr{A}_M$. При этом следует отметить, что предложенный алгоритм $\mathscr{A}_*$ является универсальным и может быть использован не только в канале с ошибками, но также и в канале со стираниями и канале с ошибками и стираниями.

В § 2.4 перечислены основные результаты главы.

В третьей главе исследуется МПП-код со специальной контрукцией и его корректирующие свойства при передаче по ДСК. Результаты опубликованы в работе [5].

В § 3.1 приведено введение к главе 3.

В § 3.2 описывается исследуемая конструкция МПП-кода. Пусть $\mathbf{H}_2$ – проверочная матрица Г-МПП-кода со скростью R_2 из ансамбля $\mathscr{E}_G(n_0, \ell, b_0)$, т.е. длина Г-МПП-кода $n = n_0 b_0$. Пусть $\mathbf{H}_1$ – проверочная матрица линейного блокового кода со скоростью R_1 и длиной n_1. Рассмотрим блочную диагональную матрицу $\mathbf{H}_{b_1}$, на главной диагонали которой стоят b_1 проверочных матриц $\mathbf{H}_1$:

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

где b_1 такая, что $b_1 n_1 = b_0 n_0$. Тогда, проверочную матрицу рассматриваемой конструкции МПП-кода можно записать следующий образом:

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_2 \\ \pi(\mathbf{H}_{b_1}) \end{pmatrix},$$

где $\pi(\mathbf{H}_{b_1})$, как и раньше, обозначает случайную перестановку столбцов матрицы $\mathbf{H}_{b_1}$.

О п р е д е л е н и е 3.1. Построенную конструкцию МПП-кода будем называть Г-МПП-кодом с добавленным одним слоем, составленным из линейных кодов (СЛ-Г-МПП-кодом).

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

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

О п р е д е л е н и е 3.2. Равновероятно выбирая проверочную матрицу $\mathbf{H}_2$ из ансамбля $\mathscr{E}_G(n_0, \ell, b_0)$ и случайную перестановку π, определим ансамбль $\mathscr{E}_L(n_0, \ell, b_0, n_1, 1, b_1)$ СЛ-Г-МПП-кодов.

В § 3.3 получена асимптотическая оценка экспоненты вероятности ошибочного декодирования МПП-кода со специальной конструкцией при передаче по ДСК без памяти. *Впервые показано, что при передаче по ДСК без памяти в ансамбле СЛ-Г-МПП-кодов существуют коды, при декодировании которых по алгоритму со сложностью $\mathcal{O}(n \log_2 n)$ вероятность ошибочного декодирования убывает экспоненциально для всех скоростей меньше пропускной способности канала.*

Алгоритм декодирования $\mathscr{A}_C$ описан в § 3.3.1. Идея алгоритма декодирования заключается в том, что каждую принятую последовательность алгоритм $\mathscr{A}_C$ декодирует только один раз. Сначала – по максимуму прадоподобия, используя независимо каждый линейный код с проверочной матрицей $\mathbf{H}_1$ из добавленного слоя, затем полученную последовательность декодирует по мажоритарному алгоритму $\mathscr{A}_M$, используя Г-МПП-код с проверочной матрицей $\mathbf{H}_2$.

Оценку вероятности ошибочного декодирования по алгоритму $\mathscr{A}_C$ для ДСК без памяти с вероятностью искажения символа p_t представим следующим образом:

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

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

В § 3.3.2 формулируется основной результат в виде следующей теоремы:

Т е о р е м а 3.1. *Пусть в ансамбле $\mathscr{E}_G\left(n_0, \ell, b_0\right)$ существует Г-МПП-код 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 $E_0\left(R_1, p_t\right)$.

Тогда в ансамбле $\mathscr{E}_L\left(n_0, \ell, b_0, n_1, 1, b_1\right)$ 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_t экспонента ошибочного декодирования со сложностью $\mathcal{O}\left(n \log n\right)$ ограничена снизу E:

$$E\left(R_1, n_1, \omega_t, p_t\right) = \min_{\omega_t \leq \beta \leq \beta_0} \left\{ \beta E_0\left(R_1, p_t\right) + E_2\left(\beta, \omega_t, p_t\right) - \frac{1}{n_1} H\left(\beta\right) \right\}, \qquad (2)$$

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

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

при этом n_1 удовлетворяет следующим условиям:

$$\frac{-\ln \beta_0}{E_0(R_1, p_t)} \leq n_1 \leq \frac{1}{R_1}\log_2\log_2(n). \tag{3}$$

В самом общем виде нижняя оценка на $E_0(R_1, p_t)$ для линейных кодов была получена Р. Г. Галлагером, откуда следует, что существуют коды, для которых $E_0(R_1, p_t) > 0$ для $R_1 < \mathscr{C}$, где $\mathscr{C}$ – пропускная способность ДСК без памяти с вероятностью ошибки p_t. *Тогда из (2) видно, что если $R \to \mathscr{C}$ так, что $R_1 < \mathscr{C}$ и $R_2 < 1$, то можно подобрать такое n_1, удовлетворяющее условию (3), что $E(R_1, n_1, \omega_t, p_t) > 0$, если $\omega_t > 0$ для $\forall R_2 < 1$.*

В § 3.3.3 приводится доказательство теоремы 3.1.

