Федеральное государственное бюджетное учереждение науки
ИНСТИТУТ ПРОБЛЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ
им А. А. Харкевича Российской академии наук

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

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
д. т. н.
Зяблов В.В.

Москва – 2012

Содержание

Введение

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 диссертацион-

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

ной 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 исследованы 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.

[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.

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:

- получены асимптотические оценки 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 [11, 13, 16], 10 статей в сборниках трудов конференций [3, 10, 12, 20, 61, 62, 70–73] и тезисах 2 докладов [14, 15].

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 [10–13, 20, 62, 70–72] получены автором самостоятельно. В работах [3, 14–16, 61, 73] 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.

Обзор литературы

В 1960 г. Р. Г. Галлагер предложил Г-МПП-коды, описанные в работе [42], в которой приведена оценка кодового расстояния и предложены практически реализуемые эффективные алгоритмы декодирования (мажоритарный алгоритм и алгоритм распространения доверия). В 1974 г. и 1975 г. В. В. Зяблов и М. С. Пинскер в работах [8, 9] исследовали реализуемые корректирующие свойства предложенных кодов для симметричного стирающего канала (ССК) и двочино-симметричного канала (ДСК). В 1981 г. Р. Таннер предложил [67] обобщеную конструкцию МПП-кода. К сожалению, в силу слабого развития вычислительной техники, интерес к Г-МПП-кодам угас на некоторое время.

Но с появлением работ М. Сипсера, Д. Спилмана [63, 65], Д. Маккея [51] и Г. Земора [69] активное исследование Г-МПП-кодов возобновилось. В настоящий момент Г-МПП-кодам посвящено большое количество работ. Рассматривались корректирующие свойства различных алгоритмов декодирования как для исправления ошибок [5, 6, 18, 24, 27, 30, 33, 34, 36, 53, 56, 68], так и для исправления стираний [37, 43, 44, 55]. Исследовались кодовое расстояние и спектр Г-МПП-кодов [23, 28, 35, 38, 47, 57, 58, 64]. Предлагались эффективные алгоритмы кодирования Г-МПП-кодов[31, 41, 49, 60]. Исследовались различные конструкции Г-МПП-кодов [4, 19, 22, 26, 29, 39, 40, 48, 50, 59].

Начиная с работ К. Ш. Зигангирова, М. Лентмайера [45, 46] и Дж. Бутроса, О. Пофиера, Г. Земора [32] всё больший интерес вызывают обобщенные МПП-коды. Из класса обобщенных МПП-кодов детально были исследованы Х-МПП-коды. В работе [66] показано, что нижняя оценка кодового расстояния Х-МПП-кода достигает границу Варшамова-Гилберта. В дальнейшем исследовались реализуемые корректирующие свойства Х-МПП-кодов [7, 25]. В настоящее время актиано исследуются различные конструкции обобщенных МПП-кодов [52, 54].

Глава 1

Исправление стираний двоичным МПП-кодом

1.1. Введение

В первой главе для симметричного стирающего канала (ССК) исследуются реализуемые корректирующие свойства двоичного МПП-кода. Рассматривается алгоритм декодирования для исправления стираний. Получена нижняя оценка доли гарантированно исправимых стираний двоичным МПП-кодом при декодировании по алгоритму для исправления стираний со сложностью $\mathcal{O}(n \log n)$. Эффективность рассматриваемого алгоритма декодирования показана с помощью иммитационным моделированием.

1.2. Структура 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:

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

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 столбцов 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 $\mathscr{E}(n_0, \ell, b_0)$.

З а м е ч а н и е 1.1. Необходимо отметить, что $\mathscr{E}(n_0, \ell, b_0)$ определяет не ансамбль всех обобщенных МПП-кодов, а ансамбль обобщенных МПП-кодов с заданным компонентным кодом. В данной работе мы будем рассматривать только код с проверкой на четность и код Хэмминга в качестве компонентных кодов. 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.

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 $\mathscr{E}_H(n_0, \ell, b_0)$.

Нижняя оценка, полученная в [67], на скорость R кода из $\mathscr{E}(n_0, \ell, b_0)$ определяется следующим неравенством:

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

где R_0 – скорость кода-компонента. Равенство достигается только в случае,

когда $\mathbf{H}$ имеет полный ранг.

Как следует из построения, обобщенный МПП-код из $\mathscr{E}(n_0, \ell, b_0)$ имеет $n = b_0 n_0$ кодовых символов, которые распределены между ℓb_0 компонентных кодов (b_0 в каждом слое) с проверочной матрицей $\mathbf{H}_0$. Такие коды могут быть представлены с помощью двудольного графа Таннера [67] $G = (V_1 : V_2, E)$ с $n = b_0 n_0$ вершинами-символами V_1 и ℓb_0 вершинами-кодами V_2, как на рис. 1.1. Каждая вершина-код включает m_0 проверочных уравнений, соот-

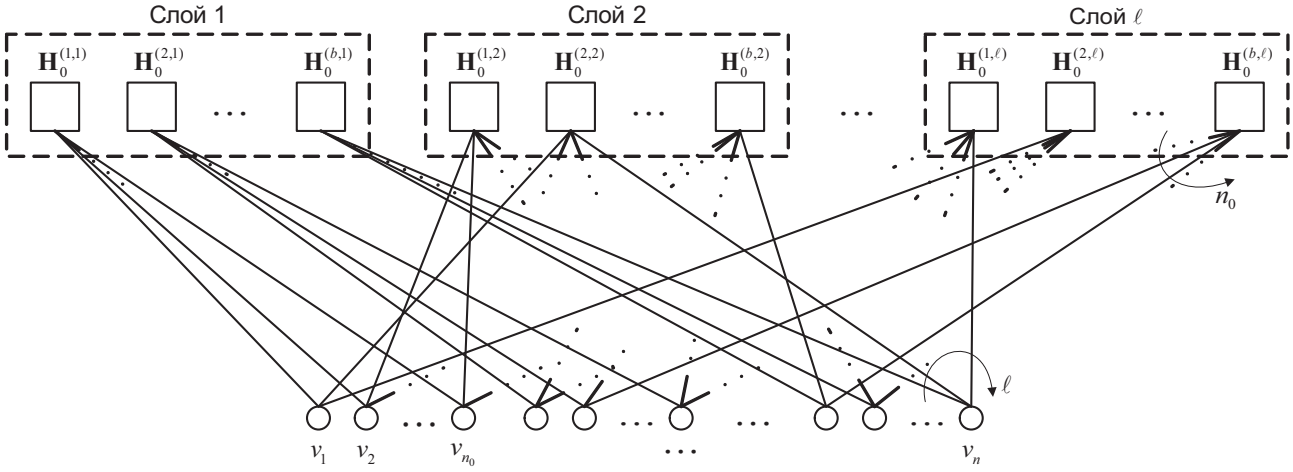

Рис. 1.1. Двудольный граф Таннера соответствующий проверочной матрице $\mathbf{H}$ обобщенного МПП-кода

ветствующих проверочной матрице $\mathbf{H}_0$. Если символ входит в проверку кода-компонента, то в графе Таннера существует ребро из E, соединяющее соответствующую вершину-символ из V_1 с соответствующей вершиной-кодом из V_2. В соответствии с конструкцией проверочной матрицы обобщенного МПП-кода каждый кодовый символ входит в проверки точно одного кода-компонента в каждом слое. Таким образом, соответствующий граф Таннера регулярен со степенью вершины-символа равной ℓ и степенью вершины-кода равной n_0.

1.3. Асимптотическая оценка доли гарантированно исправимых стираний

Впервые для симметричного стирающего канала (ССК) корректирующие свойства Г-МПП-кода исследовались в работе [8], где было доказано, что существует Г-МПП-код с длиной n, гарантированно исправляющий линейно растующее с длиной число стираний при декодировании со сложностью $\mathcal{O}(n \log n)$. Затем в работе [4] для определенного класса Г-МПП-кодов с проверочными матрицами, составленными из перестановочных матриц, был получен результат аналогичный [8]. При этом численно показано, что оценка [4] в некоторых случах превосходит результаты оценки [8]. Заметим, что в работе [4] рассматривался определенный подкласс Г-МПП-кодов, в то время, как в работе [8] рассматривался весь ансамбль Г-МПП-кодов.

В данном параграфе рассматриваются ансамбли Г-МПП-кодов и Х-МПП-кодов. Получена новая оценка доли гарантированно исправимых стрианий. При этом для Х-МПП-кода данная оценка получена впервые. 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 гарантрованно 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.

1.3.1. Алгоритм декодирования

Описание алгоритма декодирования

Идея алгоритма декодирования заключается в поиске исправимых комбинаций стираний, вошедших в компонентные коды МПП-кода, и в после-

дующем их исправлении. Результатом работы алгоритма является либо исправленная последовательность без стираний, либо неисправленная последовательность, содержащая стирания, и флаг, информирующий об успешном или об отказе от декодиования соответственно.

Рассмотрим итеративный алгоритм $\mathscr{A}_\tau$ декодирования МПП-кода, i-ая итерация, $i = 1, 2, \ldots, i_{\max}$, которого состоит из следующих шагов:

(1) Вычисляем количество стираний и составляем список комбинаций стираний, вошедших в компонентные коды, для декодируемой последовательности $\mathbf{r}^{(i)}$, где $\mathbf{r}^{(1)}$ – это принята последовательность $\mathbf{r}$.

(2) Последовательно рассматриваем все коды-компоненты, в которые вошли комбинации стираний кратности не более τ, где τ - некоторая фиксированная константа:

   – если комбинация стираний исправима, то исправляем данную комбинацию и переходим к следующему шагу;

   – если комбинация стираний неисправима, то переходим к следующему компонентному коду;

   – если все комопнентные коды рассмотренны, то переходи к следующему шагу;

(3) Рассматриваем обновленную последовательность $\mathbf{r}^{(i)}$, полученную на предыдущем шаге:

   – если последовательность не содержит стираний, то алгоритм возвращает исправленную последовательность $\mathbf{r}^{(i)}$, устанавливает флаг успешного декодирования и прекращает выполнение;

– в противном случае если количество стираний в декодируемой последовательности 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 декодирования возвращает обновленную последовательность $\mathbf{r}^{(i)}$, устанавливает флаг отказа от декодирования и завершает выполнение.

Пусть при декодировании по алгоритму $\mathscr{A}_\tau$ найдется хотя бы один код-компонент с исправимой комбинацией стираний. Тогда данная комбинация стираний будет исправлена на первой итерации алгоритма $\mathscr{A}_\tau$, а неисправимые комбинации стираний будут проигнорированы, т. е. новые стирания не будут введены. Таким образом, количество стираний в декодируемой последовательности уменьшится. Ясно, что количество стираний в декодируемой последовательности $\mathbf{r}^{(i)}$ будет уменьшаться с каждой итерацией и алгоритм $\mathscr{A}_\tau$ восстановит переданное кодовое слово $\mathbf{v}$ за конечное количество шагов, если на каждой итерации найдется хотя бы один компонентый код с исправимой комбинацией стираний.

Условие существования исправимой комбинации стираний

Введем понятие обобщенного синдрома $\mathbf{S}_\tau$:

$$\mathbf{S}_\tau = (\mathbf{S}_1\,\mathbf{S}_2\,\ldots\,\mathbf{S}_\ell) = (\underbrace{S_{1,1}\,S_{1,2}\,\ldots\,S_{1,b}}_{\text{слой}\,1}\underbrace{S_{2,1}\,S_{2,2}\,\ldots\,S_{2,b}}_{\text{слой}\,2}\ldots\underbrace{S_{\ell,1}\,S_{\ell,2}\,\ldots\,S_{\ell,b}}_{\text{слой}\,\ell}),$$

где $S_{i,j}=1$, если комбинация стираний кратности менее τ, входящая в j-ый код i-ого слоя, исправима и $S_{i,j}=0$ - если неисправима.

Тогда вес обобщенного слоя $|\mathbf{S}_\tau|$ равен числу кодов-компонентов с исправимой комбинацией стираний. Поскольку каждое стирание входит ровно в ℓ

компонентных кодов, то в общем случае условие существования исправимой комбинации стираний можно записать следующим образом:

$$|\mathbf{S}_\tau| \geq \alpha W \ell, \tag{1.1}$$

где α $(0 \leq \alpha \leq 1)$ – доля кодов-компонентов с исправимой комбинацией стираний (свободный положительный параметр).

1.3.2. Формулировка основного результата

Для формулировки основного результата необходимо ввести следующие обозначения:

- $g_0(s, n_0)$ – производящая функция количества $G_0^{(i)}$ неисправимых комбинаций стираний кратности i для заданного кода с длиной n_0:

$$g_0(s, n_0) = \sum_i G_0^{(i)} s^i.$$

- $g_1(s, n_0)$ – производящая функция количества $G_1^{(i)}$ исправимых комбинаций стираний кратности i ошибок для заданным кодом с длиной n_0:

$$g_1(s, n_0) = \sum_i G_1^{(i)} s^i.$$

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

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

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:*

$$h(\omega) - \ell F(\alpha, \omega, n_0) = 0, \tag{1.2}$$

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

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

$$+ \max\{\omega \log_2 s - \frac{1}{n_0} \log_2(g_0(s, n_0)) - \alpha\omega \log_2 \left(\frac{g_1(s, n_0)}{g_0(s, n_0)}\right)\}, \qquad (1.3)$$

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

$$\frac{\alpha\omega n_0}{1 - \alpha\omega n_0} \leq \frac{g_1(s, n_0)}{g_0(s, n_0)}, \qquad (1.4)$$

Тогда в ансамбле $\mathscr{E}(n_0, \ell, b_0)$ *существует код (с вероятностью* p *такой, что* $\lim\limits_{n\to\infty} p = 1$*), который может исправить любую комбинацию стираний кратности до* $\lfloor \omega_\tau n \rfloor$ *при декодировании по алгоритму* $\mathscr{A}_\tau$ *со сложностью порядка* $\mathcal{O}(n \log n)$*.*

1.3.3. Доказательство основного результата

Доказательство состоит из двух частей. В первой части доказано, что в ансамбле $\mathscr{E}(n_0, \ell, b_0)$ существует МПП-код (с вероятностью p такой, что $\lim\limits_{n\to\infty} p = 1$), для которого условие (1.1) выполняется для всех комбинаций стираний кратности $W < \lfloor \omega_\tau n \rfloor$.

Затем во второй части показано, что если на каждом шаге алгоритма $\mathscr{A}_\tau$ выполняется условие (1.1), то алгоритм исправит все стирания со сложностью $\mathcal{O}(n \log n)$.

Существование МПП-кода с заданными свойствами

Л е м м а 1.1. *Для фиксированной комбинации из* W *стираний вероятность* $P_W(|\mathbf{S}_\tau| \leq \alpha W \ell)$ *того, что условие (1.1) не выполняется, ограничена сверху:*

$$P_W\left(|\mathbf{S}_\tau| < \alpha W\ell\right) 2^{-n\ell F(\alpha,\omega,n_0)}$$

Д о к а з а т е л ь с т в о. Рассмотрим компоненту $\mathbf{S}_l$ обобщенного синдрома $\mathbf{S}_\tau$, соответствующую l-ому слою матрицы $\mathbf{H}$. Введем следующую производящую функцию вероятностей для l-ого слоя при кратности стираний W:

$$Q_W^l(t) = \sum_{j=0}^{b} P_W(|\mathbf{S}_l| = j)t^j, \tag{1.5}$$

где $P_W(|\mathbf{S}_l| = j)$ - вероятность того, что для заданной кратности стираний W количество кодов-компонентов в l-ом слое с исправимой комбинацией стираний в точности равно j.

Определенная выше вероятность равна:

$$P_W(|\mathbf{S}_l| = j) = \frac{N_j(W, n_0, b)\begin{pmatrix} b \\ j \end{pmatrix}}{\begin{pmatrix} n \\ W \end{pmatrix}}, \tag{1.6}$$

где $N_j(W, n_0, b)$ - количество комбинаций стираний кратности W, при которых вес обобщенного синдрома $\mathbf{S}_l$ l-ого слоя матрицы $\mathbf{H}$ равен j, т.е. $|\mathbf{S}_l| = j$.

Введем далее следующую порождающую функцию для $N_j(W, n_0, b)$:

$$E_j = \sum_{i=0}^{n} N_j(i, n_0, b)s^i. \tag{1.7}$$

Очевидно, что

$$E_j = \sum_{i=0}^{W} N_j(i, n_0, b)s^i + \sum_{i=W+1}^{n} N_j(i, n_0, b)s^i \geq N_j(W, n_0, b)s^W,$$

откуда следует

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

Полученная верхняя граница на $N_j(W, n_0, b)$ выполняется для всех s. Наиболее близкая граница определяется путем минимизации по s:

$$N_j(W, n_0, b) \leq \min_{s>0} \left\{ \frac{E_j(s)}{s^W} \right\}. \tag{1.8}$$

Каждый символ в каждом слое проверяется ровно одним компонентным кодом. Другими словами каждый из b кодов-компонентов одного слоя проверяет непересекающийся с другими набор, состоящий из n_0 символов (n_0-набор). Если в данном n_0-наборе содержится исправимая комбинация стираний, то соответствующий компонент $S_{l,i}$ обобщенного синдрома $\mathbf{S}_l$ равен единице. Иначе, компонент обобщенного синдрома равен нулю. Таким образом, мы можем записать:

$$E_j(s) = (g_1(s, n_0))^j (g_0(s, n_0))^{b-j}, \tag{1.9}$$

где $g_0(s, n_0)$ - производящая функция всех n_0-наборов, для которых соответствующий компонент $S_{l,i}$ обобщенного синдрома $\mathbf{S}_l$ равен нулю, а $g_1(s, n_0)$ - производящая функция n_0-наборов, для которых $S_{l,i} = 1$.

Следовательно, подставляя (1.9) в (1.8), получаем

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

которое будучи подставленным в (1.6), дает

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

Затем, подставив полученное неравенство в (1.5), находим:

$$Q_W^l(t) \le \sum_{j=0}^{b} \left(\frac{\binom{b}{j}}{\binom{n}{W}} \min_{s>0} \left\{ \frac{(g_1(s,n_0))^i (g_0(s,n_0))^{b-i}}{s^W} \right\} t^j \right) \le$$

$$\le \binom{n}{W}^{-1} \min_{s>0} \left\{ s^{-W} \sum_{j=0}^{b} \binom{b}{j} t^j (g_1(s,n_0))^j (g_0(s,n_0))^{b-j} \right\} = \qquad (1.10)$$

$$= \binom{n}{W}^{-1} \min_{s>0} \left\{ s^{-W} (g_0(s,n_0) + t g_1(s,n_0))^b \right\}.$$

Поскольку слои независимы, вес обобщенного синдрома $|\mathbf{S}_\tau|$ равен сумме ℓ независимых случайных величин $|\mathbf{S}_l|$, $l = 1, 2, \ldots, \ell$. Тогда производящая функция вероятностей веса обобщенного синдрома

$$Q_W(t) = \sum_{j=0}^{b\ell} P_W(|\mathbf{S}_\tau| = j) t^j \qquad (1.11)$$

равна произведению ℓ производящих функций $Q_W^l(t)$ (см. (1.5)), $l = 1, 2, \ldots, \ell$:

$$Q_W(t) = \prod_{l=1}^{\ell} Q_W^l(t) = (Q_W^1(t))^\ell. \qquad (1.12)$$

Из (1.10) и (1.12) мы получаем:

$$Q_W(t) \le \begin{pmatrix} n \\ W \end{pmatrix}^{-\ell} \min_{s>0} \left\{ s^{-W\ell} \left(g_0(s, n_0) + t g_1(s, n_0) \right)^{b\ell} \right\}. \tag{1.13}$$

Тогда вероятность того, что вес обобщенного синдрома будет не более $\alpha W \ell$ можно записать как

$$P(|\mathbf{S}_\tau| \le \alpha W \ell) = \sum_{j=0}^{\alpha W \ell} P_W(|\mathbf{S}| = j).$$

Из (1.11) мы можем вывести следующее неравенство, которое выполняется для всех $0 < t \le 1$:

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

$$\ge t^{\alpha W \ell} \sum_{j=0}^{\alpha W \ell} P_W(|\mathbf{S}_\tau| = j).$$

Первое неравенство выполняется для всех $t > 0$, когда дополнительное условие $t \le 1$ необходимо для последнего неравенства, т.к. $t^{j - \alpha W \ell} \ge 1$ для $j \le \alpha W \ell$. Откуда следует верхняя граница

$$P(|\mathbf{S}_\tau| \le \alpha W \ell) = \sum_{j=0}^{\alpha W \ell} P_W(|\mathbf{S}_\tau| = j) \le \frac{Q_W(t)}{t^{\alpha W \ell}},$$

которая после подстановки (1.13) и минимизации по t, дает

$$P(|\mathbf{S}_\tau| \le \alpha W \ell) \le \begin{pmatrix} n \\ W \end{pmatrix}^{-\ell} \min_{0<t\le 1} \min_{s>0} \left\{ (t^\alpha s)^{-W\ell} \left(g_0(s, n_0) + t g_1(s, n_0) \right)^{b\ell} \right\}.$$

Полученное неравенство может быть переписано как

$$P(|\mathbf{S}_\tau| \le \alpha W \ell) \le \begin{pmatrix} n \\ W \end{pmatrix}^{-\ell} \min_{0<t\le 1} \min_{s>0} \left\{ s^{-W\ell} \left(g_0(s,n_0)\right)^{b\ell} \left(f(t,s)\right)^{b\ell} \right\}, \quad (1.14)$$

где зависимость от t локализована в

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

Приравнивая $\frac{\partial f(t,s)}{\partial t} = 0$, находим значение t_0, на котором достигается минимум $f(t,s)$:

$$t_0 = \frac{\alpha\omega n_0}{1-\alpha\omega n_0} \left(\frac{g_1(s,n_0)}{g_0(s,n_0)} \right)^{-1}, \quad (1.15)$$

где s такое, что $t_0 \le 1$.

Тогда

$$f(t_0,s) = \frac{1}{1-\alpha\omega n_0} \left(\frac{\alpha\omega n_0}{1-\alpha\omega n_0} \right)^{-\alpha\omega n_0} \left(\frac{g_1(s,n_0)}{g_0(s,n_0)} \right)^{\alpha\omega n_0} =$$
$$= 2^{h(\alpha\omega n_0)} \left(\frac{g_1(s,n_0)}{g_0(s,n_0)} \right)^{\alpha\omega n_0}, \quad (1.16)$$

где $h(\cdot)$ - двоичная функция энтропии, которая может быть записана как $h(p) = \log_2 \frac{p^{-p}}{(1-p)^{1-p}}$.

Подставляя (1.16) в (1.14) получаем

$$P(|\mathbf{S}_\tau| \le \alpha W \ell) \le$$
$$\le \begin{pmatrix} n \\ \omega n \end{pmatrix}^{-\ell} 2^{\frac{h(\alpha\omega n_0)\ell n}{n_0}} \times \min_{s>0} \left\{ s^{-\omega n \ell} \left(g_0(s,n_0)\right)^{\frac{\ell n}{n_0}} \left(\frac{g_1(s,n_0)}{g_0\left(s,n_0\right)} \right)^{\alpha\omega n\ell} \right\}. \quad (1.17)$$

Используя неравенство

$$\begin{pmatrix} n \\ \omega n \end{pmatrix} \le 2^{nh(\omega)}, \quad (1.18)$$

где асимптотическое равенство достигается при $n \to \infty$, и (1.17) получаем:

$$P(|\mathbf{S}_\tau| \le \alpha W \ell) \le 2^{-\ell n F(\alpha,\omega,n_0)}, \tag{1.19}$$

где $F(\alpha, \omega, n_0)$ – это функция (1.3), у которой минимизация производиться по всем $s > 0$ таким, что t_0, определенная в (1.15), меньше единицы. ▲

Теперь рассмотрим вероятность того, что вес обобщенного синдрома не более $\alpha W \ell$ для любой комбинации стираний заданной кратности W. Если эта вероятность менее единицы, тогда существуют коды из ансамбля $\mathscr{E}(n_0, \ell, b_0)$, для которых условие (1.1) выполняется для любой комбинации стираний кратности W. Таким образом, существование таких кодов гарантируется, если

$$\begin{pmatrix} n \\ W \end{pmatrix} P(|\mathbf{S}_\tau| \le \alpha W \ell) < 1.$$

Логарифмируя и используя неравенства (1.18) и (1.19), получим

$$h(\omega) - \ell F(\alpha, \omega, n_0) < 0. \tag{1.20}$$

Наибольшее значение ω, удовлетворяющее (1.20), обозначим как ω_τ.

З а м е ч а н и е 1.2. Заметим, что условие (1.20) не гарантирует нам существование такого кода, что при всех W вплоть до максимального условие (1.1) выполняется. Строго говоря, возможно, что для различных значений W существуют различные коды, для которых $|\mathbf{S}_\tau| \le \alpha W \ell$. Условие (1.20) используется только для поиска максимального значения W.

Доказателство того, что в ансамбле $\mathscr{E}(n_0, \ell, b_0)$ существует код, для которого условие (1.1) выполнятся для всех W вплоть до максимального аналогично доказательству теоремы 2.2, приведенной в § 2.2.3.

Сложность алгоритма декодирования

В предыдущем параграфе мы доказали, что в ансамбле $\mathscr{E}(n_0, \ell, b_0)$ существует МПП-код, для которого условие (1.1) выполняется для любой последовательности кратности $W \leqslant \lfloor \omega_\tau n \rfloor$. Другими словами, в ансамбле $\mathscr{E}(n_0, \ell, b_0)$ существует МПП-код, при декодировании которого по алгоритму $\mathscr{A}_\tau$ для любой последовательности кратности $W \leqslant \lfloor \omega_\tau n \rfloor$ найдется исправимая комбинация стираний, т. е. $\alpha > 0$. В таком случае алгоритм $\mathscr{A}_\tau$ исправит все стирания за конечное число итераций.

Оценим количество необходимых итераций алгоритма $\mathscr{A}_\tau$ для исправления комбинации стираний кратности W при условии, что $\alpha > 0$. Запишем оценку на долю ε исправимых стираний от общего числа стираний W:

$$\alpha \leq \varepsilon \leq \alpha \ell \tau.$$

Первое неравенство следует из того, что в худшем случае каждое из исправимых стираний исправляется ровно ℓ кодами-компонентами. А второе неравенство получается в случае, если каждый код-компонент исправляет τ стираний, не входящих в другие коды-компоненты с исправимыми комбинациями.

Получив связь доли кодов-компонентов α с долей исправимых стираний ε, можно утверждать следующее:

Л е м м а 1.2. *Для любого МПП-кода, если комбинация стираний такая, что на каждой итерации декодирования алгоритма $\mathscr{A}_\tau$ существует линейная доля кодов-компонентов с исправимой комбинацией стираний (т. е. $\alpha > 0$), то алгоритм $\mathscr{A}_\tau$ восстанавливает переданное кодовое слово за $\mathcal{O}(\log n)$ итераций, где n - длина кода.*

Д о к а з а т е л ь с т в о. Обозначим ε нижнюю границу доли исправимых стираний в каждой итерации, $0 < \varepsilon < 1$. Тогда, после x итераций,

количество оставшихся стираний не превосходит $W(1-\varepsilon)^x$. Последняя итерация декодирования $i_{\max}$ достигается при выполнении условия:

$$W(1-\varepsilon)^{i_{\max}} < 1.$$

Следовательно,

$$\log W + i_{\max} \log(1-\varepsilon) < 0.$$

Откуда,

$$i_{\max} < \frac{1}{\log(\frac{1}{1-\varepsilon})} \log W.$$

Обозначим $W = \omega n$, где ω - относительная доля стираний в принятой последовательности длины n. Тогда:

$$i_{\max} < \frac{1}{\log(\frac{1}{1-\varepsilon})} \log(\omega n).$$

Таким образом, количество итераций декодирования составляет порядка логарифма от длины кода. ▲

Л е м м а 1.3. *Сложность одной итерации декодирования составляет* $\mathcal{O}(n)$

Д о к а з а т е л ь с т в о. Алгоритм проходит по не более чем n символам. На исправление комбинации стирний требуется $\mathcal{O}(1)$ операций. ▲

Следовательно, согласно лемме 1.2 и лемме 1.3 суммарная сложность декодирования будет составлять $\mathcal{O}(n \log n)$.

1.3.4. Численные значения оценки доли стираний, гарантированно исправимых Г-МПП-кодом

Выбор производящих функций

Известно, что кодовое расстояние кода с проверкой на четность $d_0 = 2$. Следовательно, при передаче данного кода по стирающему каналу гарантируется исправление любой комбинации стираний кратности до $d_0 - 1 = 1$. Переданное значение на месте стирания определяется простым суммированием принятых без стирания символов кода-компонента.

Следовательно, введенные выше производящие функции исправимых комбинаций стираний $g_1(s, n_0)$ и неисправимых комбинаций стираний $g_0(s, n_0)$ будут иметь следующий вид:

$$g_1(s, n_0) = \begin{pmatrix} n_0 \\ 1 \end{pmatrix} s$$

и

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

соответственно.

Анализ численных результатов

При рассмотрении Г-МПП-кодов с заданной скорость R удобно задавать количество слоев ℓ и вычислять необходимую длину компонентного кода n_0:

$$n_0 = \left\lceil \frac{\ell}{1 - R} \right\rceil .$$

Поэтому численные результаты были получены для заданных диапазонов скоростей кода R и количества слоев ℓ и вычисленных значений длин кода-компонента n_0.

Сформулированная в § 1.3.2 теорема 1.1 позволяет оценить долю стираний, гарантированно исправимых Г-МПП-кодом из ансамбля $\mathscr{E}_G(n_0, \ell, b_0)$ при итеративном декодировании $\mathscr{A}_{\tau=1}$. В соответствии с алгоритмом декодирования обозначим данную долю стираний как $\omega_{\tau=1}$. В соотвествии с работой [8] долю стираний, оцененную по оценке из [8], обозначим как ω_0.

На рис. 1.2 и в табл. 1.1 представлены численные результаты доли $\omega_{\tau=1}$ и ω_0 гарантированно исправимых ошибок при декодировании по алгоритму $\mathscr{A}_{\tau=1}$ от количества слоев (длины кода-компонента) для двоичного Г-МПП-кода с фиксированной скоростью $R \approx 0,5$. Из результатов следует, что значения, полученные по предложенной оценке, превосходят значения, полученные по оценке [8], при любых значениях параметров Г-МПП-кода с фиксированной скоростью $R \approx 0,5$. Также можно заметить, что при увеличении количества слоев ℓ разница между $\omega_{\tau=1}$ и ω_0 уменьшается, при этом наибольшее улучшение оценки [8] было получено при малом количестве слоев.

Как видно из рис. 1.2 для заданной скорости R существует оптимальное значение количества слоев ℓ (длины кода-компонента n_0), при котором достигается максимальное значение $\omega_{\tau=1}$ и ω_0. Рассмотрим теперь зависимость найденных наибольших значений долей гарантированно исправимых стираний $\omega_{\tau=1}$ и ω_0 от скорости R Г-МПП-кода (см. рис. 1.3 и табл. 1.2). Как видно

Таблица 1.1

Численные результаты зависимости $\omega_{\tau=1}$ и ω_0 от количества слоев (длины кода-компонента) при фиксированной скорости $R \approx 0,5$ Г-МПП-кода

Доли	$\ell(n_0)$					
	3 (6)	5 (10)	7 (14)	9 (18)	11 (22)	13 (26)
$\omega_{\tau=1}$, 10^{-2}	1,70	5,70	6,40	6,30	5,90	5,60
ω_0, 10^{-2}	1,04	4,97	5,99	6,06	5,84	5,56
$\omega_{\tau=1}/\omega_0$	1,21	1,15	1,07	1,04	1,01	1,01

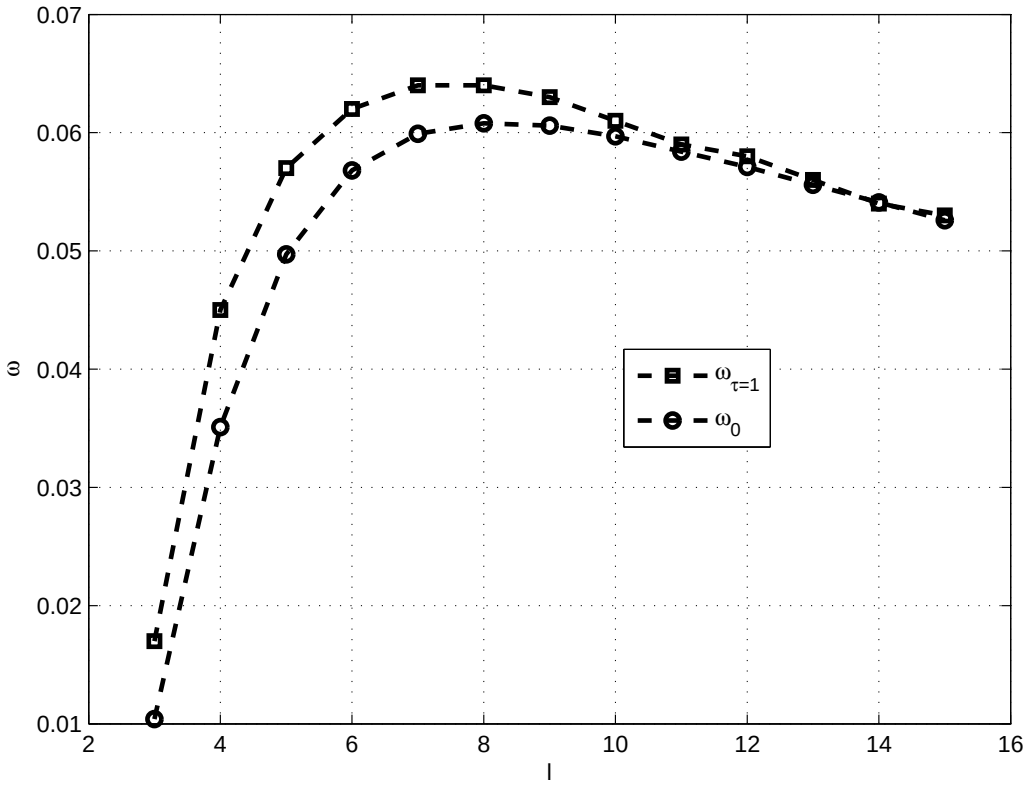

Рис. 1.2. Графики зависимости доли $\omega_{\tau=1}$ и ω_0 исправимых стираний от количества слоев ℓ при фиксированной скорости $R \approx 0,5$ Г-МПП-кода

предложенная оценка заметно улучшает оценку [8] при малых скоростях, а при увеличении скорости R Г-МПП-кода оценки совпадают.

Таблица 1.2

Численные результаты зависимости наибольших значений $\omega_{\tau=1}$ и ω_0 от скорости R Г-МПП-кода

Доли	R				
	0,1	0,3	0,5	0,7	0,9
$\omega_{\tau=1},\ 10^{-2}$	18,50	11,20	6,40	3,12	0,78
$\omega_0,\ 10^{-2}$	14,84	10,29	6,08	3,12	0,78
$\omega_{\tau=1}/\omega_0$	1,25	1,09	1,05	1	1

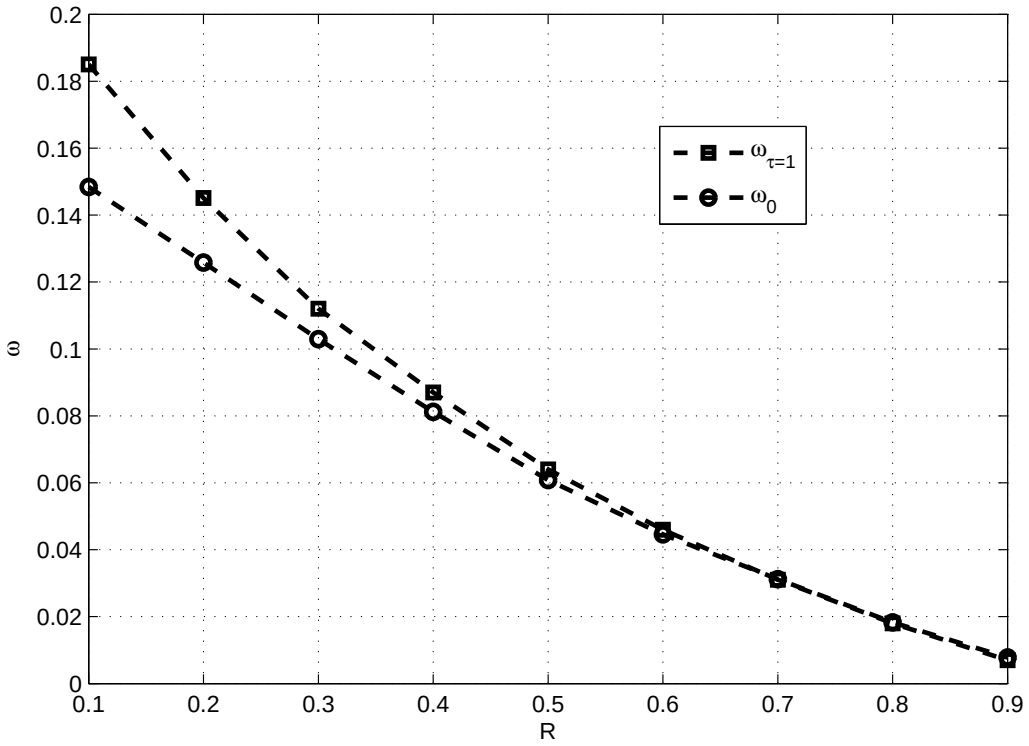

Рис. 1.3. Зависимость наибольших значений долей $\omega_{\tau=1}$ и ω_0 гарантированно исправимых стираний от скорости R Г-МПП-кода

1.3.5. Численные значения оценки доли стираний, гарантированно исправимых Х-МПП-кодом

Выбор производящих функций

Известно, что для любого натурального $m_0 \geq 2$, существует код Хэмминга с длиной $n_0 = 2^{m_0} - 1$, размерностью $k_0 = n_0 - m_0$, кодовым расстоянием $d_0 = 3$ и скоростью $R_0 = 1 - \frac{m_0}{n_0}$. Проверочная матрица $\mathbf{H}_0$ кода Хэмминга (n_0, k_0, d_0) размера $m_0 \times n_0$ состоит из столбцов всех ненулевых двоичных векторов размерности m_0.

Следовательно, для кода Хэмминга гарантируется исправление любой комбинации стираний кратности не более $d_0 - 1 = 2$. Алгоритм декодирования Х-МПП-кода, исправляющий любые комбинации кратности не более 2, обозначим $\mathscr{A}_{\tau=2}$.

Тогда производящие функии исправимых комбинаций стираний $g_1(s, n_0)$

и неисправимых комбинаций стираний $g_0(s, n_0)$ при алгоритме декодирования $\mathscr{A}_{\tau=2}$ будут иметь следующий вид:

$$g_1(s, n_0) = \begin{pmatrix} n_0 \\ 1 \end{pmatrix} s + \begin{pmatrix} n_0 \\ 2 \end{pmatrix} s^2$$

и

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

соответственно.

Тем не менее, возможно исправление кодом Хэмминга некоторых комбинаций стираний кратности до m_0. Алгоритм декодирования, исправляющий любые комбинации стираний кратности не более 2 и некоторые комбинации стираний кратности более 2 и менее m_0, обозначим $\mathscr{A}_{\tau=m_0}$.

Рассмотрим более подробно способ определения переданного значения на месте стирания в коде Хэмминга при итеративном декодировании $\mathscr{A}_{\tau=m_0}$. Для каждого i-ого, $i = 1, 2, \ldots, b$, кода-компонента из j-ого слоя, $j = 1, 2, \ldots, \ell$, выбранного на первом шаге алгоритма $\mathscr{A}_{\tau=m_0}$, строим матрицу $\mathbf{M}_{i,j}$ размера $m_0 \times \tau_{i,j}$, где $\tau_{i,j} \leqslant m_0$ – количество стираний в выбранном коде, состоящую из столбцов проверочной матрицы $\mathbf{H}_0$ кода Хэмминга, соответствующих позициям стирания. Следует отметить, что в общем случае $\mathrm{rank}(\mathbf{M}_{i,j}) \leqslant \tau_{i,j} \leqslant m_0$. Также для каждого выбранного кода-компонента вычисляем синдромы $\mathbf{s}_{i,j}$, полагая на позициях стираний нули. Обозначим теперь через $\mathbf{x}_{i,j}$ вектор размерности $\tau_{i,j}$ неизвестных (стертых) переданных символов. Эти символы могут быть восстановлены в результате решения системы линейных уравнений:

$$\mathbf{x}_{i,j}\mathbf{M}_{i,j}^T = \mathbf{s}_{i,j}.$$

Очевидно, что система уравнений имеет единственное решение тогда и только тогда, когда матрица $\mathbf{M}_{i,j}$ имеет полный ранг, то есть $\mathrm{rank}(\mathbf{M}_{i,j}) = \tau_{i,j}$.

В этом случае комбинация стираний называется исправимой.

Но, как упоминалось выше, только часть комбинаций стираний кратности более $d_0 - 1$ являются исправимыми. Следующая лемма позволяет определить число исправимых комбинаций:

Л е м м а 1.4. *Пусть* $\mathbf{M}$ *размера* $m_0 \times \tau$ *состоит из* τ *столбцов проверочной матрицы* $\mathbf{H}_0$ *кода Хэмминга длины* n_0 *, где* $1 \leqslant \tau \leqslant m_0$ *и* $m_0 = \log_2(n_0 + 1)$. *Тогда количество матриц* $\mathbf{M}$ *с полным рангом,* $rank(\mathbf{M}) = \tau$, *равно:*

$$M(\tau, m_0) = \frac{1}{\tau!} \prod_{i=0}^{\tau-1} \left(2^{m_0} - 2^i\right).$$

Д о к а з а т е л ь с т в о. Столбцы проверочной матрицы $\mathbf{H}_0$ кода Хэмминга длины $n_0 = 2^{m_0} - 1$ состоят из всех ненулевых двоичных векторов размерности m_0. Пусть $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_\tau\}$ - набор из τ линейно независимых столбцов матрицы $\mathbf{H}_0$. Тогда количество таких наборов определяется следующим образом:

- В качестве $\mathbf{b}_1$ выбираем любой из $2^{m_0} - 1$ ненулевых двоичных векторов размерности m_0;
- В качестве $\mathbf{b}_2$ выбираем отличный от $\mathbf{b}_1$ вектор, т.е. $\mathbf{b}_2 \neq c_1\mathbf{b}_1$, где $c_1 \in \{0, 1\}$. Это можно сделать $2^{m_0} - 2$ способами;
- В качестве $\mathbf{b}_i$, $i = 3, 4, \ldots, \tau$, выбираем такие ненулевые вектора, которые не являются линейной комбинацией предыдущих выбранных $i - 1$ векторов, т.е. $\mathbf{b}_i \neq c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + \ldots + c_{i-1}\mathbf{b}_{i-1}$, где $c_1, c_2, \ldots, c_{i-1} \in \{0, 1\}$. Ясно, что всего выборов $\mathbf{b}_i$, $i = 3, 4, \ldots, \tau$, $2^{m_0} - 2^{i-1}$.

Заметим, что порядок следования векторов $\mathbf{b}_i$ в наборе $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_\tau\}$ несущественен. Тогда, общее количество таких наборов:

$$M(\tau, m_0) = \frac{\prod_{i=0}^{\tau-1} \left(2^{m_0} - 2^i\right)}{\tau!}.$$

Что завершает доказательство. ▲

Обратим внимание ещё раз на то, что комбинация стираний исправима тогда и только тогда, когда матрица $\mathbf{M}$, составленная из τ столбцов $\mathbf{H}_0$, соответствующих позициям стираний, имеет ранг равный τ, $\mathrm{rank}(\mathbf{M}) = \tau$. Тогда, мы имеем следующее:

С л е д с т в и е. *Количество комбинаций стираний кратности* $\tau \leqslant m_0$, *исправимых кодом Хэмминга с длиной* $n_0 = 2^{m_0} - 1$, *определяется по формуле* $M(\tau, m_0)$.

Следовательно, производящие функции исправимых комбинаций стираний $\tilde{g}_1(s, n_0)$ и неисправимых комбинаций стираний $\tilde{g}_0(s, n_0)$ при алгоритме декодирования $\mathscr{A}_{\tau=m_0}$ имеют следующий вид:

$$\tilde{g}_1(s, n_0) = \sum_{\tau=1}^{m_0} M(\tau, m_0) s^\tau = \sum_{\tau=1}^{m_0} \frac{\prod_{i=0}^{\tau-1} \left(2^{m_0} - 2^i\right)}{\tau!} s^\tau$$

и

$$\tilde{g}_0(s, n_0) = (1+s)^{n_0} - \tilde{g}_1(s, n_0)$$

соответственно.

Следует отметить, что функцию $\tilde{g}_1(s, n_0)$ можно переписать следующим образом:

$$\tilde{g}_1(s, n_0) = \sum_{\tau=1}^{m_0} \frac{\prod_{i=0}^{\tau-1} \left(2^{m_0} - 2^i\right)}{\tau!} s^\tau = g_1(s, n_0) + \sum_{\tau=3}^{m_0} \frac{\prod_{i=0}^{\tau-1} \left(2^{m_0} - 2^i\right)}{\tau!} s^\tau,$$

где $g_1(s, n_0)$ - введенная выше производящая функция исправимых комбинаций стираний при алгоритме декодирования $\mathscr{A}_{\tau=2}$.

Анализ численных результатов

Поскольку в отличие от кода с проверкой на четность код Хэммига существует только для определенного набора длин, то при рассмотрении Х-МПП-кодов с заданной скорость R удобно задавать длину кода-компонента n_0 и вычислять количество слоев ℓ:

$$\ell = \left\lfloor \frac{n_0}{\log_2(n_0+1)}(1-R) \right\rfloor .$$

Поэтому численные результаты были получены для заданных диапазонов скоростей кода R и длин компонентных кодов n_0 и вычисленных значений ℓ.

В § 1.3.2 была доказана теорема 1.1, позволяющая оценить долю гарантированно исправимых стираний $\omega_{\tau=2}$ и $\omega_{\tau=m_0}$ при декодировании Х-МПП-кода из ансамбля $\mathscr{E}_H(n_0, \ell, b_0)$ по алгоритмам $\mathscr{A}_{\tau=2}$ и $\mathscr{A}_{\tau=m_0}$ соответственно.

На рис. 1.4 и в табл. 1.3 представлены численные результаты доли $\omega_{\tau=2}$ и $\omega_{\tau=m_0}$ гарантированно исправимых стираний при декодировании по алгоритмам $\mathscr{A}_{\tau=2}$ и $\mathscr{A}_{\tau=m_0}$ от длины кода-компонента (количества слоев) при фиксированном значении скорости $R \approx 0,5$ Х-МПП-кода. Из результатов следует, что доля гарантированно исправимых стираний $\omega_{\tau=m_0}$ значительно превосходит $\omega_{\tau=2}$ для всех параметров Х-МПП-кода при фиксированной скорости $R \approx 0,5$. Также стоит отметить, что с увеличение длины код-компонента разница между $\omega_{\tau=m_0}$ и $\omega_{\tau=2}$ медленно уменьшается, при этом наибольшее улучшение было получено при малой длине кода-компонента.

Как видно из рис. 1.4 для заданной скорости R существует оптимальное значение длины кода-компонента n_0 (количества слоев ℓ), при которой достигается максимальное значение $\omega_{\tau=2}$ и $\omega_{\tau=m_0}$. Рассмотрим теперь зависимость найденных наибольших значений долей гарантированно исправимых стираний $\omega_{\tau=2}$ и $\omega_{\tau=m_0}$ от скорости R Х-МПП-кода (см. рис. 1.5 и табл. 1.4). Как видно наибольшие значения $\omega_{\tau=m_0}$ значительно превосходят наибольшие значения $\omega_{\tau=2}$ для всех рассмотренных скоростей Х-МПП-кода. При этом

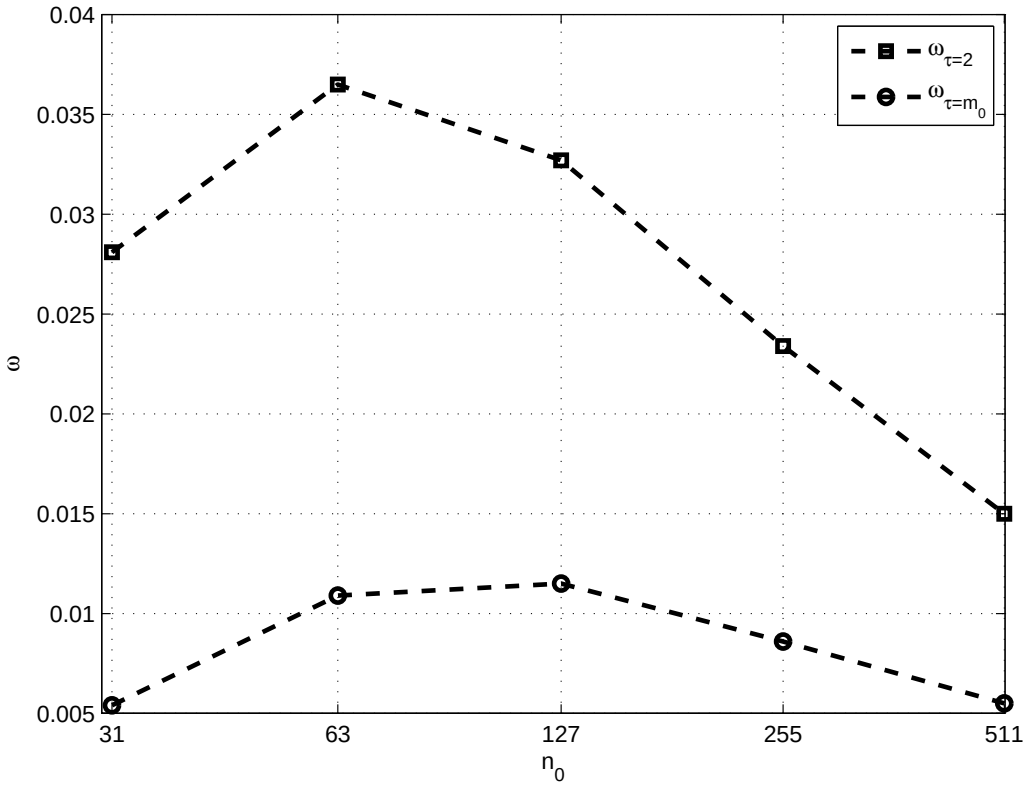

Рис. 1.4. График зависимости доли стираний $\omega_{\tau=2}$ и $\omega_{\tau=m_0}$, исправимой алгоритмами $\mathscr{A}_{\tau=2}$ и $\mathscr{A}_{\tau=m_0}$, от длины n_0 кода-компонента при фиксированном значении скорости $R \approx 0,5$ Х-МПП-кода

интересно отметить, что наибольший выигрыщ $\omega_{\tau=m_0}$ по сравнению с $\omega_{\tau=2}$ достигается при скорости близкой к $R = 0,5$.