В § 3.3.4 анализируются численные значения оценки экспоненты вероятности ошибочного декодирования СЛ-Г-МПП-кода. Значение экспоненты вероятности ошибки будем максимизировать по таким скоростям R_1 линейного кода и R_2 Г-МПП-кода, что $R = R_1 + R_2 - 1$. Обозначим полученное значение следующим образом:

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

Рассмотрим зависимость $E(R, p)$ от скорости R СЛ-Г-МПП-кода при фиксированной длине линейного кода $n_1 = 2000$ и входной вероятности ошибки $p = 0,001$. Из рис. 5 видно, что полученная оценка $E(R, p)$ уступает наилучшей известной экспоненте вероятности ошибочного декодирования $E_0(R, p)$ примерно два порядка при $p = 0,001$. При этом сложность декодирования СЛ-Г-МПП-кода с экспонентой вероятности ошибки $E(R, p)$ составляет порядка $\mathcal{O}(n \log n)$, а сложность декодирования линейного кода по максимуму правдоподобия с экспонентой вероятности ошибки $E_0(R, p)$ составляет порядка $\mathcal{O}(2^n)$.

В § 3.4 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_C$ для различных параметров СЛ-Г-МПП-кода. В качетсве линейных кодов были выбраны коды БЧХ (31, 21) и (63, 39). Рассматривались коды длины $n \approx 2000$, с количеством слоев в диапазоне $\ell = 3, 4, ..., 7$ и скоростям R, примерно равными $0,25$ и $0,5$. Из полученных результатов следует, что СЛ-Г-МПП-код с кодом БЧХ (63, 39) имеет лучшие корректирующие свойства, чем СЛ-Г-МПП-код с кодом БЧХ (31, 21), в том смысле, что вероятность отказа от декодирования 10^{-5} достигается при больших значениях входной вероятности ошибки. Важно отметить, что при некоторых значениях p_t экспериментально полученная экспонента вероятности ошибочного декодирования значительно превосходит полученную оценку.

В § 3.5 перечислены основные результыта главы.

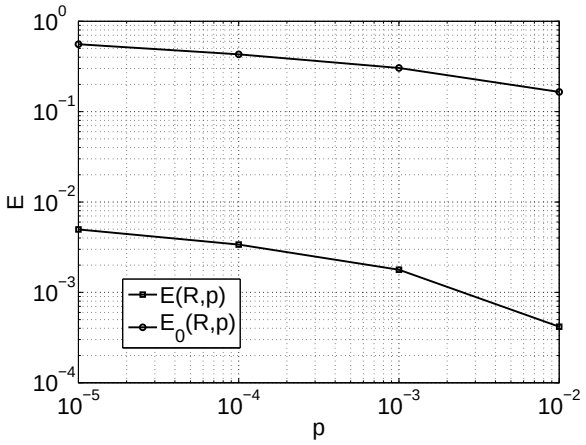

Рис. 5. Зависимость $E(R,p)$ при фиксированной $n_1 = 2000$ и $E_0(R,p)$ от скорости R при вероятности ошибки $p = 0,001$

В Заключении приведены основные результаты, полученные в диссертационной работе:

- получена новая оценка доли гарантированно исправимых стираний при декодировании МПП-кода со сложностью $\mathcal{O}(n \log n)$;
- численно показано, что полученная оценка превосходит лучшую известную оценку доли гарантированно исправимых стираний при декодировании Г-МПП-кода со сложностью $\mathcal{O}(n \log n)$;
- впервые получена оценка доли гарантированно исправимых стираний при декодировании Х-МПП-кода по двум алгоритмам: по алгоритму, гарантированно исправляющему не более двух стираний в компонентном коде, и по алгоритму, гарантированно исправляющему не более двух стираний и некоторые комбинации стираний большей кратности до m_0 в комопнентном коде;
- получена новая оценка доли гаратированно исправимых ошибок при декодировании МПП-кода со сложностью $\mathcal{O}(n \log n)$;
- численно показано, что полученная оценка превосходит лучшие известные оценки доли гарантированно исправимых ошибок при декодировании Г-МПП-кода и Х-МПП-кода со сложностью $\mathcal{O}(n \log n)$;
- предложен новый алгоритм декодирования с вводом стираний;
- предложена новая конструкция МПП-кодов (СЛ-Г-МПП-коды) и алгоритм их декодирования;