1.3.6. Сравнение численных значений оценки доли стираний, гарантированно исправимых Г-МПП-кодом и Х-МПП-кодом

Сравним полученные значения оценок долей $\omega_{\tau=1}$ и $\omega_{\tau=m_0}$, гарантированно исправимых Г-МПП-кодом и Х-МПП-кодом при декодировании по алгоритмам $\mathscr{A}_{\tau=1}$ и $\mathscr{A}_{\tau=m_0}$ соответственно (см. рис. 1.6 и табл. 1.5). Из приведенных результатов видно, что полученная оценка доли $\omega_{\tau=1}$ гарантированно исправимых стираний Г-МПП-кодом при декодировании по алгоритму $\mathscr{A}_{\tau=1}$ превосходит оценку доли $\mathscr{A}_{\tau=m_0}$ гарантированно исправимых стираний Х-МПП-кодом при декодировании по алгоритму $\mathscr{A}_{\tau=m_0}$.

Таблица 1.3

Численные результаты зависимости $\omega_{\tau=2}$ и $\omega_{\tau=m_0}$ от длины кода-компонента (количества слоев) при фиксированной скорости $R \approx 0,5$ Х-МПП-кода

Доли	$n_0(\ell)$				
	31 (3)	63 (5)	127 (9)	255 (16)	511 (28)
$\omega_{\tau=m_0}$, 10^{-2}	2,81	3,65	3,27	2,34	1,50
$\omega_{\tau=2}$, 10^{-2}	0,54	1,09	1,15	0,86	0,55
$\omega_{\tau=m_0}/\omega_{\tau=2}$	5,20	3,34	2,84	2,72	2,72

1.4. Имитационное моделирование алгоритма декодирования МПП-кода для исправления стираний

В данном параграфе приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_\tau$, описанного в § 1.3.1. Рассматривались алгоритмы декодирования $\mathscr{A}_{\tau=1}$ и $\mathscr{A}_{\tau=m_0}$ для различных параметров Г-МПП-кода и Х-МПП-кода соотвественно.

В качестве модели канала был выбран симметричный стирающий канал (ССК) с вероятностью перехода в стирание (входной вероятностью стираний) p_τ. Для каждого значения p_τ испытания проводились до тех пор, пока не будет накоплено не менее 20 отказов от декодирования МПП-кода. Имита-

Таблица 1.4

Численные результаты зависимости наибольших значений $\omega_{\tau=2}$ и $\omega_{\tau=m_0}$ от скорости R Х-МПП-кода

Доли	R			
	0,1	0,3	0,5	0,7
$\omega_{\tau=m_0}$, 10^{-2}	9,98	6,54	3,65	1,77
$\omega_{\tau=2}$, 10^{-2}	4,25	2,12	1,15	0,56
$\omega_{\tau=m_0}/\omega_{\tau=2}$	2,35	3,08	3,17	3,16

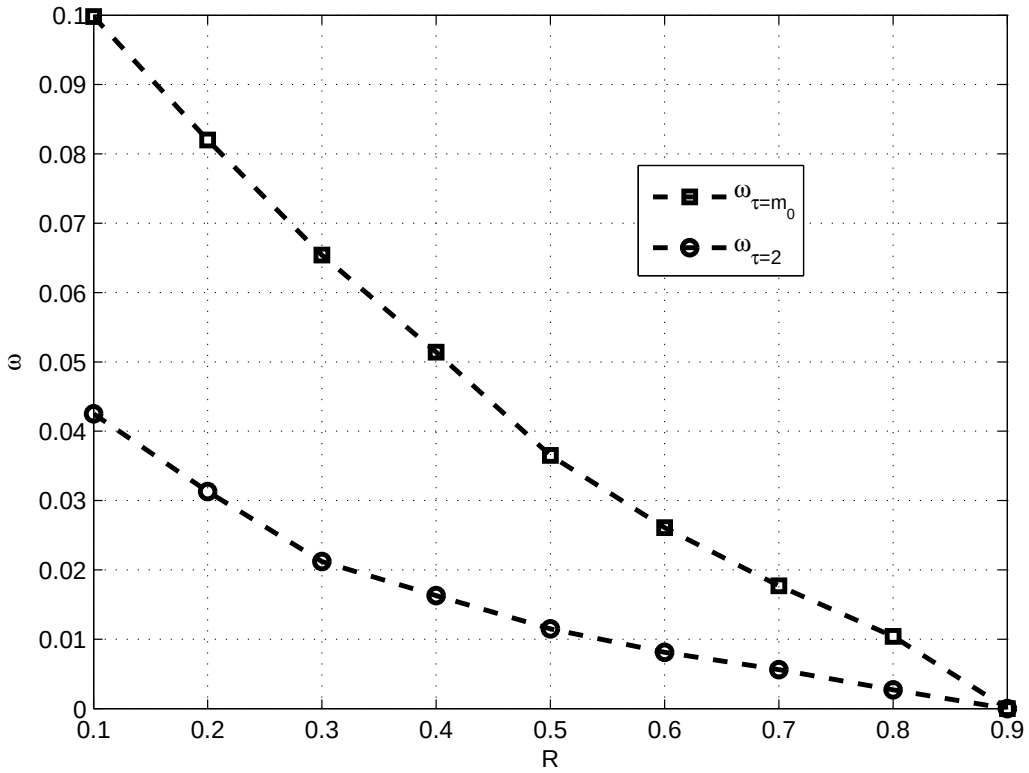

Рис. 1.5. Зависимость наибольших значений долей $\omega_{\tau=2}$ и $\omega_{\tau=m_0}$ гарантированно исправимых стираний от скорости R Х-МПП-кода

ционное моделирование останавливалось, если вероятность отказа от декодирования заданного МПП-кода была меньше 10^{-5}.

1.4.1. Анализ результатов моделирования алгоритма декодирования Г-МПП-кода

Рассмотрим результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_{\tau=1}$ Г-МПП-кода при передаче по ССК с входной вероятностью стирания p_τ. Результаты были получены для заданных значений скоростей кода $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$, количества слоев $\ell = 3, 4, ..., 7$ и соответствующих значений длин кода-компонента n_0.

На рис. 1.7 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_{\tau=1}$ Г-МПП-кода со скоростью $R \approx 0,25$ с различным количеством слоев ℓ при различных значениях входной вероятности p_τ. Как

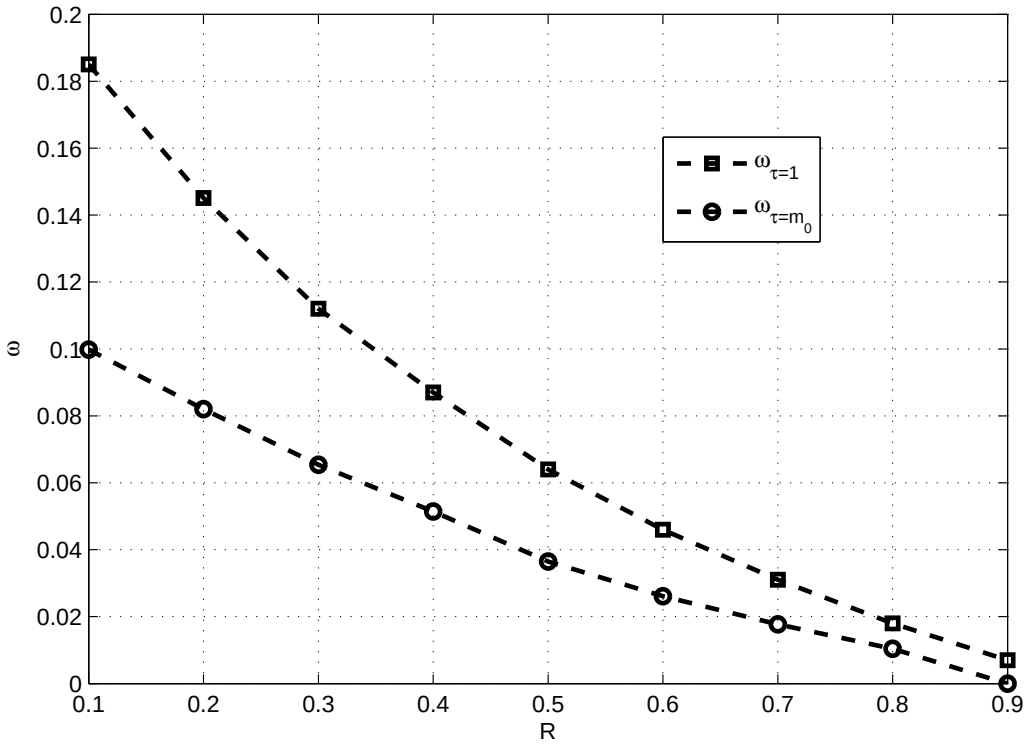

Рис. 1.6. Зависимость наибольших значений долей $\omega_{\tau=1}$ и $\omega_{\tau=m_0}$ гарантированно исправимых стираний от скорости R Г-МПП-кода и Х-МПП-кода

видно, вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_τ для Г-МПП-кода с $\ell = 3$.

На рис. 1.8 представлены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_{\tau=1}$ Г-МПП-кода со скоростью $R \approx 0,5$ с различным количеством слоев ℓ при различных значениях входной вероятности p_τ. Как и ранее, вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_τ для Г-МПП-кода с $\ell = 3$.

На рис. 1.9 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_{\tau=1}$ Г-МПП-кода со скоростью $R \approx 0,75$ с различным количеством слоев ℓ при различных значениях входной вероятности p_τ. Видно, что в этом случае вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_τ для Г-МПП-кода с $\ell = 4$. При этом Г-МПП-код с $\ell = 3$ в данном случае обладает наихудшей корректирующей способностью, что можно объяснить малым кодовым расстоянием

Таблица 1.5

Численные результаты зависимости наибольших значений $\omega_{\tau=1}$ и $\omega_{\tau=m_0}$ от скорости R Г-МПП-кода и Х-МПП-кода

Доли	R				
	0,1	0,3	0,5	0,7	0,9
$\omega_{\tau=1}$, 10^{-2}	18,50	11,20	6,40	3,12	0,78
$\omega_{\tau=m_0}$, 10^{-2}	9,98	6,54	3,65	1,77	–
$\omega_{\tau=1}/\omega_0$	1,85	1,71	1,75	1,76	–

Г-МПП-кода с $\ell = 3$ при $R \approx 0,75$.

Теперь для каждой из рассмотренных скоростей $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$ Г-МПП-кода выбирем те параметры Г-МПП-кода, при которых вероятность отказа от декодирования равная 10^{-5} достигалась при наибольших значения входной вероятности p_τ. На рис. 1.10 представлены графики вероятности отказа от декодирования Г-МПП-кодов с выбранными параметрами в зависимости от входной вероятности стирания p_τ.

1.4.2. Анализ результатов моделирования алгоритма декодирования Х-МПП-кода

Рассмотрим результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_{\tau=m_0}$ Х-МПП-кода при передаче по ССК с входной вероятностью стирания p_τ. Результаты были получены для заданных значений скоростей кода $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$, длин кода-компонента $n_0 = 15, 31, 63, 127, 255, 511$ и соответствующего количества слоев ℓ. Причем для каждой скорости Х-МПП-кода выбиралось наименьшая длина кода-компонента так, чтобы $\ell > 2$.

На рис. 1.11 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_{\tau=m_0}$ Х-МПП-кода со скоростью $R \approx 0,25$ и различной длиной кода-компонента n_0 при различных значениях входной вероятно-

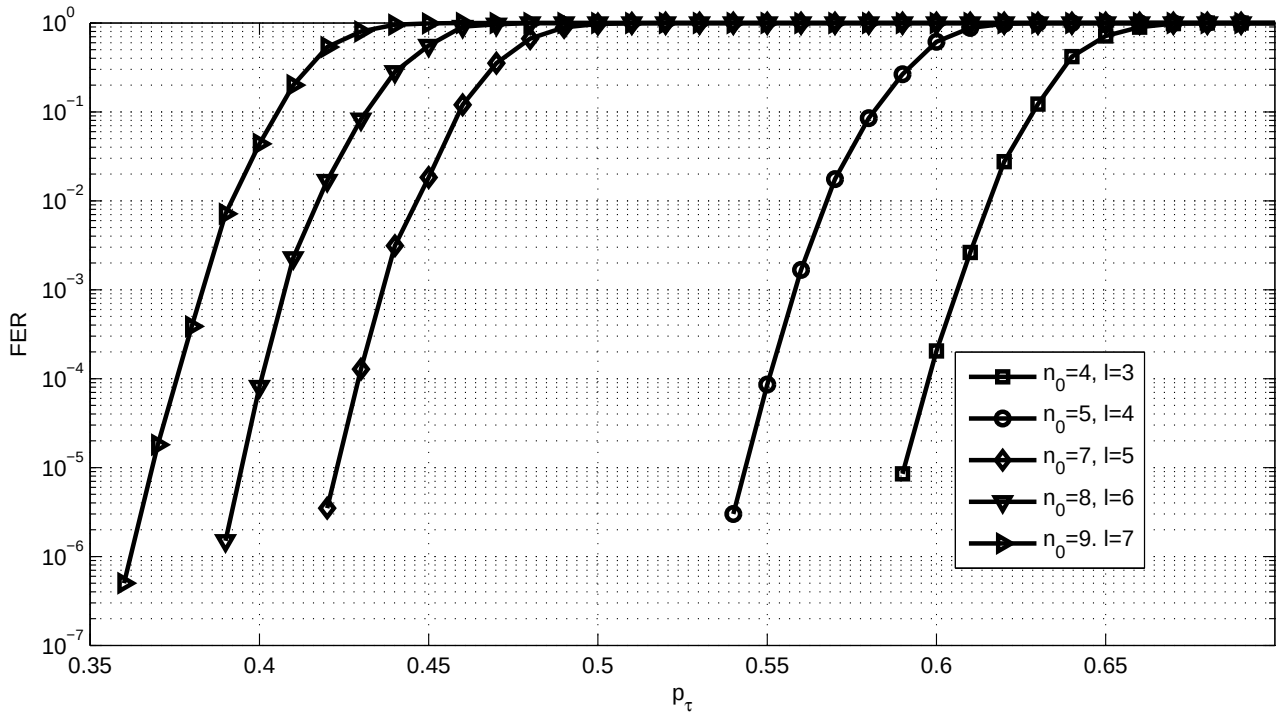

Рис. 1.7. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_{\tau=1}$ в зависимости от входной вероятности стираний p_τ для Г-МПП-кодов со скоростью $R \approx 0,25$ и различным количеством слоев ℓ

сти p_τ. Как видно, вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_τ для Х-МПП-кода с $n_0 = 15$.

На рис. 1.12 представлены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_{\tau=m_0}$ Х-МПП-кода со скоростью $R \approx 0,5$ и различной длиной кода-компонента n_0 при различных значениях входной вероятности p_τ. Вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_τ для Х-МПП-кода с $n_0 = 31$.

На рис. 1.13 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_{\tau=m_0}$ Х-МПП-кода со скоростью $R \approx 0,75$ и различной длиной кода-компонента n_0 при различных значениях входной вероятности p_τ. Видно, что в этом случае вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_τ для Х-МПП-кода с $n_0 = 63$.

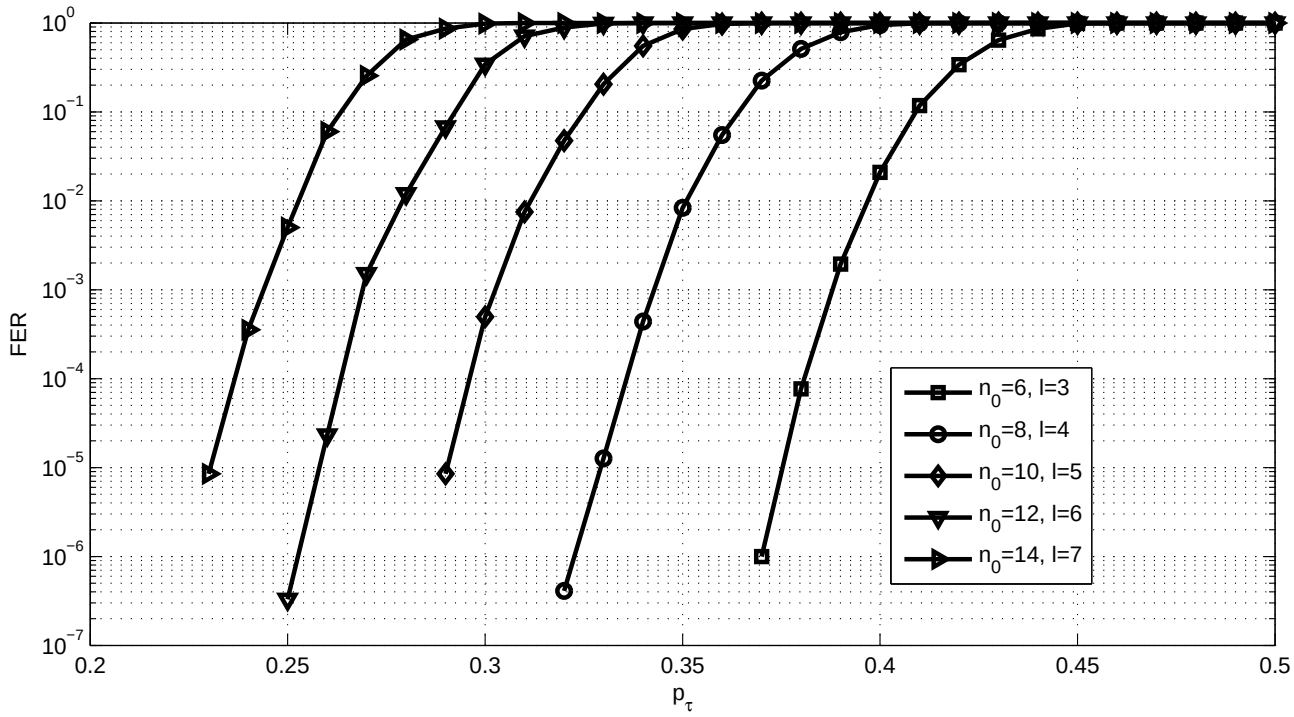

Рис. 1.8. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_{\tau=1}$ в зависимости от входной вероятности стираний p_τ для Г-МПП-кодов со скоростью $R \approx 0,5$ и различным количеством слоев ℓ

Теперь для каждой из рассмотренных скоростей $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$ Х-МПП-кода выбирем те параметры Х-МПП-кода, при которых вероятность отказа от декодирования равная 10^{-5} достигалась при наибольших значения входной вероятности p_τ. На рис. 1.14 представлены графики вероятности отказа от декодирования Х-МПП-кодов с выбранными параметрами в зависимости от входной вероятности стирания p_τ.

1.4.3. Сравнение результатов моделирования алгоритмов декодирования Г-МПП-кода и Х-МПП-кода

Сравним результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_{\tau=1}$ и $\mathscr{A}_{\tau=m_0}$ Г-МПП-кода и Х-МПП-кода соотвественно при передаче по ССК с входной вероятностью стирания p_τ. Для каждой скорости $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$ выбирем такие параметры Г-МПП-кода и Х-МПП-кода, что веро-

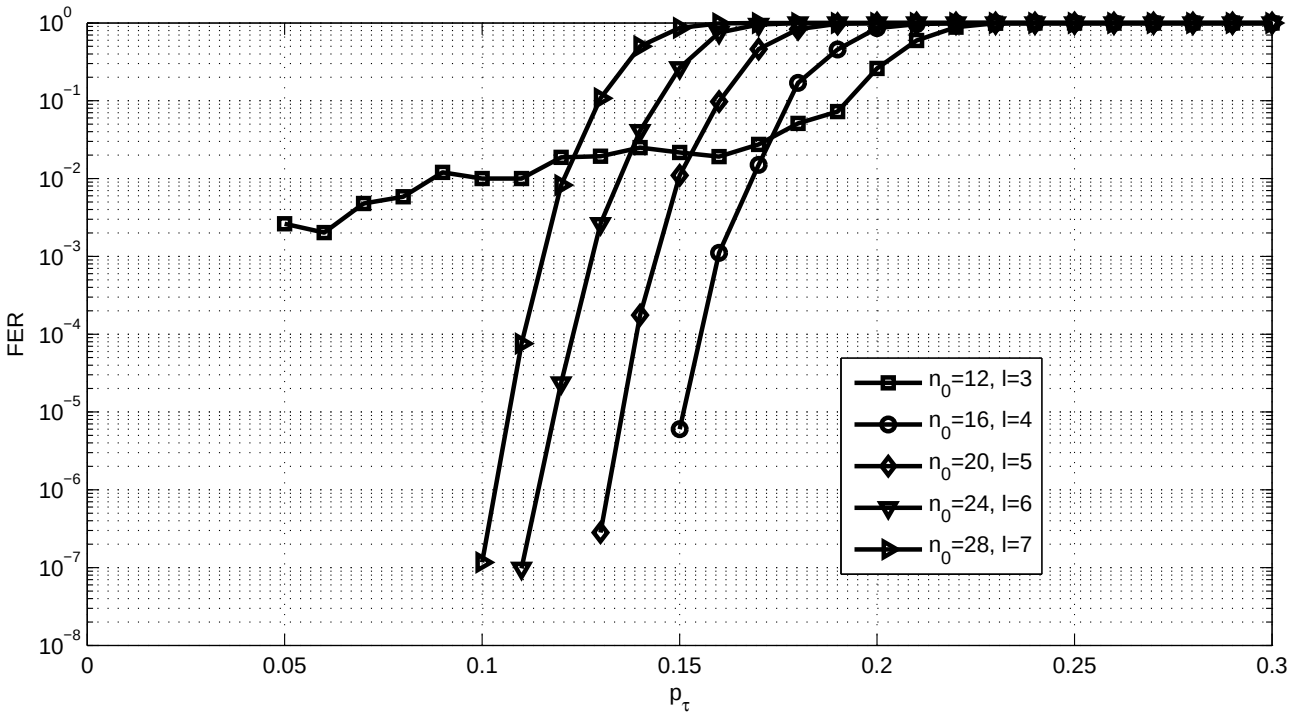

Рис. 1.9. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_{\tau=1}$ в зависимости от входной вероятности стираний p_τ для Г-МПП-кодов со скоростью $R \approx 0,75$ и различным количеством слоев ℓ

ятность отказа от декодирования равная 10^{-5} достигалась при наибольшем значении входной вероятности p_τ. На рис. 1.15 приведены графики вероятности отказа от декодирования Г-МПП-кодов и Х-МПП-кодов с выбранными параметрами в зависимости от входной вероятности стирания p_τ.

Как видно из рис. 1.15 для всех рассматриваемых скоростей вероятность отказа 10^{-5} при декодировании Г-МПП-кода достигается при больших значениях входной вероятности стирания p_τ, чем при декодировании Х-МПП-кода, т.е. в этом смысле Г-МПП-код имеет лучшие корректирующие свойства, чем Х-МПП-код. Так же можно заметить, что при увеличении скорости разница между результатами для Г-МПП-кода и Х-МПП-кода уменьшается. Интересно отметить, что полученная в § 1.3 оценка доли гарантированно исправимых стираний для Г-МПП-кода также превосходит аналогичную оценку для Х-МПП-кода. При увеличении скорости разница между оценками доли га-

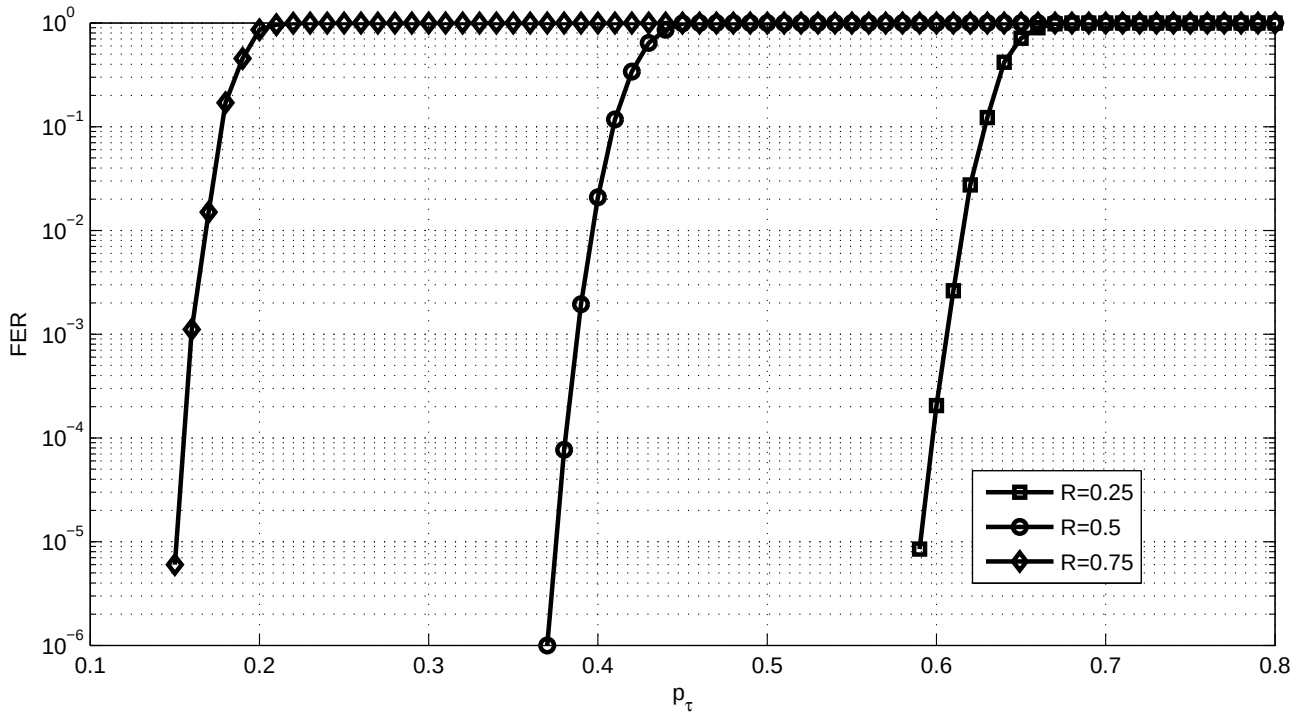

Рис. 1.10. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_{\tau=1}$ в зависимости от входной вероятности стираний p_τ для Г-МПП-кодов с различной скоростью R

рантированно исправимых стираний для Г-МПП-кода и Х-МПП-кода также уменьшается. Но доля гарантированно исправимых стираний определяет такую кратности стираний, при которой вероятность отказа от декодирования равна нулю, а полученные результаты имитационного моделирования имеют некоторую ненулевую вероятность отказа. При этом входные вероятности p_τ, при которых достигается вероятность отказа от декодирования 10^{-5}, значительно превосходят результаты полученной нижней оценки доли ω_τ гарантированно исправимых стираний.

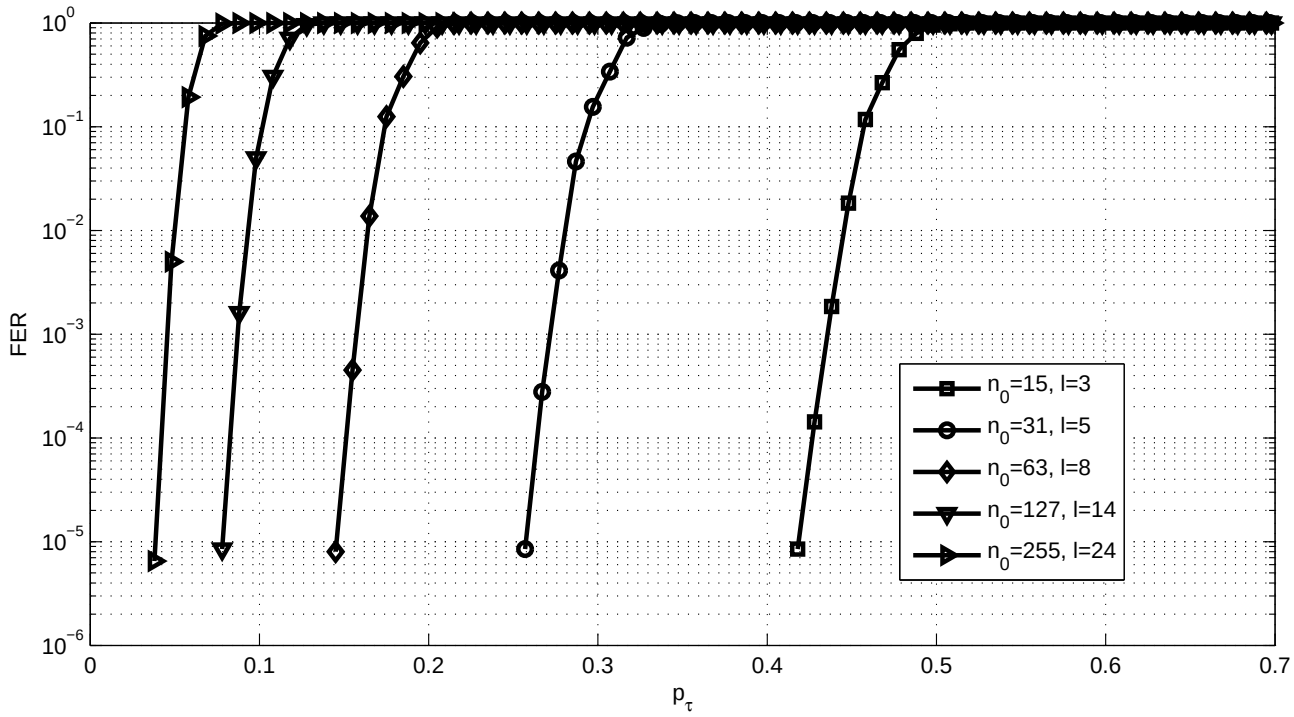

Рис. 1.11. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_{\tau=m_0}$ в зависимости от входной вероятности стираний p_τ для Х-МПП-кодов со скоростью $R \approx 0,25$ и различной длиной кода-компонента n_0

1.5. Выводы к главе

- Получена новая оценка доли гарантированно исправимых стираний при декодировании МПП-кода по алгоритму $\mathscr{A}_\tau$ со сложнсотью $\mathcal{O}(n \log n)$.
- Численно показано, что полученная оценка превосходит лучшую известную оценку доли гарантированно исправимых стираний при декодировании Г-МПП-кода по алгоритму $\mathscr{A}_{\tau=1}$ со сложнсотью $\mathcal{O}(n \log n)$.
- Впервые получена оценка доли гарантированно исправимых стираний при декодировании Х-МПП-кода по алгоритмам $\mathscr{A}_{\tau=2}$ и $\mathscr{A}_{\tau=m_0}$ со сложностью $\mathcal{O}(n \log n)$.
- Численно показано, что оценка доли гарантированно исправимых стираний при декодировании Х-МПП-кода по алгоритму $\mathscr{A}_{\tau=m_0}$ значительно превосходит оценку доли гарантированно исправимых стираний при

декодировани Х-МПП-кода по алгоритму $\mathscr{A}_{\tau=2}$.

- Проведено имитационное моделирование алгоритмов $\mathscr{A}_{\tau=1}$ и $\mathscr{A}_{\tau=m_0}$ декодирования Г-МПП-кода и Х-МПП-кода соответственно. Показано, что алгоритм $\mathscr{A}_{\tau=1}$ декодирования Г-МПП-кода имеет лучшие корректирующие свойства, чем алгоритм $\mathscr{A}_{\tau=m_0}$ Х-МПП-кода.

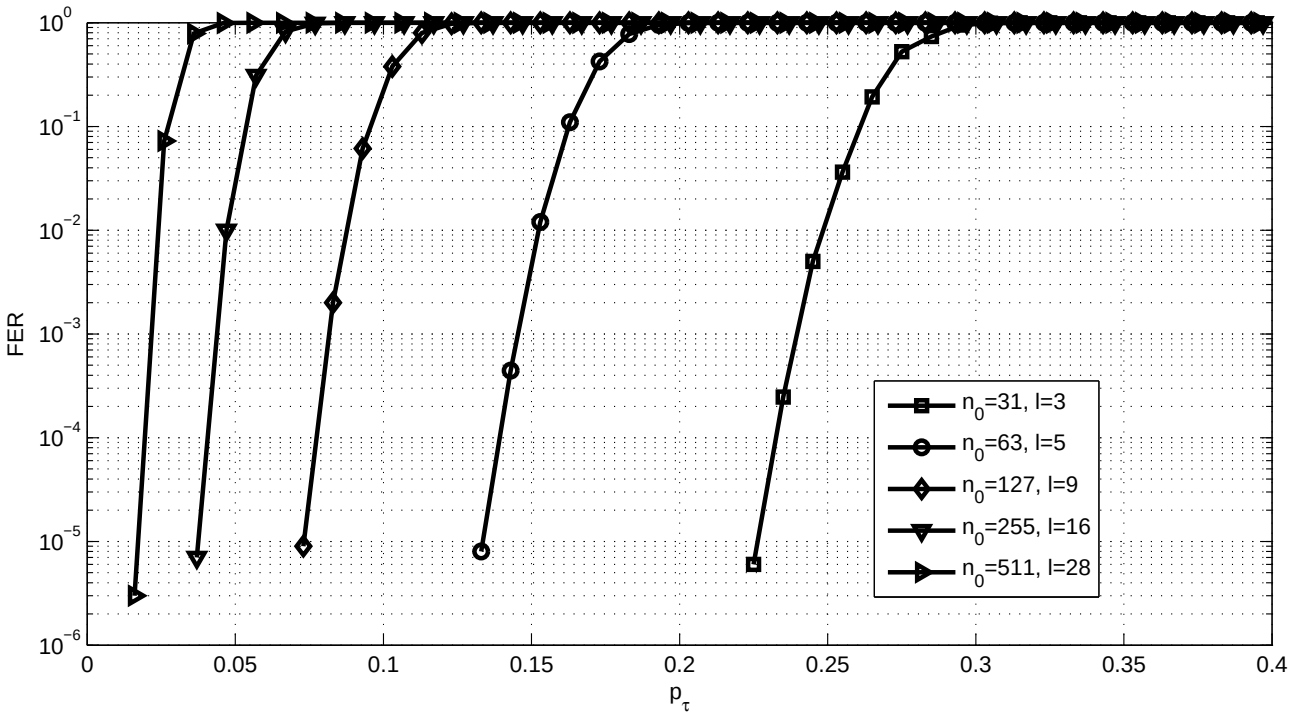

Рис. 1.12. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_{\tau=m_0}$ в зависимости от входной вероятности стираний p_τ для Х-МПП-кодов со скоростью $R \approx 0,5$ и различной длиной кода-компонента n_0

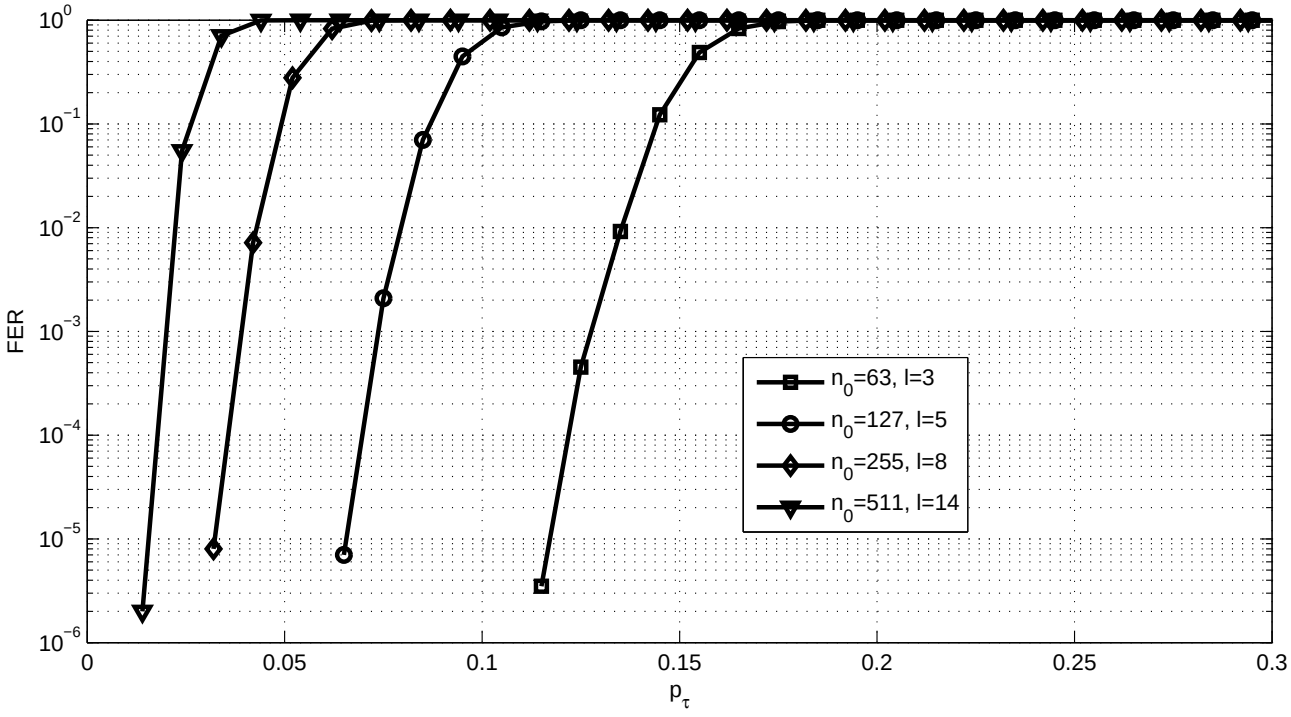

Рис. 1.13. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_{\tau=m_0}$ в зависимости от входной вероятности стираний p_τ для Х-МПП-кодов со скоростью $R \approx 0,75$ и различной длиной кода-компонента n_0

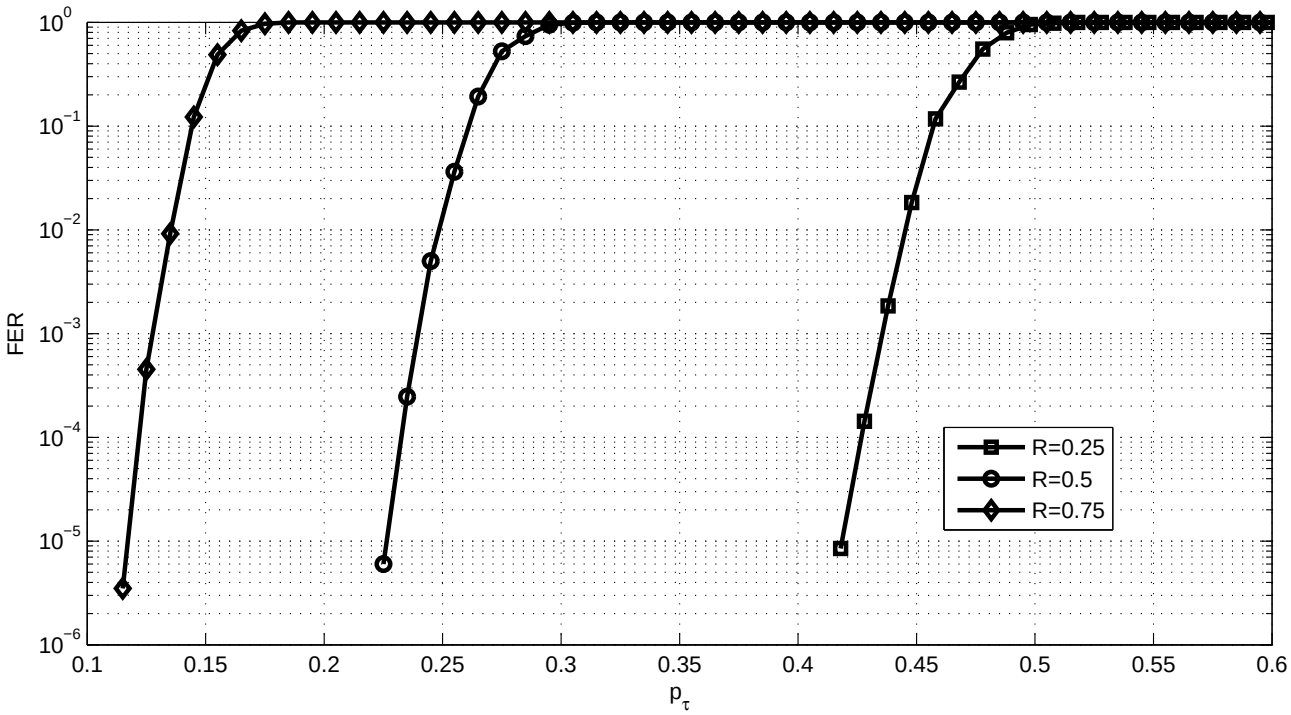

Рис. 1.14. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_{\tau=m_0}$ в зависимости от входной вероятности стираний p_τ для Х-МПП-кодов с различной скоростью R

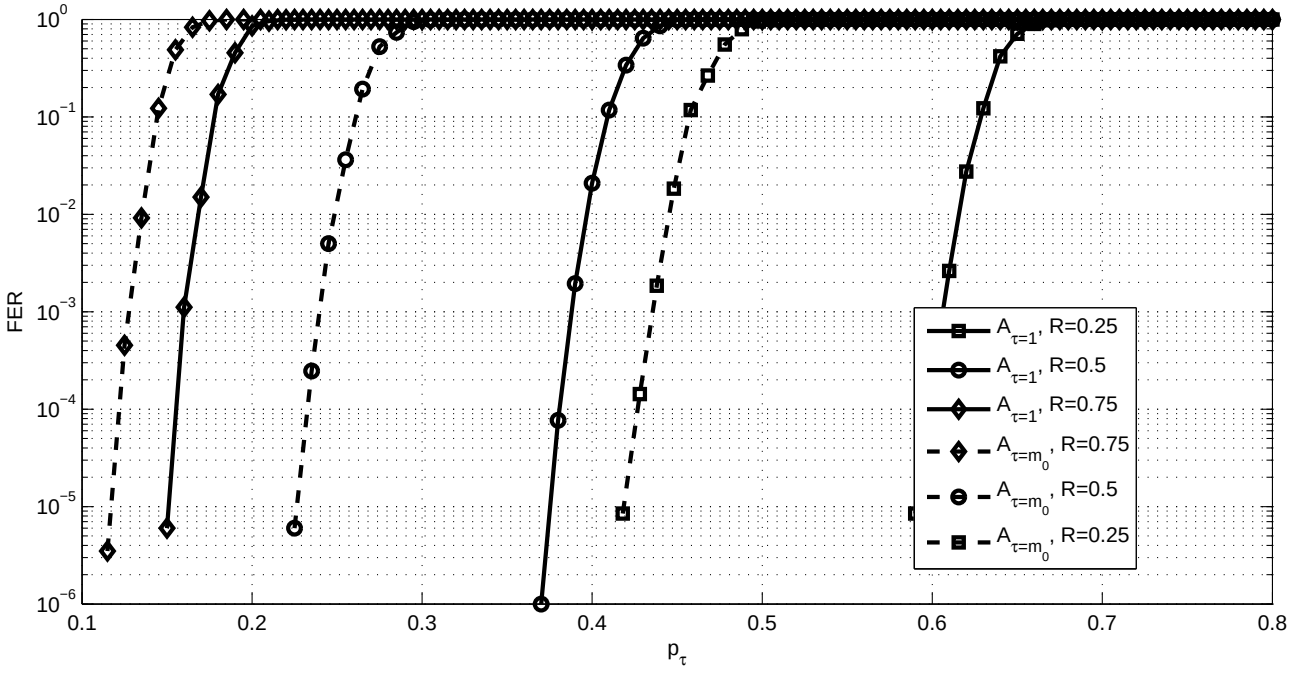

Рис. 1.15. Графики вероятности отказа от декодирования по алгоритмам $\mathscr{A}_{\tau=1}$ и $\mathscr{A}_{\tau=m_0}$ в зависимости от входной вероятности стираний p_τ для Г-МПП-кодов и Х-МПП-кодов с различной скоростью R

Глава 2

Исправление ошибок двоичным МПП-кодом

2.1. Введение

Во второй главе для двоично-симметричного канала (ДСК) исследуются реализуемые корректирующие свойства МПП-кода. Рассматривается мажоритарный алгоритм декодирования. Получена нижняя оценка доли гарантированно исправимых ошибок двоичным МПП-кодом при декодированию по мажоритарному алгоритму со сложностью $\mathcal{O}(n \log n)$. Также предложен новый алгоритм декодирования с относительно простой реализацией. Эффективность рассматриваемых алгоритмов исследовалась с помощью имитационного моделирования.

2.2. Асимптотическая оценка доли гарантированно исправимых ошибок

Корректирующие свойства Г-МПП-кода для двоично-симметричного канала (ДСК) впервые были исследованы в работе [9], где было показано, что существует Г-МПП-код, способный гарантированно исправить линейно растущее с длиной число ошибок при декодировании со сложностью порядка $\mathcal{O}\left(n \log n\right)$, где n – длина Г-МПП-кода. Затем в работе [6] комбинаторными методами была получена более простая для вычисления аналитическая оценка корректирующей способности декодера Г-МПП-кода, но численные результаты оказались в большинстве случаев не лучше результатов, полученных по старой оценке [9]. Следует отметить, что алгоритм декодирования, рассмотренный в работе [6], отличается от алгоритма, описанного в работе [9].

Х-МПП-код был рассмотрен в работе [45]. Затем кодовое расстояние и декодирование по алгоритму распространения доверия было исследовано в работах [46] и [32]. В работе [66] было показано, что ансамбль Х-МПП-кодов содержит коды с минимальным кодовым расстоянием, почти достигающим границу Варшамова-Гилберта. Затем путем обобщения методов, разработанных в [9], в работе [7] впервые были получены результаты для Х-МПП-кодов, аналогичные результату из [9]. Затем в [25] была получена оригинальная оценка для двоичных кодов на графах при передаче по ДСК. Численные значения оценки [25] для Х-МПП-кодов превосходят численные значения ранее известных лучших оценок корректирующей способности Х-МПП-кодов.

В данном параграфе рассматриваются такие же Г-МПП-коды и Х-МПП-коды и соответствующие итеративные алгоритмы декодирования, что и в работах [9] и [25] соответственно. Получена новая нижняя оценка доли гарантированно исправимых ошибок. 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.

2.2.1. Алгоритм декодирования

Описание алгоритма декодирования

Идея алгоритма декодирования заключается в уменьшении количества невыполненных проверок на каждой итерации декодирования, как и в работах [9] и [25]. Результатом работы алгоритма является “исправленная” после-

довательность 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 найден символ, замена которого уменьшит количество невыполненных проверок (т.е. выполняется критерий замены), 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 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 после-

довательностью $\mathbf{r}^{(i+1)}$, которая в точности совпадает с обновленной последовательностью $\mathbf{r}^{(i)}$;

– иначе алгоритм возвращает обноленную последовательность $\mathbf{r}^{(i)}$, устанавливает флаг отказа от декодирования и завершает выполнение.

Критерий замены символа

Предположим, что для данного принятого вектора с W ошибками некоторые коды-компоненты МПП-кода обнаружили эти ошибки, т.е. имеют ненулевой синдром для заданной комбинации. Тогда все n символов кода распределились между ℓb компонентными кодами, проверки которых либо выполнены, либо нет.

Следовательно, для каждого i-ого, $i = 1, .., n$, символа принятой последовательности все ℓ проверок, в которые он входит делятся на следующие множества (см. рис. 2.1):

- **A** - множество кодов-компонентов, обнаруживших ошибки, которые в свою очередь делятся на два подмножества:
  - $\mathbf{A}_{1\to 0}$ - множество кодов-компонентов, проверки которых станут выполненными после замены данного символа;
  - $\mathbf{A}_{1\to 1}$ - множество кодов-компонентов, проверки которых останутся невыполненными после замены данного символа.
- **C** - множество кодов-компонентов с выполненными проверками.

Тогда мы можем ввести следующие обозначения ребер графа Таннера:

- $e^{(i)}_{A_{1\to 0}}$ – число ребер, выходящих из i-ой вершины-символа и входящих в множество $A_{1\to 0}$;

- $e^{(i)}_{A_{1\to 1}}$ – число ребер, выходящих из i-ой вершины-символа и входящих в множество $A_{1\to 1}$;

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

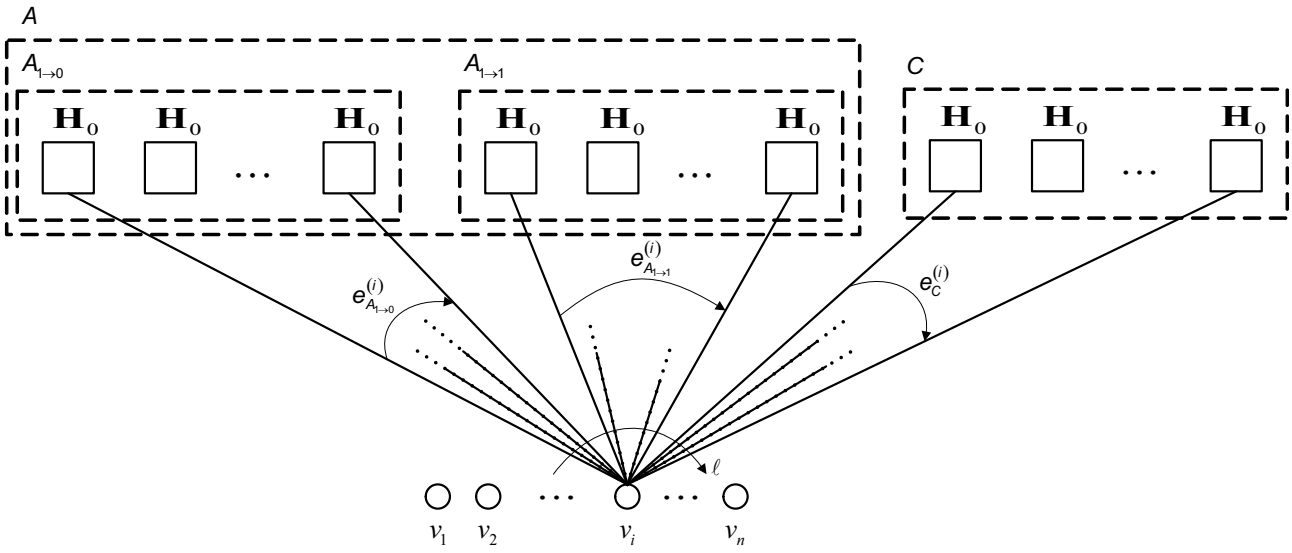

Рис. 2.1. Двудольный граф Таннера с введенными обозначениями ребер и множеств невыполненных и выполненных проверок

З а м е ч а н и е 2.1. Стоит отметить, что число ребер $e^{(i)}_{A_{1\to 0}}$ также равно количеству проверок, которые станут выполненными после замены i-ого символа. Аналогично $e^{(i)}_{A_{1\to 1}}$ – число проверок, которые останутся невыполненными, а $e^{(i)}_{C}$ – число проверок, которые окажутся невыполненными после замены i-ого символа.