- впервые получена оценка экспоненты вероятности ошибочного декодирования СЛ-Г-МПП-кода по предложенному алгоритму со сложностью $\mathcal{O}(n \log n)$;

- впервые показано, что при передаче по ДСК без памяти существует СЛ-Г-МПП-код, при декодировании которого со сложностью $\mathcal{O}(n \log n)$ вероятность ошибки убывает экспоненциально для любой скорости меньше пропускной способности.

Список публикаций

1. Жилин И. В., Рыбин П. С., Зяблов В. В. Сравнение алгоритмов декодирования двоичных МПП-кодов с жестким входом // Сборник трудов конференции информационные технологии и системы (ИТиС'11), Геленджик, Россия. М: ИППИ РАН, 2011. С. 221 – 227.

2. Зяблов В. В., Рыбин П. С. Исправление стираний низкоплотностными кодами Галлагера // Сборник трудов конференции информационные технологии и системы (ИТиС'08), Геленджик, Россия. М: ИППИ РАН, 2008. С. 167 – 172.

3. Зяблов В. В., Рыбин П. С. Исправление стираний кодами с малой плотностью проверок // Пробл. передачи информ. 2009. Т. 45, № 3. С. 15—32.

4. Зяблов В. В., Рыбин П. С. Оценивание в графе Таннера числа ребер с заданными свойствами // Сборник трудов конференции информационные технологии и системы (ИТиС'10), Геленджик, Россия. М: ИППИ РАН, 2010. С. 79 – 84.

5. Зяблов В. В., Рыбин П. С. Оценка экспоненты вероятности ошибки декодирования обобщенного МПП-кода специальной конструкции // Информационные процессы. 2012. Т. 12, № 1. С. 84—97.

6. Зяблов В. В., Рыбин П. С., Жилин И. В. и др. Применение помехоустойчивых кодов с малой плотностью проверок (МПП) в радиолиниях ДЗЗ // IV Всероссийская научно-техническая конференция "Актуальные проблемы ракетно-космического приборостроения и информационных технологий". 2011. С. 79.

7. Зяблов В. В., Рыбин П. С., Петров С. В., Пятошин Ю. П. Сравнительная оценка практической целесообразности использования современных сигнально-кодовых конструкций в высокоскоростных радиолиниях // III

Всероссийская научно-техническая конференция “Актуальные проблемы ракетно-космического приборостроения и информационных технологий”. 2010. С. 101.

8. Зяблов В. В., Рыбин П. С., Фролов А. А. Алгоритм декодирования с вводом стираний для МПП-кодов, построенных над полем GF(q) // Информационно-управляющие системы. 2011. Т. 50, № 1. С. 62—68.

9. Рыбин П. С., Зяблов В. В. Оценка доли гарантированно исправимых ошибок двоичным Х-МПП-кодом // Сборник трудов конференции информационные технологии и системы (ИТиС’11), Геленджик, Россия. М: ИППИ РАН, 2011. С. 189 – 194.

10. Rybin P., Zyablov V. Decoding with Erasure Insertion of Binary LDPC Codes // XII International Symposium on Problems of redundancy in information and control systems, St. Petersburg, Russia. 2009. P. 150 – 154.

11. Rybin P., Zyablov V. Asymptotic estimation of error fraction corrected by binary LDPC code // Proceedings of IEEE International Symposium on Information Theory (ISIT), St. Petersburg, Russia. 2011. P. 351 – 355.

12. Zyablov V., Loncar V., Johannesson R., Rybin P. On the Asymptotic Performance of Low-Complexity Decoded LDPC Codes with Constituent Hamming Codes // 5th International Symposium on Turbo Codes and Related Topics, Lausanne, Switzerland. 2008. P. 174 –179.

13. Zyablov V., Loncar V., Johannesson R., Rybin P. On the Erasure-Correcting capabilities of Low-Complexity Decoded LDPC Codes with Constituent Hamming Codes // Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria. 2008. P. 338 – 347.

14. Zyablov V., Loncar V., Johannesson R., 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, Pamporovo, Bulgaria. 2008. P. 326 – 337.

15. Zyablov V., Rybin P. Majority decoding and decoding with erasure insertion of binary LDPC codes // Twelfth International Workshop on Algebraic and Combinatorial Coding Theory, Akademgorodok, Novosibirsk, Russia. 2010. P. 329 – 334.