Для Г-МПП-кода критерий замены символа очевиден и его можно записать в веденных выше обозначениях следующим образом:

$$e^{(i)}_{A_{1\to 0}} > \frac{\ell}{2}. \tag{2.1}$$

Иными словами требуется, чтобы для рассматриваемого i-ого символа количество невыполненных проверок было больше половины. В этом случае его

замена уменьшит количество невыполненных проверок. Критерий (2.1) рассматривался в работе [9] для Г-МПП-кода и в работе [7] для Х-МПП-кода.

Однако, в то время, как критерий (2.1) для Г-МПП-кода является естественным и оптимальным (в том смысле, что его не представляется возможным смягчить), то для Х-МПП-кода данный критерий - очень жесткий. Поэтому в данной работе мы используем следующий критерий:

$$e^{(i)}_{A_{1\to 0}} > e^{(i)}_{C}, \tag{2.2}$$

т.е. требуем только, чтобы количество проверок, которые станут выполненными, было больше количества проверок, которые станут невыполненными после замены i-ого символа. Очевидно, что при замене i-ого символа количество невыполненных проверок уменьшится.

З а м е ч а н и е 2.2. Понятно, что для компонентного кода с проверкой на четность условие (2.2) аналогично условию (2.1), т.к. при заменен символа проверка, содержащая данный символ, становится либо выполненной, либо невыполненной. Но для кода Хэмминга условия (2.1) и (2.2) различны, т.к. для i-ого символа существует множество проверок, которые останутся невыполненными и после замены i-ого символа.

Условие существования заменяемого символа

Получим следующее условие, при котором гарантируется, что для заданного МПП-кода и заданной комбинации ошибок кратности W гарантированно найдется символ, замена которого уменьшит количество невыполненных проверок:

Л е м м а 2.1. *Для существования по крайней мере одного символа, который будет заменен алгоритмом $\mathscr{A}_M$ в течение одной итерации декодирования заданного МПП-кода, достаточно выполнения условия:*

$$E_{\sum}^{(W)} = 2\sum_{j=1}^{W} e_{A_{1\to 0}}^{(i_j)} + \sum_{j=1}^{W} e_{A_{1\to 1}}^{(i_j)} > W\ell, \tag{2.3}$$

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

Доказательство. Запишем условие замены i-ого символа (2.2) в следующем виде, учитывая то, что в силу конструкции МПП-кода каждый символ входит ровно в ℓ проверок:

$$e_{A_{1\to 0}}^{(i)} > e_C^{(i)} = \ell - e_{A_{1\to 0}}^{(i)} - e_{A_{1\to 1}}^{(i)}.$$

Тогда

$$2e_{A_{1\to 0}}^{(i)} + e_{A_{1\to 1}}^{(i)} > \ell. \tag{2.4}$$

Следуя работе [17], рассмотрим подграф графа Таннера, содержащий вершины, соответствующие ошибочным символам(которых ровно W), и все вершины-коды, соединенные с выбранными вершинами-символами (см. рис. 2.2).

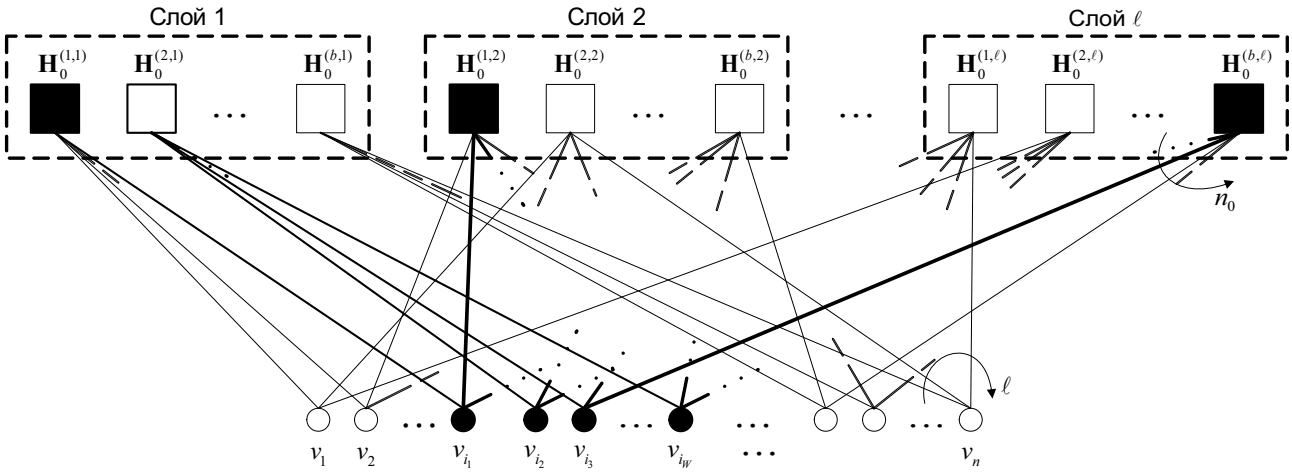

Рис. 2.2. Подграф графа Таннера содержащий вершины-символы, соответствующие ошибочным символам

Заметим, что количество ребер в данном подграфе в точности равно $W\ell$, т.к. каждый символ входит ровно в ℓ проверок, т.е. каждая вершина-символ

соединена ровно с ℓ вершинами-кодами. Поскольку каждая вершина-символ имеет набор из ℓ смежных ребер, непересекающийся с наборами других вершин-символов, то условие (2.4) можно записать в следующем виде:

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

Понятно, что если полученное условие для рассматриваемого подграфа выполняется, то среди W рассматриваемых символов, найдется символ, удовлетворяющий условию (2.2), поскольку в противном случае если

$$2e_{A_{1\to 0}}^{(i)} + e_{A_{1\to 1}}^{(i)} < \ell, \forall i = 1, .., W,$$

то

$$2\sum_{j=1}^{W} e_{A_{1\to 0}}^{(i_j)} + \sum_{j=1}^{W} e_{A_{1\to 1}}^{(i_j)} < W\ell.$$

А значит и среди всех n символов Х-МПП-кода гарантированно найдется символ, удовлетворяющий этому условию, что завершает доказательство. ▲

З а м е ч а н и е 2.3. Заметим, что условие (2.3) гарантирует лишь то, что среди всех n символов найдется символ удовлетворяющий условию (2.2). При это не гарантируется, что символ будет непременно ошибочный. При замене правильного символа алгоритмом $\mathscr{A}_M$ будет внесена ошибка, но при этом количество невыполненных проверок будет уменьшено.

З а м е ч а н и е 2.4. Именно путем оценки вероятности выполнения условия (2.3) получена оценка на долю гарантированно исправимых ошибок, представленную в следующей параграфе.

2.2.2. Формулировка основного результата

Для формулировки основного результата необходимо ввести следующие обозначения:

- $g_0(s, n_0)$ – производящая функция количества $G_0^{(i)}$ кодовых слов веса i заданного кода с длиной n_0:

$$g_0(s, n_0) = \sum_i G_0^{(i)} s^i.$$

- $g_1(s, n_0)$ – производящая функция количества $G_1^{(i)}$ комбинаций i ошибок, обнаруживаемых заданным кодом с длиной n_0:

$$g_1(s, n_0) = \sum_i G_1^{(i)} s^i.$$

- $g_e(s, v, n_0)$ – производящая функция количества таких $G_e^{(i,j)}$ комбинаций j ошибок, что $E_{\sum}^{(W)}$ (см. (2.3)) равна в точности i:

$$g_e(s, v, n_0) = \sum_i \sum_j G_e^{(i,j)} s^j v^i.$$

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

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

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:*

$$h(\omega) - \ell F_e(\omega, n_0) = 0, \tag{2.5}$$

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 уравнения:

$$h(\omega_0) - \ell F_{\mathbf{s}}(\alpha, \omega_0, n_0, \ell) = 0, \tag{2.6}$$

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 $\mathscr{E}(n_0, \ell, b_0)$ *(с вероятностью* p *такой, что* $\lim\limits_{n\to\infty} p = 1$*) 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* $\mathcal{O}(n \log n)$.

2.2.3. Доказательство основного результата

Доказательство состоит из двух частей. В первой части доказано, что в ансамбле $\mathscr{E}(n_0, \ell, b_0)$ существует МПП-код (с вероятностью p, которая $\lim\limits_{n\to\infty} p = 1$), для которого условие (2.3), т.е. $E_{\sum}^{(W)} > W\ell$, выполняется для всех комбинаций ошибок веса $W < \lfloor \omega_0 n \rfloor$.

Во второй части показано, что если вес начальной комбинации ошибок $W < \lfloor \omega_t n \rfloor = \lfloor \alpha_0 \omega_0 n \rfloor$ и на каждом шаге алгоритма $\mathscr{A}_M$ выполняется условие (2.3), $E_{\sum}^{(W)} > W\ell$, то вес декодируемой последовательности не превысит $\lfloor \omega_0 n \rfloor$ и алгоритм исправит все ошибки со сложностью $\mathcal{O}(n \log_2 n)$.

Существование МПП-кода с заданными свойствами

Л е м м а 2.2. *Для фиксированной комбинации из* W *ошибок вероятность того, что условие (2.3) не выполняется, т.е.* $E_{\sum}^{(W)} \leqslant W\ell$*, ограничена сверху величиной* $2^{-n\ell F_e(\omega, n_0) + o(n)}$*:*

$$P_W\left(E_{\sum}^{(W)} \leqslant W\ell\right) \leqslant 2^{-n\ell F_e(\omega, n_0) + o(n)},\ \omega = \frac{W}{n}.$$

З а м е ч а н и е 2.5. При доказательстве леммы 2.2 рассматривается

произвольная фиксированная комбинация ошибок и все МПП-коды из ансамбля $\mathscr{E}(n_0, \ell, b_0)$. Очевидно, что перестановки столбцов слоя проверочной матрицы МПП-кода эквивалентны перестановкам ошибок, что облегчает рассмотрение.

Д о к а з а т е л ь с т в о. Рассмотрим один l-ый слой случайного МПП-кода (иными словами подграф графа Таннера, соответствующего l-ому слою МПП-кода), для которого сумма условия (2.3) равна $E_{\sum}^{(W,l)}$ при заданной фиксированной комбинации W ошибок. Введем следующую производящую функцию:

$$U_W^{(l)}(u) = \sum_{i \geq 0} P_W\left(E_{\sum}^{(W,l)} = i\right) u^i, \tag{2.7}$$

где $P_W\left(E_{\sum}^{(W,l)} = i\right)$ – вероятность того, что сумма $E_{\sum}^{(W,l)}$ в точности равна i в l-ом слое МПП-кода при фиксированной комбинации W ошибок.

Введем понятие обобщенного синдрома $\mathbf{S}$.

$$\mathbf{S} = (\mathbf{S}_1\, \mathbf{S}_2 \ldots \mathbf{S}_\ell) = \left(\underbrace{S_{1,1}\, S_{1,2} \ldots S_{1,b}}_{\mathbf{S}_1}\, \underbrace{S_{2,1}\, S_{2,2} \ldots S_{2,b}}_{\mathbf{S}_2} \ldots \underbrace{S_{\ell,1}\, S_{\ell,2} \ldots S_{\ell,b}}_{\mathbf{S}_\ell} \right),$$

где $S_{j,l} = 1$ если синдром j-го, $j = 1, 2, ..., b$, кода-компонента l-го, $l = 1, 2, ..., \ell$, слоя не равен нулю, иначе – $S_{j,l} = 0$.

Компонента $\mathbf{S}_l$ обобщенного синдрома $\mathbf{S}$ соответствует l-ому слою МПП-кода. Определим вероятность пересечения двух событий, $E_{\sum}^{(W,l)} = i$ и $|\mathbf{S}_l| = j$:

$$P_W\left(E_{\sum}^{(W,l)} = i \cap |\mathbf{S}_l| = j\right) = \frac{\begin{pmatrix} b \\ j \end{pmatrix} N_{i,j}(W, n_0, b)}{\begin{pmatrix} n \\ W \end{pmatrix}}, \tag{2.8}$$

где $N_{i,j}\left(W, n_0, b\right)$ – количество таких перестановок слоя проверочной матрицы МПП-кода (или, что тоже самое, количество комбинаций W ошибок), что сумма условия (2.3) для данного слоя равна i и фиксированные j позиций, например, первые, компоненты $\mathbf{S}_l$ обобщенного синдрома $\mathbf{S}$ равны единице при фиксированной комбинации W ошибок (при фиксированной перестановке слоя проверочной матрицы МПП-кода).

Введем производящую функцию $V_j\left(s, v\right)$ для величины $N_{i,j}\left(W, n_0, b\right)$ следующим образом:

$$V_j\left(s, v\right) = \sum_{i \geq 0} \sum_{t=0}^{n} N_{i,j}\left(t, n_0, b\right) v^i s^t.$$

Откуда следует очевидное неравенство:

$$V_j\left(s, v\right) = \sum_{i \geq 0} \sum_{t=0}^{n} N_{i,j}\left(t, n_0, b\right) v^i s^t \geqslant N_{i,j}\left(W, n_0, b\right) v^i s^W,$$

которое верно при любых $v,\ s > 0$.

Следовательно, величину $N_{i,j}\left(W, n_0, b\right)$ можно оценить сверху:

$$N_{i,j}\left(W, n_0, b\right) \leqslant \frac{V_j\left(s, v\right)}{s^W v^i},\ \forall s,\ v > 0.$$

Наиболее близкая граница получается при минимизации по $v,\ s > 0$:

$$N_{i,j}\left(W, n_0, b\right) \leqslant \min_{s, v > 0} \left\{ \frac{V_j\left(s, v\right)}{s^W v^i} \right\} \tag{2.9}$$

Каждый из b кодов-компонентов одного слоя МПП-кода проверяет непересекающийся с другими набор, состоящий из n_0 символов. Если код-компонент обнаруживает ошибку, то соответствующий компонент $S_{l,i}$ обобщенного синдрома $\mathbf{S}$ по определению равен единице, иначе - нулю. Также ясно, что ребра, рассматриваемые в сумме условия (2.3), смежны с компонентными кодами, которые обнаружили ошибки. В силу определений производящих

функций $g_e(s, v, n_0)$ и $g_0(s, n_0)$ и условия, что фиксированные j позиции обобщенного синдрома $\mathbf{S}$ равны единице, производящую функцию $V_j(s, v)$ можно записать следующим образом:

$$V_j(s, v) = (g_e(s, v, n_0))^j (g_0(s, n_0))^{b-j}. \tag{2.10}$$

Подставив (2.10) в (2.9), получим:

$$N_{i,j}(W, n_0, b) \leqslant \min_{s,v>0} \left\{ \frac{(g_e(s, v, n_0))^j (g_0(s, n_0))^{b-j}}{s^W v^i} \right\}$$

Полученную оценку на $N_{i,j}(W, n_0, b)$ подставив в (2.8), найдем:

$$P_W\left(E_\Sigma^{(W,l)} = i \cap |\mathbf{S}_l| = j\right) \leqslant$$

$$\leqslant \frac{\begin{pmatrix} b \\ j \end{pmatrix}}{\begin{pmatrix} n \\ W \end{pmatrix}} \min_{s,v>0} \left\{ \frac{(g_e(s, v, n_0))^j (g_0(s, n_0))^{b-j}}{s^W v^i} \right\}. \tag{2.11}$$

Вероятность $P_W\left(E_\Sigma^{(W,l)} = i\right)$ можно вычислить как сумму вероятностей $P_W\left(E_\Sigma^{(W,l)} = i \cap |\mathbf{S}_l| = j\right)$ по всем возможным значениям $|\mathbf{S}_l|$:

$$P_W\left(E_\Sigma^{(W,l)} = i\right) = \sum_{j=0}^{b} P\left(E_\Sigma^{(W,l)} = i \cap |\mathbf{S}_l| = j\right). \tag{2.12}$$

Подставляя (2.11) в (2.12), получим оценку на $P_W\left(E_\Sigma^{(W,l)} = i\right)$:

$$P_W\left(E_\Sigma^{(W,l)} = i\right) \leqslant \sum_{j=0}^{b} \frac{\begin{pmatrix} b \\ i \end{pmatrix}}{\begin{pmatrix} n \\ W \end{pmatrix}} \min_{s,v>0} \left\{ \frac{(g_e(s, v, n_0))^j (g_0(s, n_0))^{b-j}}{s^W v^i} \right\} \leqslant$$

$$\leqslant \begin{pmatrix} n \\ W \end{pmatrix}^{-1} \min_{s,v>0} \left\{ s^{-W} v^{-i} \sum_{j=0}^{b} \begin{pmatrix} b \\ j \end{pmatrix} \left(g_e\left(s,v,n_0\right)\right)^j \left(g_0\left(s,n_0\right)\right)^{b-j} \right\} =$$

$$= \begin{pmatrix} n \\ W \end{pmatrix}^{-1} \min_{s,v>0} \left\{ s^{-W} v^{-i} \left(g_e\left(s,v,n_0\right) + g_0\left(s,n_0\right)\right)^b \right\}. \qquad (2.13)$$

Следовательно, можно записать оценку на производящую функцию $U_W^{(l)}(u)$, подставив (2.13) в (2.7):

$$U_W^{(l)}(u) = \sum_{i=0}^{W} P_W\left(E_\Sigma^{(W,l)} = i\right) u^i \leqslant$$

$$\leqslant \begin{pmatrix} n \\ W \end{pmatrix}^{-1} \sum_{i=0}^{W} \min_{s,v>0} \left\{ s^{-W} v^{-i} \left(g_e\left(s,v,n_0\right) + g_0\left(s,n_0\right)\right)^b \right\} u^i \leqslant$$

$$\leqslant \begin{pmatrix} n \\ W \end{pmatrix}^{-1} \min_{s,v>0} \left\{ s^{-W} \left(g_e\left(s,v,n_0\right) + g\left(v,n_0\right)\right)^b \sum_{i=0}^{W} \left(\frac{u}{v}\right)^i \right\}. \qquad (2.14)$$

Рассмотрим следующее неравенство:

$$\sum_{i=0}^{W} \left(\frac{u}{v}\right)^i \leqslant \sum_{i\geqslant 0} \left(\frac{u}{v}\right)^i, \forall u, v > 0.$$

Тогда можно записать:

$$\sum_{i\geqslant 0} \left(\frac{u}{v}\right)^i = \frac{1}{1-\frac{u}{v}}, \; \forall u, v : 0 < \frac{u}{v} < 1. \qquad (2.15)$$

Запишем оценку на $U_W^{(l)}(u)$ в замкнутом виде, подставив (2.15) в (2.14):

$$U_W^{(l)}(u) \leqslant \begin{pmatrix} n \\ W \end{pmatrix}^{-1} \min_{s,v>0} \left\{ s^{-W} \left(g_e\left(s,v,n_0\right) + g_0\left(s,n_0\right)\right)^b \frac{1}{1-\frac{u}{v}} \right\}, \qquad (2.16)$$

которая верна при любых $0 < u < v$.

Поскольку слои независимы, то полная сумма условия (2.3) $E_{\sum}^{(W)}$ складывается из ℓ независимых случайных величин, равных частичным суммам $E_{\sum}^{(W,l)}$, $l = 1, 2, ..., \ell$.

Тогда производящая функция вероятностей того, что сумма условия (2.3) равна заданному числу,

$$U_W(u) = \sum_{i \geq 0} P_W\left(E_{\sum}^{(W)} = i\right) u^i \tag{2.17}$$

равна произведению ℓ производящих функций $U_W^{(l)}(u)$, $l = 1, 2, ..., \ell$:

$$U_W(u) = \prod_{l=1}^{\ell} U_W^{(l)}(u) = \left(U_W^{(1)}(u)\right)^{\ell}. \tag{2.18}$$

Из (2.16) и (2.18) получаем:

$$U_W(u) \leqslant \begin{pmatrix} n \\ W \end{pmatrix}^{-\ell} \min_{s,v>0} \left\{ s^{-W\ell} \left(g_e(s, v, n_0) + g_0(s, n_0)\right)^{b\ell} \frac{1}{\left(1 - \frac{u}{v}\right)^{\ell}} \right\}, \tag{2.19}$$

для $0 < u < v$.

Вероятность того, что сумма условия (2.3) меньше $W\ell$ равна

$$P_W\left(E_{\sum}^{(W)} \leqslant W\ell\right) = \sum_{i=0}^{W\ell} P_W\left(E_{\sum}^{(W)} = i\right),$$

т.е. равна сумме коэффициентов первых $W\ell$ членов производящей функции $U_W(u)$ (см. (2.17)).

Введем следующую производящую функцию:

$$Q_W(u) = U_W(u) \frac{1}{1-u} \tag{2.20}$$

Заметим, что коэффициент при $u^{W\ell}$ производящей функции $Q_W(u)$ равен сумме коэффициентов первых $W\ell$ членов производящей функции $U_W(u)$, т.е.:

$$Q_W(u) = \sum_{i \geqslant 0} P_W\left(E_\Sigma^{(W)} \leqslant i\right) u^i.$$

Запишем неравенство

$$\frac{1}{1-u} \leqslant \frac{1}{1-\frac{u}{v}}, \tag{2.21}$$

которое верно при $0 < u < v$ и $0 < v < 1$.

Тогда, подставив (2.19) в (2.20) и воспользовавшись (2.21), можно записать

$$Q_W(u) \leqslant$$

$$\leqslant \begin{pmatrix} n \\ W \end{pmatrix}^{-\ell} \min_{s,v>0} \left\{ s^{-W\ell} \left(g_e(s,v,n_0) + g_0(s,n_0)\right)^{b\ell} \frac{1}{\left(1-\frac{u}{v}\right)^\ell} \right\} \frac{1}{1-u} \leqslant$$

$$\leqslant \begin{pmatrix} n \\ W \end{pmatrix}^{-\ell} \min_{s>0,0<v<1} \left\{ s^{-W\ell} \left(g_e(s,v,n_0) + g_0(s,n_0)\right)^{b\ell} \frac{1}{\left(1-\frac{u}{v}\right)^{\ell+1}} \right\},$$

для $0 < u < v$.

Известно, что коэффициент при $u^{W\ell}$ производящей функции $\frac{1}{\left(1-\frac{u}{v}\right)^{\ell+1}}$ равен

$$\begin{pmatrix} \ell + W\ell \\ \ell \end{pmatrix} v^{-W\ell}.$$

Тогда вероятность $P_W\left(E_\Sigma^{(W)} \leqslant W\ell\right)$ можно записать следующим образом:

$$P_W\left(E_\Sigma^{(W)} \leqslant W\ell\right) \leqslant \begin{pmatrix} n \\ W \end{pmatrix}^{-\ell} \begin{pmatrix} \ell + W\ell \\ \ell \end{pmatrix} \times$$

$$\times \min_{s>0,0<v<1} \left\{ (sv)^{-W\ell} \left(g_e(s,v,n_0) + g_0(s,n_0)\right)^{b\ell} \right\}. \tag{2.22}$$

Используя неравенство

$$\begin{pmatrix} n \\ \omega n \end{pmatrix} \leqslant 2^{nh(\omega)},$$

где асимптотическое равенство достигается при $n \to \infty$, и (2.22), получаем

$$P_W\left(E_\Sigma^{(W)} \leqslant W\ell\right) \leqslant 2^{-n\ell F_e(\omega, n_0)}.$$

▲

Рассмотрим вероятность найти код, сумма условия (2.3) для которого меньше либо равна $W\ell$ хотя бы для одной комбинации ошибок веса W. Если эта вероятность меньше единицы, значит, существует код, для которого условие (2.3) выполняется для любой комбинации ошибок веса W:

$$\begin{pmatrix} n \\ W \end{pmatrix} P_W\left(E_\Sigma^{(W)} \leqslant W\ell\right) < 1. \tag{2.23}$$

Для того, чтобы найти максимальную кратность ошибок, для которой выполняется условие (2.23) нужно решить уравнение:

$$\begin{pmatrix} n \\ W \end{pmatrix} P_W\left(E_\Sigma^{(W)} \leqslant W\ell\right) = 1.$$

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

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

Заметим, что условие (2.23) не гарантирует нам существование такого кода, что при всех W вплоть до максимального условие (2.3) выполняется.

Строго говоря, возможно, что для различных значений W существуют различные коды, для которых $E_{\sum}^{(W)} \geqslant W\ell$. Условие (2.23) используется только для поиска максимального значения W.

Докажем теперь, что в ансамбле $\mathscr{E}(n_0, \ell, b_0)$ существует код, для которого условие (2.3) выполняется при всех W вплоть до максимального. Введем следующую функцию:

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

Если существует ω_0, удовлетворяющее следующим условиям

$$\begin{cases} G(\omega_0) = 0 \\ G(\omega) > 0 \quad \forall \omega \in (0, \omega_0) \end{cases} \tag{2.24}$$

то верно следующее

Т е о р е м а 2.2. *В ансамбле $\mathscr{E}(n_0, \ell, b_0)$ МПП-кодов существует коды (с вероятностью p: $\lim\limits_{n\to\infty} p = 1$), такие что $E_{\sum}^{(W)} > W\ell$ для любой комбинации ошибок веса $W \leqslant \lfloor \omega_0 n \rfloor$, $\omega_0 = \bar{\omega_0} - \varepsilon \ \forall \varepsilon > 0$.*

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

$$\sum_{W=1}^{\lfloor \omega_0 n \rfloor} \begin{pmatrix} n \\ W \end{pmatrix} P_W\left(E_{\sum}^{(W)} \leqslant W\ell\right) < 1.$$

В левой части стоит оценка сверху для вероятности кодов, условие (2.3) для которых не выполняется при какой-либо последовательности. Перепишем это условие в следующем виде

$$\lim_{n\to\infty} \sum_{W=1}^{\lfloor \omega_0 n \rfloor} 2^{-n\left(\ell F_e\left(\frac{W}{n}, n_0\right) - h\left(\frac{W}{n}\right)\right)} < 1.$$

Выберем сколь угодно малую величину ε' и разобьем наш придел на следующие два:

$$\lim_{n\to\infty}\sum_{W=1}^{\lfloor\varepsilon' n\rfloor} 2^{-n\left(\ell F_e\left(\frac{W}{n},n_0\right)-h\left(\frac{W}{n}\right)\right)} \tag{2.25}$$

$$\lim_{n\to\infty}\sum_{W=\lceil\varepsilon' n\rceil}^{\lfloor\omega_0 n\rfloor} 2^{-n\left(\ell F_e\left(\frac{W}{n},n_0\right)-h\left(\frac{W}{n}\right)\right)} \tag{2.26}$$

Рассмотрим сначала предел (2.26). Функция $G(\omega)=\ell F_e(\omega,n_0)-h(\omega)>0\ \forall\omega\in[\varepsilon',\omega_0]$, следовательно, она ограничена снизу на этом отрезке. Пусть $G_0=\min\limits_{\omega\in[\varepsilon',\omega_0]} G(\omega)$, $G_0>0$, тогда

$$0\leqslant\lim_{n\to\infty}\sum_{W=\lceil\varepsilon' n\rceil}^{\lfloor\omega_0 n\rfloor} 2^{-n\left(\ell F_e\left(\frac{W}{n},n_0\right)-h(\omega)\right)}\leqslant$$

$$\leqslant\lim\sum_{W=\lceil\varepsilon' n\rceil}^{\lfloor\omega_0 n\rfloor} 2^{-nG_0}=\lim_{n\to\infty}\left(\left(\lfloor\omega_0 n\rfloor-\lceil\varepsilon' n\rceil+1\right)2^{-nG_0}\right)=0.$$

Таким образом,

$$\lim_{n\to\infty}\sum_{W=\lceil\varepsilon' n\rceil}^{\lfloor\omega_0 n\rfloor} 2^{-n\left(\ell F_e\left(\frac{W}{n},n_0\right)-h\left(\frac{W}{n}\right)\right)}=0.$$

Теперь рассмотрим предел (2.25). Перепишем функцию $G(\omega)$ в следующем виде:

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

Поскольку переменные s и v являются фиктивными, то они могут принимать любое значение, если выполняются условия $s>0$ и $0<v<1$. Тогда положим $s=v=\sqrt[4]{\omega}$:

$$G^*(\omega)=(\ell-1)h(\omega)+$$

$$+\ell\left(\frac{\omega}{2}\log_2\omega-\frac{1}{n_0}\log_2\left(g_e\left(\sqrt[4]{\omega},\sqrt[4]{\omega},n_0\right)+g_0\left(\sqrt[4]{\omega},n_0\right)\right)\right).$$

Преобразуем $G^*(\omega)$ к следующему виду:

$$G^*(\omega)=-\left(\frac{\ell}{2}-1\right)\omega\log_2\omega-(\ell-1)(1-\omega)\log_2(1-\omega)-$$
$$-\frac{\ell}{n_0}\log_2\left(g_e\left(\sqrt[4]{\omega},\sqrt[4]{\omega},n_0\right)+g_0\left(\sqrt[4]{\omega},n_0\right)\right).$$

Можно показать, что $g_e(s,v,n_0)+g_0(s,n_0)\leqslant(1+s)^{n_0}$ при $0<s<1$ и $0<v<1$. Тогда после преобразований получим:

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

Легко заметить, что

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

Как следует из построения МПП-кода $\ell>2$, тогда $\left(\frac{\ell}{2}-1\right)>0$, следовательно:

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

$$\lim_{n\to\infty}\sum_{W=1}^{\lfloor\varepsilon' n\rfloor}2^{-nG\left(\frac{W}{n}\right)}\leqslant\lim_{n\to\infty}\sum_{W=1}^{\lfloor\varepsilon' n\rfloor}2^{n\cdot c_1\cdot\frac{W}{n}\cdot\log_2\frac{W}{n}-n\cdot c_2\cdot\frac{W}{n}}=$$
$$=\lim_{n\to\infty}\sum_{W=1}^{\lfloor\varepsilon' n\rfloor}\left(\frac{W}{n}\right)^{c_1W}2^{-c_2W}\leqslant\lim_{n\to\infty}\sum_{W=1}^{\lfloor\varepsilon' n\rfloor}\left((\varepsilon')^{c_1}2^{-c_2}\right)^W=\frac{(\varepsilon')^{c_1}2^{-c_2}}{1-(\varepsilon')^{c_1}2^{-c_2}}=\varepsilon''$$

Отметим, что знак c_2 не важен, т.к. значение ε'' всегда можно сделать сколь угодно малым, правильно подобрав ε'.

Так как оба предела существуют и конечны, то

$$\lim_{n\to\infty}\sum_{W=1}^{\lfloor\omega_0 n\rfloor} 2^{-n\left(\ell F_e\left(\frac{W}{n},n_0\right)-h\left(\frac{W}{n}\right)\right)} \leqslant \varepsilon'' < 1.$$

▲

Таким образом, мы доказали, что в ансамбле $\mathscr{E}(n_0,\ell,b_0)$ почти для всех кодов выполняется условие (2.3) для любой последовательности веса $W \leqslant \lfloor\omega_0 n\rfloor$.

Корректирующая способность и сложность алгоритма декодирования

В предыдущем разделе мы доказали, что в ансамбле $\mathscr{E}(n_0,\ell,b_0)$ существует МПП-код, для которого выполняется условие (2.3) для любой последовательности веса $W \leqslant \lfloor\omega_0 n\rfloor$. Другими словами, в ансамбле $\mathscr{E}(n_0,\ell,b_0)$ существует МПП-код, при декодировании которого алгоритм $\mathscr{A}_M$ для любой последовательность веса $W \leqslant \lfloor\omega_0 n\rfloor$ найдет такой символ, что его замена уменьшит вес обобщенного синдрома. Таким образом, если бы на каждой итерации алгоритма $\mathscr{A}_M$ вес обобщенного синдрома уменьшался, ты мы рано или поздно получили бы нулевой синдром в силу его конечности. Но как отмечалось ранее, условие (2.3) не гарантирует, что будет заменен непременно ошибочный символ, т.е. может случиться так, что новый ошибочный символ будет добавлен в последовательность. А это значит, что на i-ой итерации алгоритма $\mathscr{A}_M$ вес последовательности может стать равным $W^{(i)} \geqslant \lfloor\omega_0 n\rfloor$. В результате чего мы не сможем гарантировать, что в ансамбле $\mathscr{E}(n_0,\ell,b_0)$ найдется МПП-код, для которого будет выполняться условие (2.3) для данной последовательности. Следовательно, необходимо найти найти такую начальную кратность ошибок $W_0 = \lfloor\alpha_0\omega_0 n\rfloor \leqslant \lfloor\omega_0 n\rfloor$, что при декодировании по алгоритму $\mathscr{A}_M$ вес последовательности не превысит $\lfloor\omega_0 n\rfloor$.

Л е м м а 2.3. *Если начальная кратность ошибок* $W_0 \leqslant \lfloor\alpha_0\omega_0 n\rfloor$, *где* α_0

– корень следующего уравнения:

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

то количество ошибок в декодируемой последовательности не превысит $\lfloor \omega_0 n \rfloor$ *при декодировании МПП-кода из ансамбля* $\mathscr{E}(n_0, \ell, b_0)$ *по алгоритму* $\mathscr{A}_M$.

Доказательство. Пусть начальная кратность ошибок составляет $W_1 = \alpha_0 W$, где $W \leqslant \lfloor \omega_0 n \rfloor$. Тогда вес обобщенного синдрома $\mathbf{S_1}$ для данной комбинации ошибок можно оценить следующим образом:

$$|\mathbf{S_1}| \leqslant W_1 \ell = \alpha_0 W \ell.$$

Пусть в некоторый момент при декодировании по алгоритму $\mathscr{A}_M$ кратность ошибок достигла значения $W_2 = W$, т.е в последовательность было добалено $W_2 - W_1 = (1 - \alpha_0) W$ новых ошибок. Поскольку замена каждого символа уменьшает вес обобщенного синдрома как минимум на единцу, то вес синдрома $\mathbf{S_2}$ можно оценить следующим образом:

$$|\mathbf{S_2}| \leqslant |\mathbf{S_1}| - (1 - \alpha_0) W \leqslant \frac{\ell - \frac{1-\alpha_0}{\alpha_0}}{\ell} \alpha_0 W \ell.$$

В работе [7] показано, что вероятность того, что для случайного МПП-кода вес синдрома $|\mathbf{S}| < \alpha W \ell$ для последовательности веса $W = \omega n$, ограничена сверху:

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

Таким образом, при $n \to \infty$ почти у всех МПП-кодов вес обобщенного синдрома $|\mathbf{S}| > \alpha W \ell$ для последовательности веса W.

Следовательно, если выбрать такой код, что для него $|\mathbf{S_2}| > \frac{\ell - \frac{1-\alpha_0}{\alpha_0}}{\ell} \alpha_0 W \ell$ при количестве ошибок $W = \lfloor \omega_0 n \rfloor$, то при декодировании последовательности с начальной кратностью ошибок $W_0 \leqslant \lfloor \alpha_0 \omega_0 n \rfloor$ вес последовательности

не превысит $\lfloor \omega_0 n \rfloor$, иначе противоречие. Тогда используя результат работы [7], составим следующее уравнение, положив $\omega = \omega_0$:

$$h(\omega_0) - \ell F_{\mathbf{S}}(\alpha, \omega_0, n_0),$$

откуда получим α_0. ▲

Рассмотрим теперь сложность декодирования по алгоритму $\mathscr{A}_M$.

Л е м м а 2.4. *Сложность одной итерации декодирования равна* $\mathcal{O}(n)$.

Д о к а з а т е л ь с т в о. Алгоритм проходит по всем n символам. На проверку количества смежных корректирующих ребер требуется порядка $\mathcal{O}(1)$ операций. ▲

Л е м м а 2.5. *Пусть* $E_{\sum}^{(W)} > (1+\varepsilon) W\ell$, *где* $\varepsilon > 0$ – *сколь угодно малая величина, тогда за одну итерацию алгоритма* $\mathscr{A}_M$ *будут заменены по крайней мере* δW *ошибочных символов, где*

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

Д о к а з а т е л ь с т в о. Обозначим через W_1 количество символов, которые удовлетворяют условию замены (2.2) в алгоритме $\mathscr{A}_M$. Как отмечалось выше, условие замены (2.2) можно записать в виде условия (2.4). Поскольку сумма условия (2.4) для символа, удовлетворяющего условию замены, равна не более 2ℓ, а для символа, не удовлетворяющего условию замены, равна не более ℓ, то можно записать следующее неравенство:

$$2W_1\ell + (W - W_1)\ell \geqslant E_{\sum}^{(W)} > (1+\varepsilon) W\ell.$$

Откуда

$$\delta' = \frac{W_1}{W} > \varepsilon.$$

Так как синдром и сумма условия (2.4) пересчитываются после каждой замены символа, то его замена влияет на решение относительно оставшихся символов. Как следует из построения кода каждый символ входит ровно в ℓ проверок, каждая проверка содержит ровно n_0, следовательно, замена одного символа влияет не более чем на $\ell\,(n_0-1)$ оставшийся символ (за исключением его самого).

Таким образом,

$$\delta = \frac{\delta'}{\ell\,(n_0-1)} > \frac{\varepsilon}{\ell\,(n_0-1)}.$$

▲

С л е д с т в и е 2.1. *Обозначим через* $|\mathbf{S}_{i-1}|$ *вес обобщенного синдрома до* i*-ой 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 предыдущему результату, 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 $W_{i-1} \geqslant \frac{|S_{i-1}|}{\ell}$, то

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

▲

Т е о р е м а 2.3. *При* $E_{\sum}^{(W)} > (1+\varepsilon)\,W\ell$ *и начальном количестве ошибок* $W_0 = \lfloor \alpha_0\omega_0 n \rfloor$ *алгоритм* $\mathscr{A}_M$ *исправит все ошибки за* $\mathcal{O}\,(n\log_2 n)$ *операций.*

Доказательство. Оценим число итераций:

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

Так как $|\mathbf{S}_0|=\sigma W\ell$, где $\sigma>0$, то:

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

▲

2.2.4. Численные значения оценки доли ошибок, гарантированно исправимых Г-МПП-кодом

Выбор производящих функций

Запишем введенные выше производящие функции для компонентного кода с проверкой на четность. Поскольку компонентный код с проверкой на четность обнаруживает только комбинацию ошибок нечетной кратности, можно записать:

$$g_0(s,n_0)=\frac{(1+s)^{n_0}+(1-s)^{n_0}}{2},$$
$$g_1(s,n_0)=\frac{(1+s)^{n_0}-(1-s)^{n_0}}{2}.$$

Отметим, что условие (2.3) было получено для подграфа графа Таннера (см. рис. 2.2), содержащего только вершины-символы, соответствующие ошибочным символам, и все вершины-проверки, связанные с этими вершинами-символами. Следовательно, и производящая функция $g_e(s,v,n_0)$ должна быть записана для данного подграфа. Понятно, что множество $A_{1\to1}$ для компонентного кода с проверкой на четность всегда пусто, т.к. при инвертировании любого символа кода с проверкой на четность его проверка становится либо выполненной, либо невыполненной. Таким образом, нам необходимо

посчитать только количество ребер в рассматриваемом подграфе, которые соединены с компонентными кодами, обнаружившими ошибки ($A_{1\to 0}$). Понятно, что из каждого такого компонентного кода выходит количество ребер равное количеству ошибок, содержащихся в данном коде (нечетное число). Но в силу условия (2.3) мы должны посчитать их удвоенное значение. Следовательно, можно записать:

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

Анализ численных результатов

При рассмотрении Г-МПП-кодов с заданной скорость R удобно задавать количество слоев ℓ и вычислять необходимую длину компонентного кода n_0:

$$n_0 = \left\lceil \frac{\ell}{1-R} \right\rceil.$$

Поэтому численные результаты были получены для заданных диапазонов скоростей кода R и количества слоев ℓ и вычисленных значений длин кода-компонента n_0.

В соответствии с теоремой 2.1, значение доли гарантировано исправимых ошибок, полученное по оценке представленной в данной работе, будем обозначать ω_t, а значение, полученное по оценке [9], в соответствии с работой [9] – $\omega_\alpha/2$.

На рис. 2.3 представлено семейство зависимостей доли ω_t гарантированно исправимых ошибок от количества слоев ℓ при различных скоростях R. Как видно из рис. 2.3 для каждой скорости R существует оптимальное значение количества слоев ℓ (длины кода-компонента n_0), при котором достигается максимальное значение ω_t. Также можно заметить, что при $\ell < 5$ доля гарантированно исправимых ошибок ω_t уменьшается до нуля, а при увеличении

количества слоев ℓ после достижения максимума значение ω_t медленно убывает. При увеличении скорости R достигаемые значения ω_t плавно убывают.

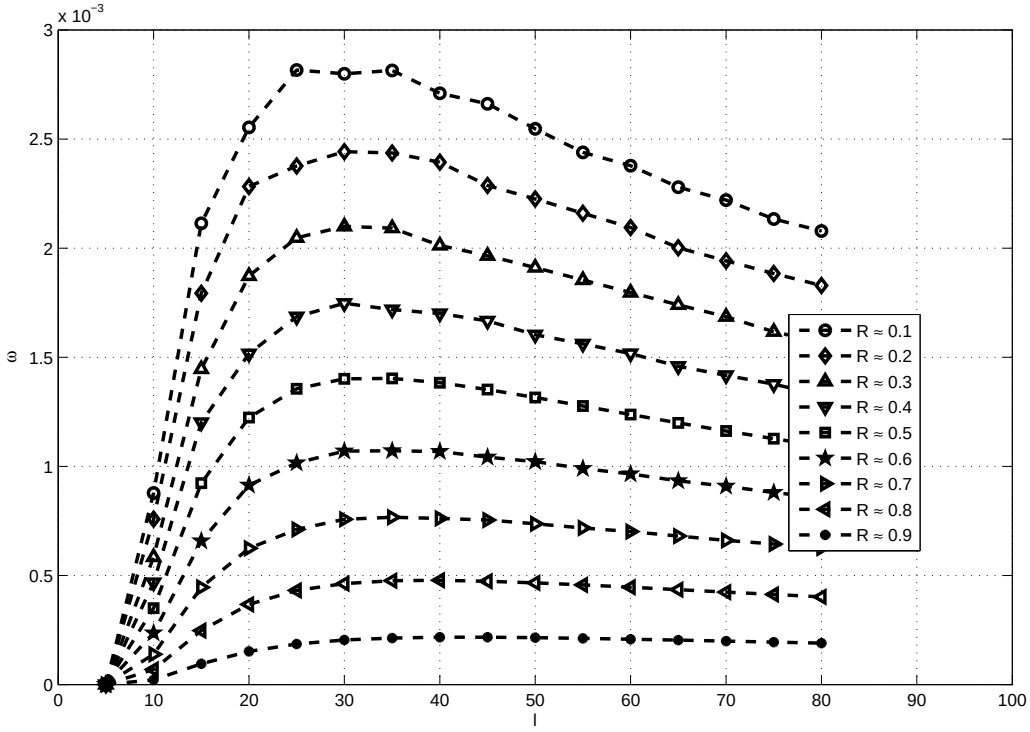

Рис. 2.3. Семейство зависимостей доли ω_t гарантированно исправимых ошибок от количества слоев ℓ при различных скоростях R Г-МПП-кода

На рис. 2.4 и в табл. 2.1 представлены численные результаты доли ω_t и $\omega_\alpha/2$ гарантированно исправимых ошибок при декодировании по алгоритму $\mathscr{A}_M$ от количества слоев (длины кода-компонента) двоичного Г-МПП-кода с фиксированной скоростью $R \approx 0,5$. Из результатов следует, что значения, полученные по предложенной оценке, превосходят значения, полученные по оценке [9], при любых параметрах Г-МПП-кода с фиксированной скоростью $R = 0,5$.

На рис. 2.5 и в табл. 2.2 приведена зависимость найденных наибольших значений долей гарантированно исправимых ошибок от скорости R Г-МПП-кода. Интересно отметить, что предложенная оценка улучшает ранее известную лучшую оценку [9] почти в фиксированное число раз: примерно, в $1,06$ раза при скорости $R \leq 0,5$ и в $1,05$ раза при $R > 0,5$.

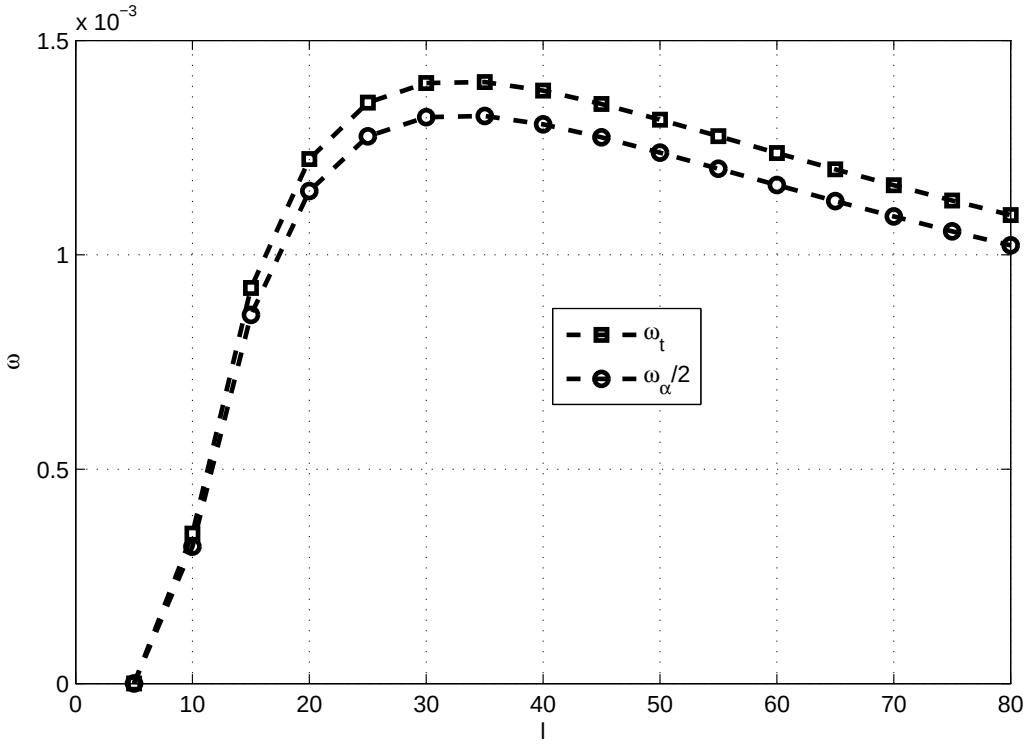

Рис. 2.4. Зависимости долей ω_t и $\omega_\alpha/2$ гарантированно исправимых ошибок от количества слоев ℓ при фиксированной скорости $R \approx 0,5$ Г-МПП-кода

2.2.5. Численные значения оценки доли ошибок, гарантированно исправимых Х-МПП-кодом

Выбор производящих функций

Запишем введенные выше производящие функции $g_0(s, n_0)$ и $g_1(s, n_0)$ для компонентного кода Хэмминга:

$$g_0(s, n_0) = \frac{(1+s)^{n_0} + n_0(1-s)\left(1-s^2\right)^{\frac{n_0-1}{2}}}{n_0+1}, \tag{2.27}$$

$$g_1(s, n_0) = (1+s)^{n_0} - g_0(s, n_0). \tag{2.28}$$

Очевидно, что если проверка кода Хэмминга не выполняется, то всегда существует ровно один символ, замена которого даст нулевой синдром. Иными словами для любой обнаруженной комбинации ошибок всегда найдется

Таблица 2.1

Численные результаты зависимости ω_t и $\omega_\alpha/2$ от количества слоев (длины кода-компонента) при фиксированной скорости $R \approx 0,5$ Г-МПП-кода

Доли	$\ell(n_0)$					
	10 (20)	20 (40)	30 (60)	40 (80)	50 (100)	60 (120)
ω_t, 10^{-3}	0,35	1,22	1,40	1,38	1,32	1,24
$\omega_\alpha/2$, 10^{-3}	0,32	1,15	1,32	1,30	1,24	1,16
$\omega_t/\left(\omega_\alpha/2\right)$	1,09	1,06	1,06	1,06	1,06	1,07

Таблица 2.2

Численные результаты зависимости наибольших значений ω_t и $\omega_\alpha/2$ от скорости R Г-МПП-кода

Доли	R				
	0,1	0,3	0,5	0,7	0,9
ω_t, 10^{-3}	2,87	2,10	1,41	0,77	0,22
$\omega_\alpha/2$, 10^{-3}	2,70	1,98	1,33	0,73	0,21
$\omega_t/\left(\omega_\alpha/2\right)$	1,06	1,06	1,06	1,05	1,05

единственное кодовое слово на расстоянии 1. При этом вес обнаруженной комбинации ошибок может быть как на единицу больше (например, комбинации ошибок веса один), так и на единицу меньше (например, комбинации ошибок кратности два), чем вес ближайшего кодового слова. Следовательно, замена данного символа у комбинации ошибок с весом большим, чем у ближайшего кодового слова, приведет к уменьшению количества ошибок, а у комбинации ошибок с меньшим весом - к введению новых. Также важно заметить, что в случае обнаруженной комбинации ошибок замена символа на оставшихся $n_0 - 1$ позициях приведет к тому, что проверка кода Хэмминга останется невыполненной.

Рассмотрим теперь введенный выше подграф графа Таннера, изображенный на рис. 2.2. Каждая проверка данного подграфа с такой обнаруженной

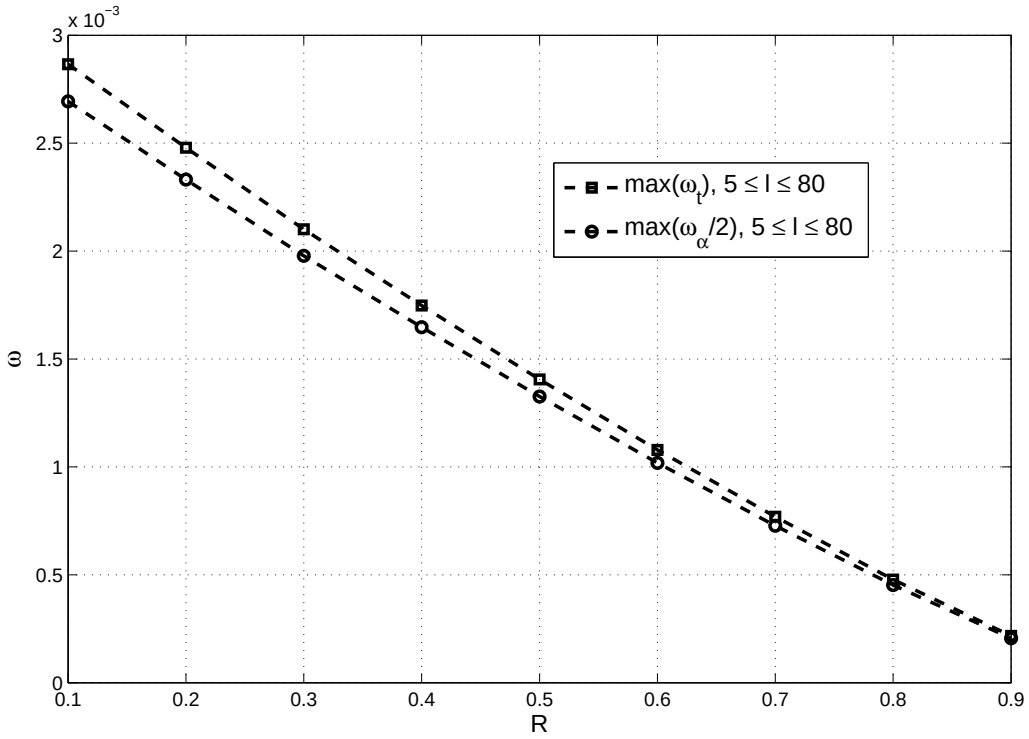

Рис. 2.5. Зависимость максимального значения доли ω_t и $\omega_\alpha/2$ гарантированно исправимых ошибок от скорости R Г-МПП-кода

комбинацией ошибок кратности i, что ее вес на единицу меньше ближайшего кодового слова, входит в множество $A_{1\to1}$ ровно для i символов рассматриваемого подграфа. Иными словами, каждая такая проверка добавляет к сумме $\sum_{i=1}^{W} e_{A_{1\to1}}^{(i)}$ ровно i ребер, а, следовательно, и к сумме условия (2.3) также добавляет ровно i ребер. Если же вес i обнаруженной комбинации ошибок на единицу больше ближайшего кодового слова, то данная проверка входит в множество $A_{1\to0}$ ровно для одного символа подграфа и в $A_{1\to1}$ ровно для $i-1$ символов подграфа. Таким образом, данная проверка добавляет к сумме $\sum_{i=1}^{W} e_{A_{1\to0}}^{(i)}$ одно ребро, а к сумме $\sum_{i=1}^{W} e_{A_{1\to1}}^{(i)}$ – $i-1$ ребро. Тогда к сумме из условия (2.3) добавляется $i+1$ ребро, т.к. сумма $\sum_{i=1}^{W} e_{A_{1\to0}}^{(i)}$ удваивается.

Для формирования таких комбинаций ошибок веса $i+1$, что вес ближайшего кодового слова равен i, необходимо в комбинации ошибок, формирующих кодовые слова веса i, на оставшихся $n_0 - i$ позициях разместить одну ошибку. Пусть $G_0^{(i)}$ количество кодовых слов веса i, тогда количество комби-

наций ошибок, вес которых на единицу больше ближайшего кодового слова, равен $(n_0 - i)\, G_0^{(i)}$. Теперь запишем вспомогательную производящую функцию $g_{A_{1\to 0}}(s, n_0)$ таких комбинаций ошибок, вес которых на единицу больше, чем вес ближайшего кодового слова:

$$g_{A_{1\to 0}}(s, n_0) = \left(n_0 g_0(s, n_0) - \frac{\partial g_0(s, n_0)}{\partial s} s \right) s. \tag{2.29}$$

Тогда производящую функцию $g_e(s, v, n_0)$ таких комбинаций ошибок заданной кратности, что дают ровно заданную сумму ребер из условия (2.3), можно записать следующим образом:

$$g_e(s, v, n_0) = g_{A_{1\to 0}}(sv, n_0)\, v + g_1(sv, n_0) - g_{A_{1\to 0}}(sv, n_0).$$

Анализ численных результатов

Поскольку в отличие от кода с проверкой на четность код Хэммига существует только для определенного набора длин, то при рассмотрении Х-МПП-кодов с заданной скорость R удобно задавать длину кода-компонента n_0 и вычислять количество слоев ℓ:

$$\ell = \left\lfloor \frac{n_0}{\log_2(n_0 + 1)} (1 - R) \right\rfloor.$$

Поэтому численные результаты были получены для заданных диапазонов скоростей кода R и длин компонентных кодов n_0 и вычисленных значений ℓ.

В соответствии с теоремой 2.1, значение доли гарантировано исправимых ошибок, полученное по оценке представленной в данной работе, будем обозначать ω_t, а значение, полученное по оценке [25] – γ_0.

На рис. 2.6 представлено семейство зависимостей доли ω_t гарантированно исправимых ошибок от длины кода-компонента n_0 при различных скоростях R. Как видно из рис. 2.6 для каждой скорости R существует оптимальное значение длины кода-компонента n_0 (количества слоев ℓ), при котором

достигается максимальное значение ω_t. Также можно заметить, что при при увеличении скорости R минимальное значение длины кода-компонента, при котором значение ω_t становится отлично от нуля, увеличивается. При увеличении длины n_0 после достижения максимума значение ω_t резко убывает.

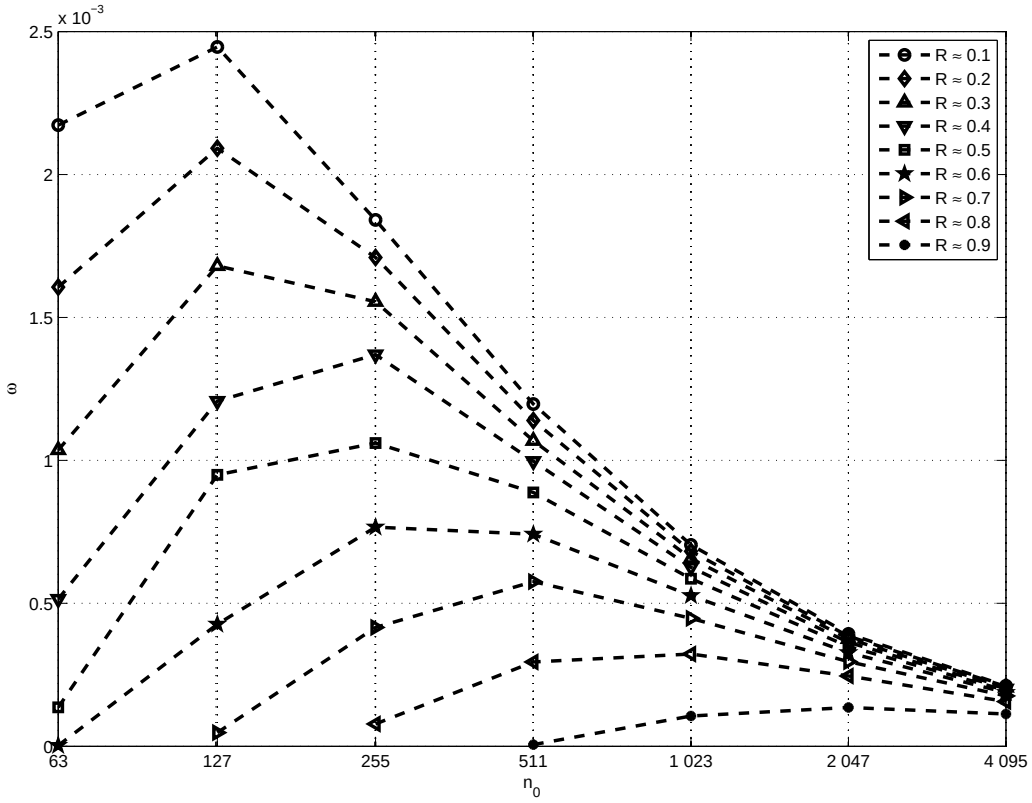

Рис. 2.6. Семейство зависимостей доли ω_t гарантированно исправимых ошибок от длины кода-компонента n_0 при различных скоростях R Х-МПП-кода

На рис. 2.7 и в табл. 2.3 представлены численные результаты доли ω_t и γ_0 гарантированно исправимых ошибок при декодировании по алгоритму $\mathscr{A}_M$ от длины кода-компонента (количества слоев) для двоичного Х-МПП-кода с фиксированной скоростью $R \approx 0,5$. Из результатов следует, что значения, полученные по предложенной оценке, значительно превосходят значения, полученные по оценке [25], при любых значениях параметров МПП-кода Галлагера с фиксированной скоростью $R \approx 0,5$.

На рис. 2.8 и в табл. 2.4 приведена зависимость найденных наибольших значение долей гарантированно исправимых ошибок от скорости R Х-МПП-

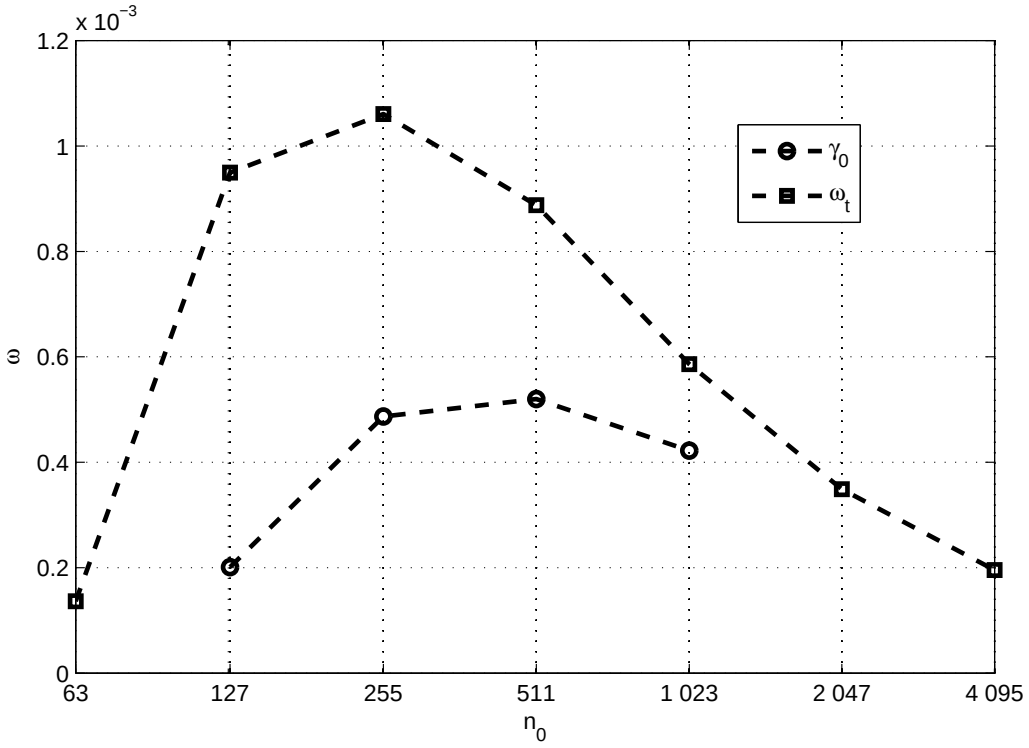

Рис. 2.7. Зависимости долей ω_t и γ_0 гарантированно исправимых ошибок от длины компонентного кода n_0 при фиксированной скорости $R \approx 0,5$ Х-МПП-кода

кода.

2.2.6. Сравнение численных значений оценки доли ошибок, гарантированно исправимых Г-МПП-кодом и Х-МПП-кодом

Сравним полученные значения оценки доли ошибок ω_t, гарантированно исправимых Г-МПП-кодом и Х-МПП-кодом при декодировании по алгоритму $\mathscr{A}_M$ (см. рис. 2.9 и табл. 2.5). Из приведенных результатов видно, что оценка доли ошибок, гарантированно исправимых Г-МПП-кодом, превосходит оценку доли ошибок, гарантированно исправимых Х-МПП-кодом.

Таблица 2.3

Численные результаты зависимости ω_t и γ_0 от количества слоев (длины кода-компонента) при фиксированной скорости $R = 0,5$ Х-МПП-кода

Доли	$n_0(\ell)$			
	127 (9)	255 (15)	511 (28)	1023 (51)
ω_t, 10^{-3}	0,95	1,06	0,89	0,59
γ_0, 10^{-3}	0,20	0,49	0,52	0,42
$omega_t/\gamma_0$	4,75	2,16	1,71	1,40

Таблица 2.4

Численные результаты зависимости наибольших значений ω_t от скорости R Х-МПП-кода

Доли	R				
	0,1	0,3	0,5	0,7	0,9
$\alpha_0\omega_0$, 10^{-3}	2,44	1,68	1,06	0,59	0,14

2.3. Имитационное моделирование алгоритмов декодирования МПП-кода для исправления ошибок

В данном параграфе приведены результаты имитационного моделирования некоторых алгоритмов декодирования МПП-кодов для исправисления ошибок. Рассматривались алгоритмы декодирования Г-МПП-кода и Х-МПП-кода.

В качестве модели канала был выбран двоично-симметричный канал (ДСК) с вероятностью перехода в ошибку (входной вероятностью ошибки) p_t. Для каждого значения p_t испытания проводились до тех пор, пока не будет накоплено не менее 20 отказов от декодирования МПП-кода. Имитационное моделирование останавливалось, если вероятность отказа от декодирования заданного МПП-кода была меньше 10^{-5}.

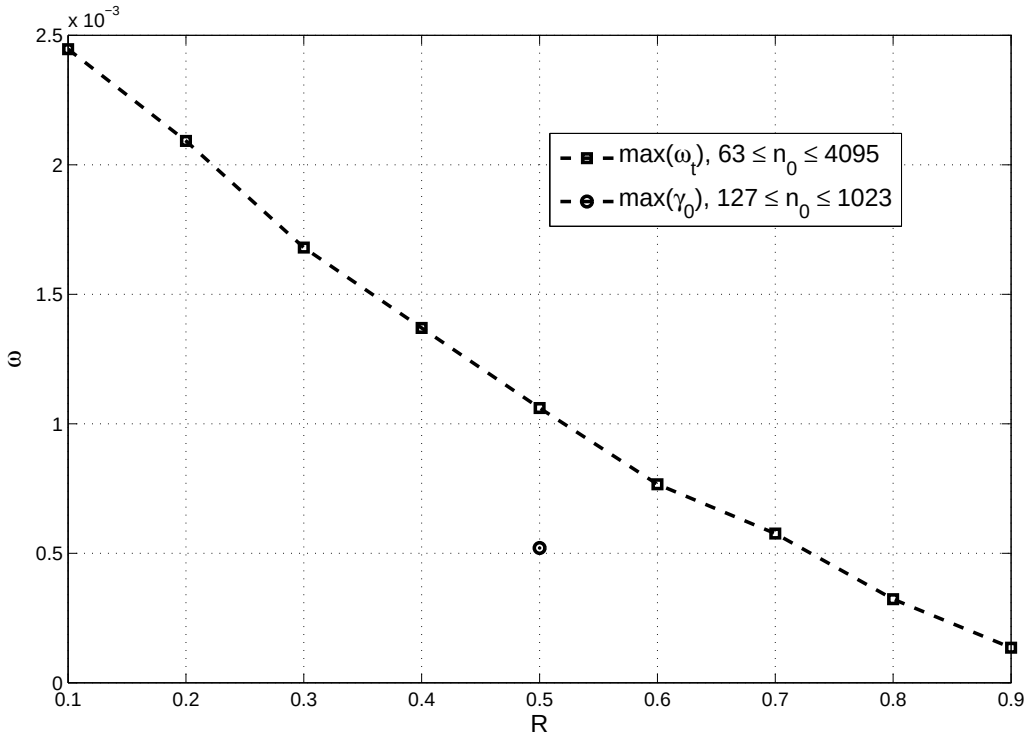

Рис. 2.8. Зависимость максимального значения доли ω_t и γ_0 гарантированно исправимых ошибок от скорости R Х-МПП-кода

2.3.1. Мажоритарный алгоритм декодирования

Одним из самых простых в реализации алгоритмов декодирования является мажоритарный алгоритм $\mathscr{A}_M$, описанный в § 2.2.1. Данный алгоритм рассматривалася применительно к Г-МПП-коду и Х-МПП-коду с различными параметрми.

Анализ результатов моделирования декодирования Г-МПП-кода

Рассмотрим результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Г-МПП-кода при передаче по ДСК с входной вероятностью ошибки p_t. Результаты были получены для заданных заданных значений скоростей кода $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$, количества слоев $\ell = 3, 4, ..., 7$ и соответствующих значений длин кода-компонента n_0.

На рис. 2.10 приведены результаты имитационного моделирования алго-

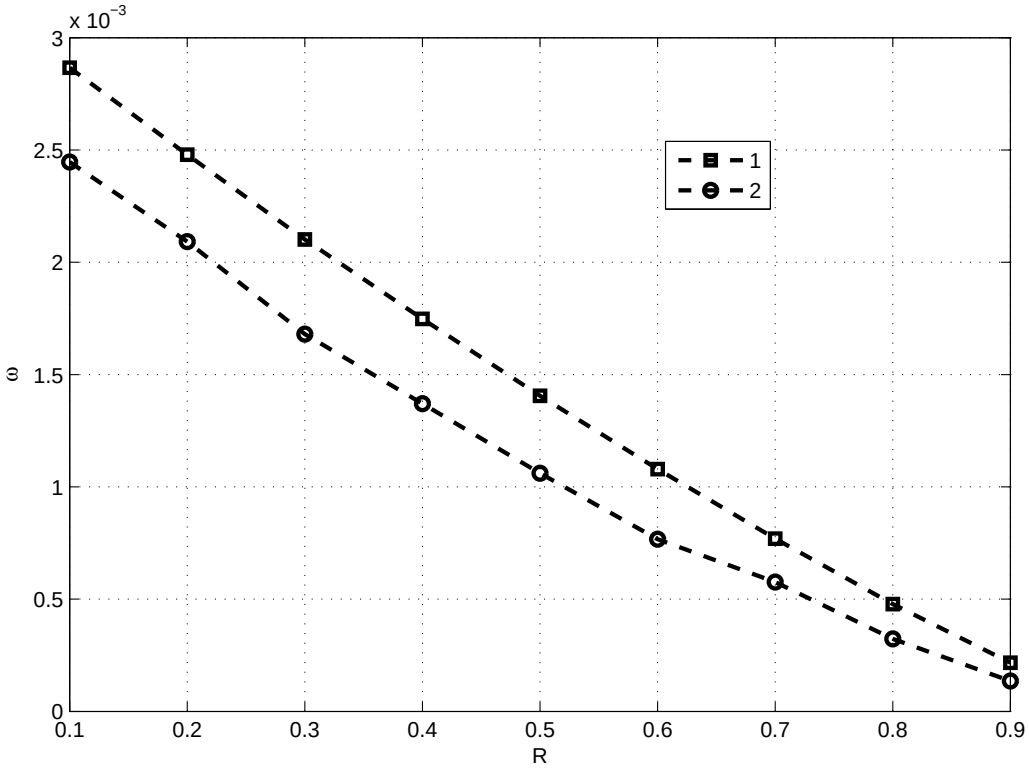

Рис. 2.9. Зависимость наибольших значений оценки доли ω_t гарантированно исправимых ошибок от скорости R Г-МПП-кода (1) и Х-МПП-кода (2)

ритма декодирования $\mathscr{A}_M$ Г-МПП-кода со скоростью $R \approx 0,25$ с различным количеством слоев ℓ при различных значениях входной вероятности p_t. Как видно, вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_t для Г-МПП-кода с $\ell = 6$.

На рис. 2.11 представлены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Г-МПП-кода со скоростью $R \approx 0,5$ с различным количеством слоев ℓ при различных значениях входной вероятности p_t. В данном случае вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_t для Г-МПП-кода с $\ell = 5$.

На рис. 2.12 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Г-МПП-кода со скоростью $R \approx 0,75$ с различным количеством слоев ℓ при различных значениях входной вероятности p_τ. Видно, что в этом случае вероятность отказа от декодирования равная 10^{-5}

Таблица 2.5

Численные результаты зависимости наибольших значений оценки ω_t от скорости R Г-МПП-кода и Х-МПП-кода

МПП-код	R				
	0,1	0,3	0,5	0,7	0,9
Г-МПП-код, 10^{-3}	2,87	2,10	1,41	0,77	0,22
Х-МПП-код, 10^{-3}	2,44	1,68	1,06	0,58	0,14

достигается на наибольшей входной вероятности p_τ для Г-МПП-кода с $\ell = 6$.

Теперь для каждой из рассмотренных скоростей $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$ выбирем те параметры Г-МПП-кода, при которых вероятность отказа от декодирования равная 10^{-5} достигалась при наибольших значения входной вероятности p_t. На рис. 2.13 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Г-МПП-кода с выбранными параметрами в зависимости от входной вероятности ошибки p_t.

Анализ результатов моделирования декодирования Х-МПП-кода

Рассмотрим результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Х-МПП-кода при передаче по ДСК с входной вероятностью ошибки p_t. Результаты были получены для заданных значений скоростей кода $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$, длин кода-компонента $n_0 = 15, 31, 63, 127, 255, 511$ и соотвествующего количества слоев ℓ. Причем для каждой скорости Х-МПП-кода выбиралось наименьшая длина кода-компонента так, чтобы $\ell > 2$.

На рис. 2.14 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Х-МПП-кода со скоростью $R \approx 0,25$ и различной длиной кода-компонента n_0 при различных значениях входной вероятности p_t. Как видно, вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_τ для Х-МПП-кода с $n_0 = 31$.

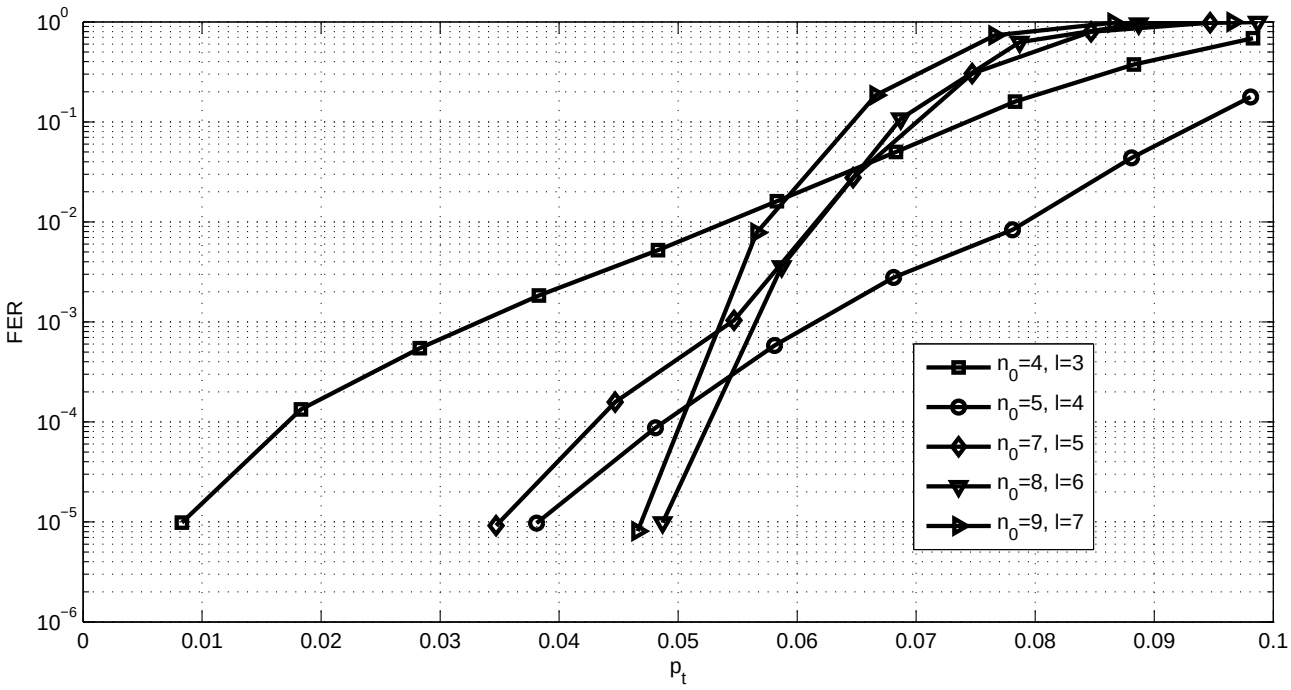

Рис. 2.10. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_M$ в зависимости от входной вероятности ошибки p_t для Г-МПП-кодов со скоростью $R \approx 0,25$ и различным количеством слоев ℓ

На рис. 2.15 представлены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Х-МПП-кода со скоростью $R \approx 0,5$ и различной длиной кода-компонента n_0 при различных значениях входной вероятности p_t. Вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_t для Х-МПП-кода с $n_0 = 127$.

На рис. 2.16 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Х-МПП-кода со скоростью $R \approx 0,75$ и различной длиной кода-компонента n_0 при различных значениях входной вероятности p_t. Видно, что в этом случае вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_t для Х-МПП-кода с $n_0 = 127$.

Теперь для каждой из рассмотренных скоростей кода $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$ выберем те параметры Х-МПП-кода, при которых вероятность отказа от декодирования равная 10^{-5} достигалась при наибольших значения входной вероят-

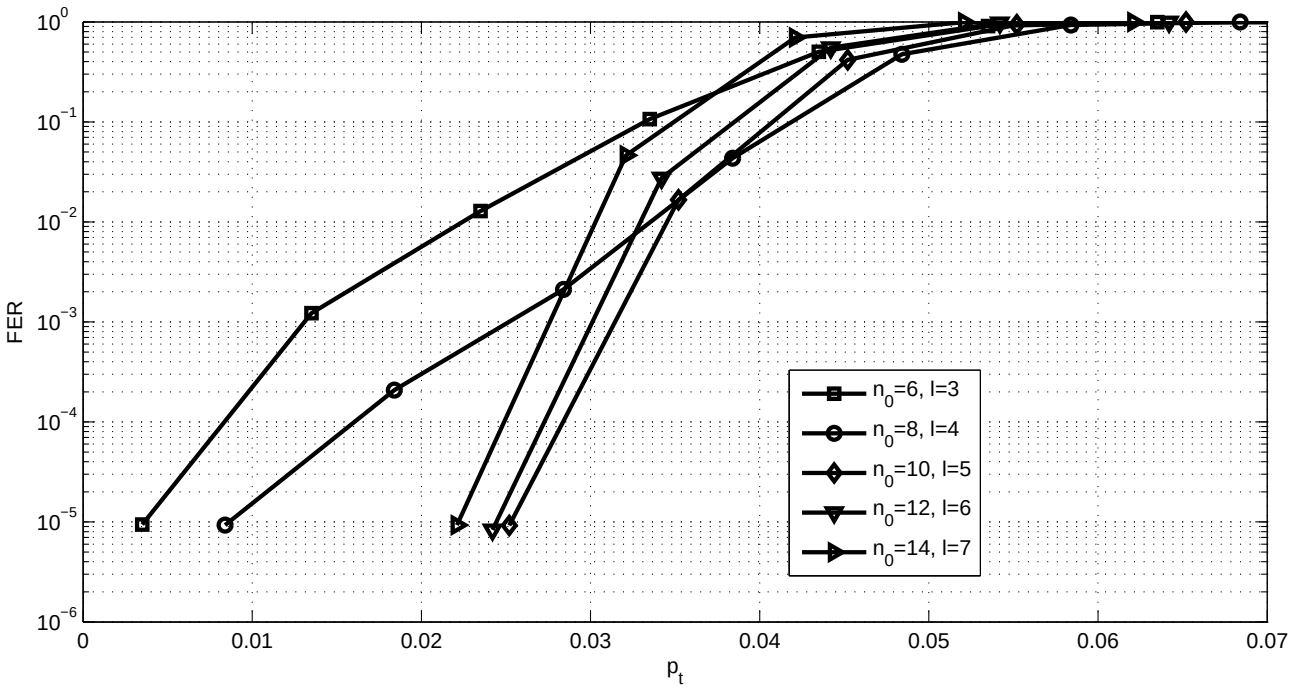

Рис. 2.11. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_M$ в зависимости от входной вероятности ошибки p_t для Г-МПП-кодов со скоростью $R \approx 0,5$ и различным количеством слоев ℓ

ности p_t. На рис. 2.17 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Х-МПП-кода с выбранными параметрами в зависимости от входной вероятности ошибки p_t.

Сравнение результатов моделирования декодирования Г-МПП-кода и Х-МПП-кода

Сравним результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Г-МПП-кода и Х-МПП-кода при передаче по ДСК с входной вероятностью ошибки p_t. Для каждой скорости $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$ выбирем такие параметры Г-МПП-кода и Х-МПП-кода, что вероятность отказа от декодирования равная 10^{-5} достигалась при наибольшем значении входной вероятности p_t. На рис. 2.18 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_M$ Г-МПП-кодов и Х-МПП-кода с выбранными параметрами в зависимости от входной вероятности ошибки p_t

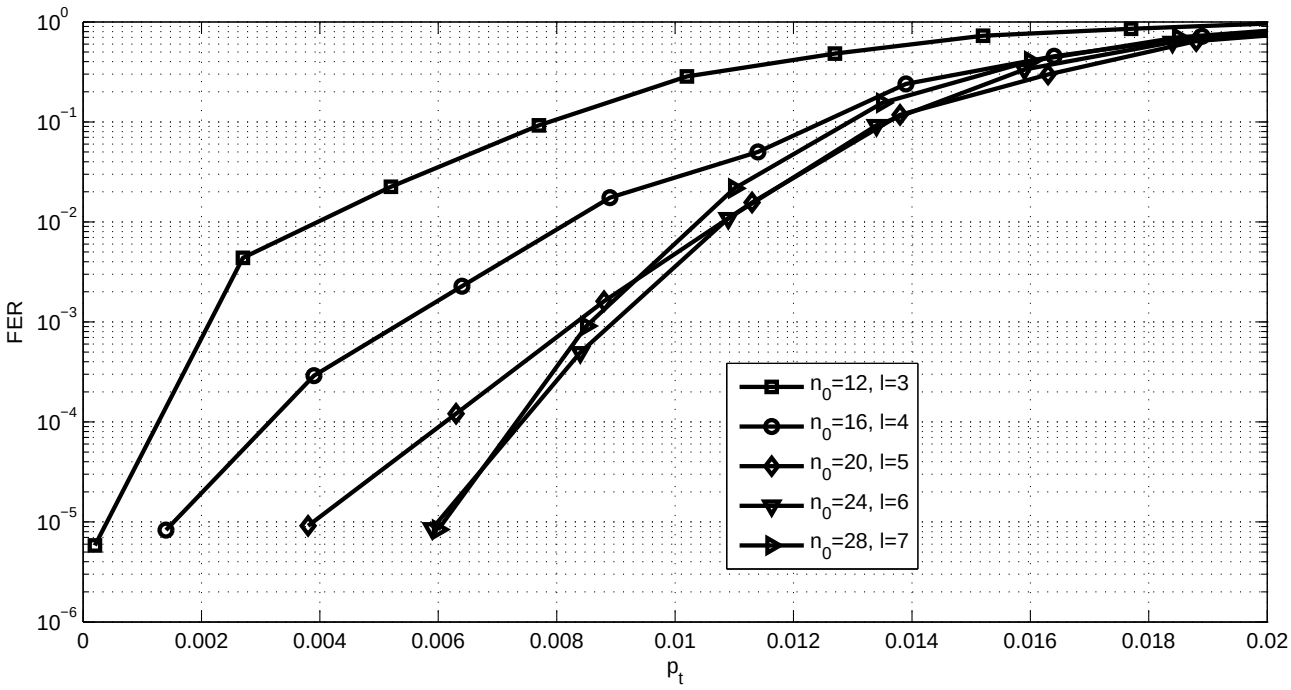

Рис. 2.12. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_M$ в зависимости от входной вероятности ошибки p_t для Г-МПП-кодов со скоростью $R \approx 0,75$ и различным количеством слоев ℓ

Как видно из рис. 2.18 для всех рассматриваемых скоростей вероятность отказа 10^{-5} при декодировании Г-МПП-кода достигается при больших значениях входной вероятности ошибки p_t, чем при декодировании Х-МПП-кодов, т.е. в этом смысле Г-МПП-код имеет лучшие корректирующие свойства, чем Х-МПП-код. Следует отметить, что полученная в § 2.2 оценка доли гарантированно исправимых ошибок для Г-МПП-кода также превосходит аналогичную оценку для Х-МПП-кода. Но доля гарантированно исправимых стираний определяет такую кратность ошибок, при которой вероятность отказа от декодирования равна нулю, а полученные результаты имитационного моделирования имеют некоторуб ненулевую вероятность отказа. При этом входные вероятности p_t, при которых достигается вероятность отказа от декодирования 10^{-5}, значительно превосходят результаты полученной нижней оценки доли ω_t гарантированно исправимых ошибок.

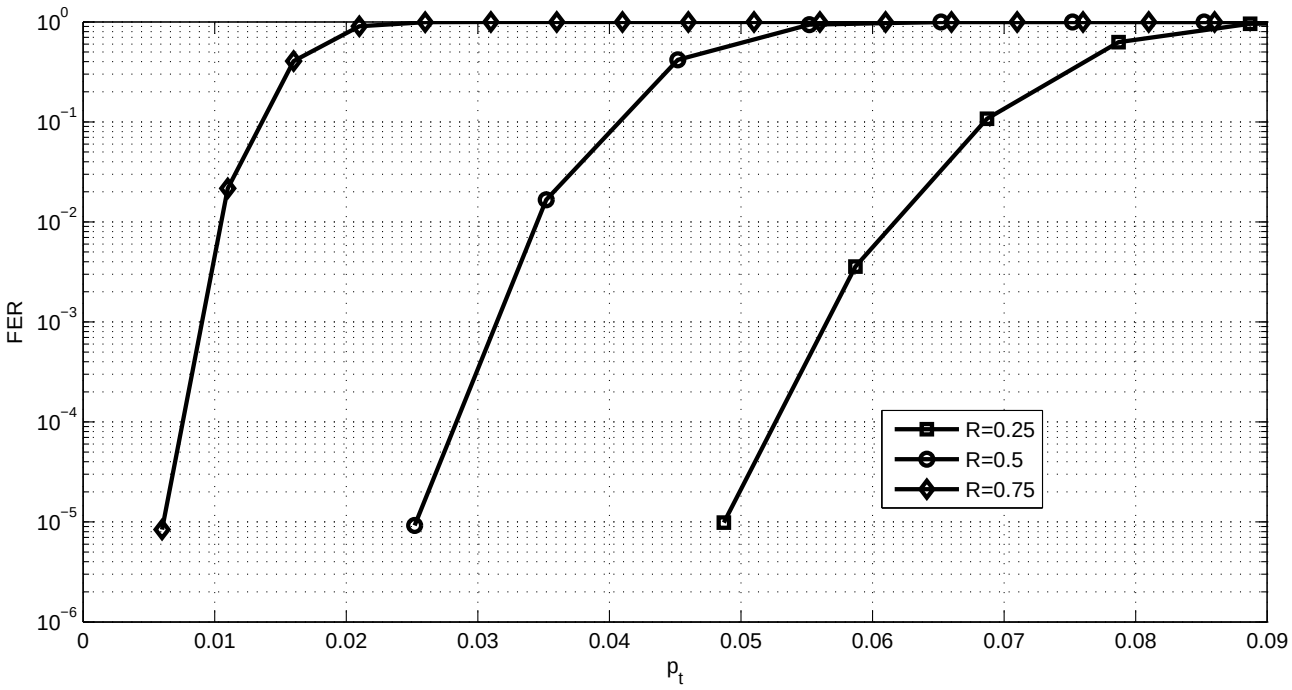

Рис. 2.13. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_M$ в зависимости от входной вероятности стираний p_t для Г-МПП-кодов с различной скоростью R

2.3.2. Алгоритм декодирования с введением стираний

Описание алгоритма декодирования

При сравнении как теоретических результатов § 1.3 и § 2.2, так и результатов имитационного моделирования § 1.4 и § 2.3, видно, что двоичный МПП-код исправляет (гарантированно или с некоторой вероятностью отказа) комбинации стираний гораздо большей кратности, чем комбинации ошибок, при декодировании с малой сложностью $\mathcal{O}(n \log n)$. Таким образом, если, используя структуру МПП-кода, покрыть ошибочные символы стираниями, то можно значительно улучшить корректирующие свойства МПП-кода в ДСК.

В результате развития данной идеи был разработан 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,

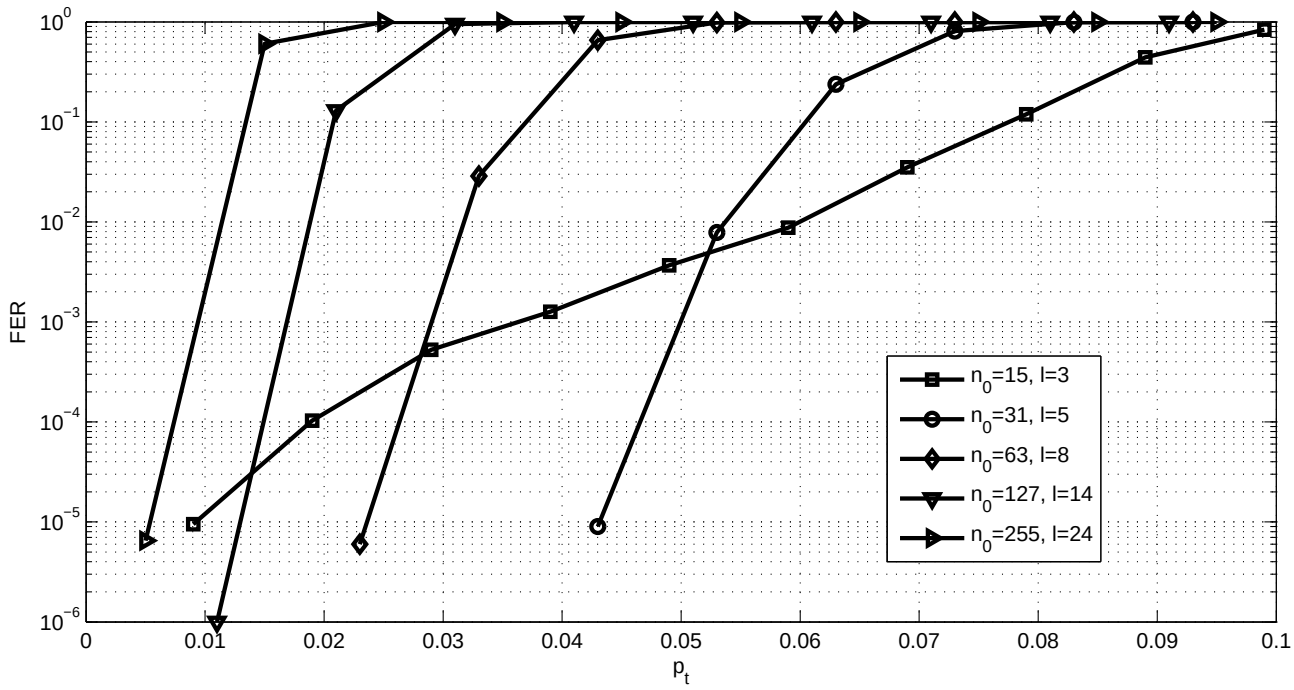

Рис. 2.14. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_M$ в зависимости от входной вероятности ошибки p_t для Х-МПП-кодов со скоростью $R \approx 0,25$ и различной длиной кода-компонента n_0

если они не были исправлены, устанавливаются изначальные (принятые) значения.

Сформулируем алгоритм декодирования с введением стираний $\mathscr{A}_*$, 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) Находим множество символов декодируемой последовательности $\mathbf{r}^{(i)}$, каждый из которых входит в наибольшее количество невыполненных проверок кодов-компонентов;

(3) Устанавливаем стирание на позиции символов, найденных на предыдущем шаге, при этом сохранив значение символа;

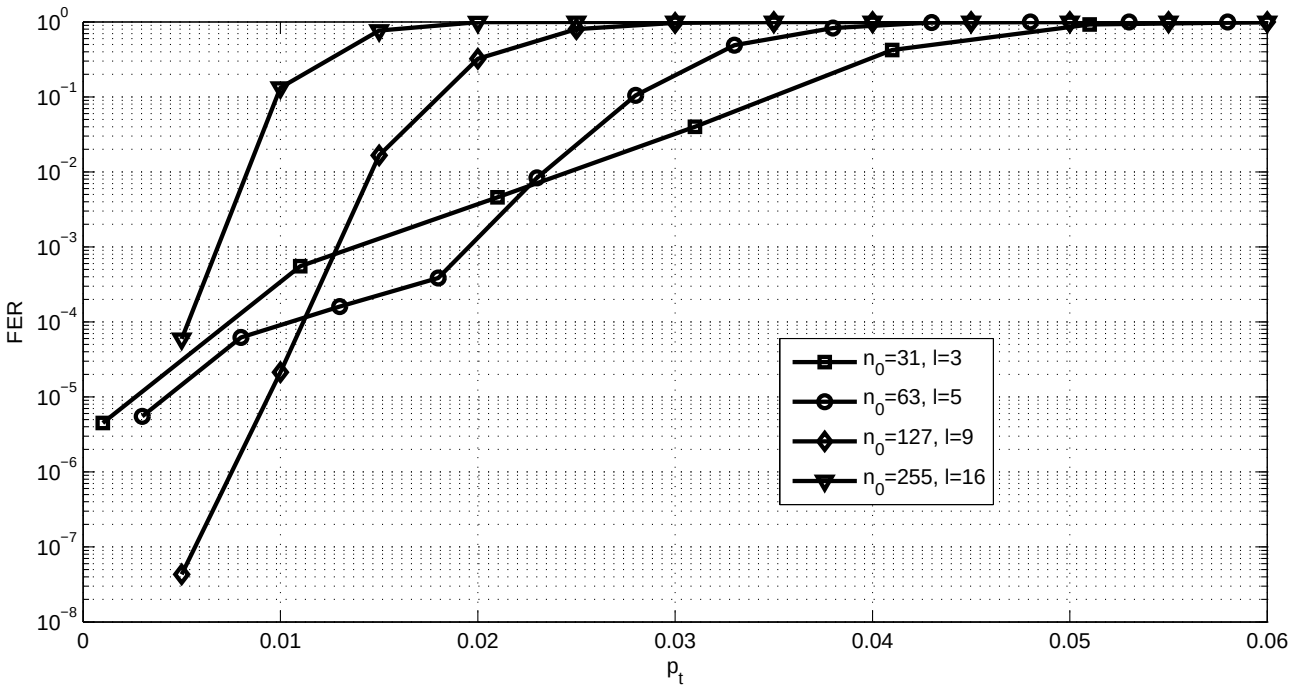

Рис. 2.15. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_M$ в зависимости от входной вероятности ошибки p_t для Х-МПП-кодов со скоростью $R \approx 0,5$ и различной длиной кода-компонента n_0

(4) Последовательно рассматриваем стирания последовательности, полученной на предыдущем шаге:

- если стирание входит хотя бы в одну проверку кода-компонента, содержащего исправимую комбинацию стираний, то для данного символа составляется список решений каждой проверки кода-компонента с исправимой комбинацией стираний и мажоритарным принципом выбирается решение для данного стирания (решение сохраняется, стирание помечается как исправленное);
- если для данного стирания нет ни одного кода-компонента с исправимой комбинацией стираний, то переходим к следующему стиранию;
- если все стирания рассмотрены, то переходим к следующему шагу;

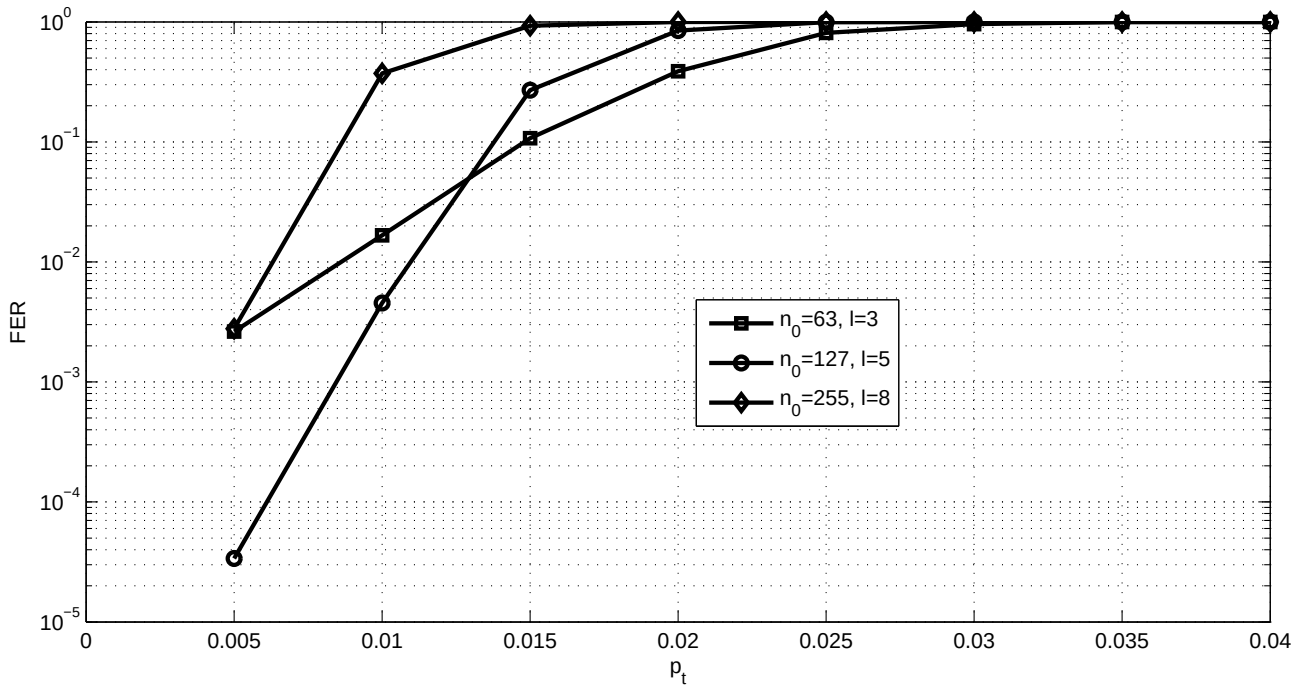

Рис. 2.16. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_M$ в зависимости от входной вероятности ошибки p_t для Х-МПП-кодов со скоростью $R \approx 0,75$ и различной длиной кода-компонента n_0

(5) Все исправленные на предыдущем шаге стирания замеяются полученными решениями, а неисправленные заменяются сохраненными изначальными значениями;

(3) Рассматриваем обновленную последовательность $\mathbf{r}^{(i)}$, полученную на предыдущем шаге:

- если синдром МПП-кода 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

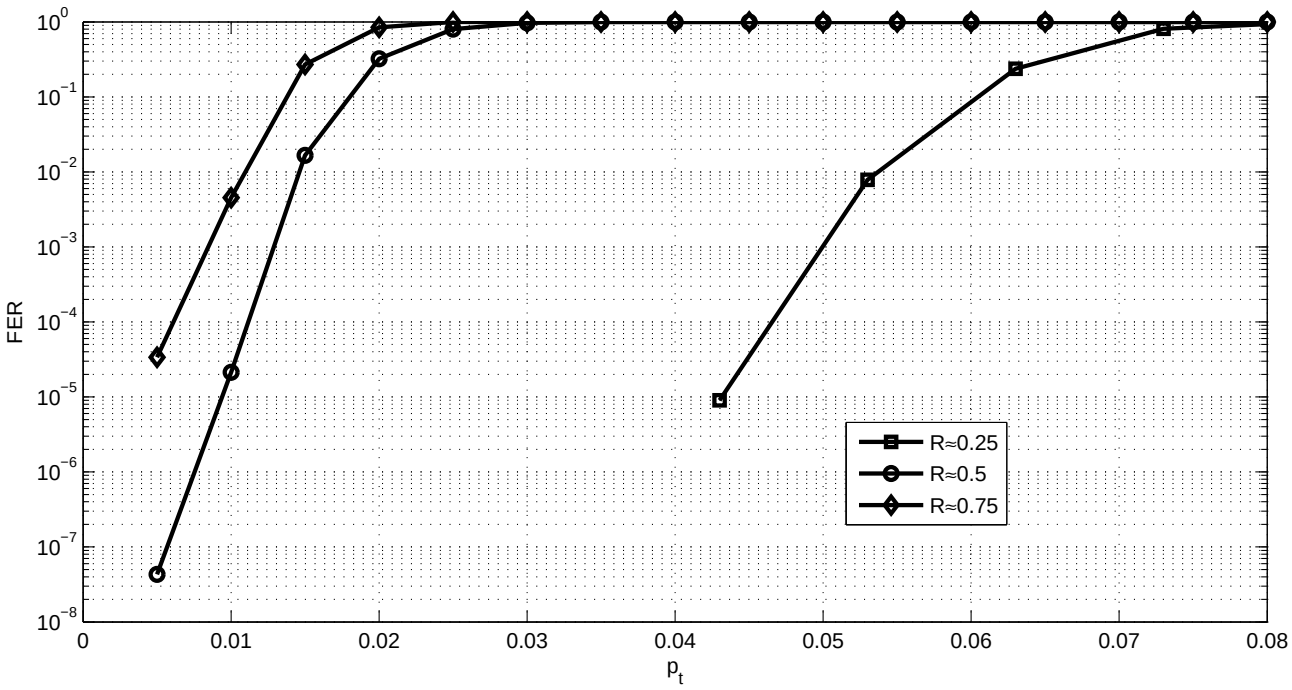

Рис. 2.17. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_M$ в зависимости от входной вероятности ошибки p_t для Х-МПП-кодов с различной скоростью R

последовательностью $\mathbf{r}^{(i)}$;

– иначе алгоритм возвращает обноленную последовательность $\mathbf{r}^{(i)}$, устанавливает флаг отказа от декодирования и завершает выполнение.

Анализ результатов моделирования алгоритма декодирования

Рассмотрим результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_*$ Г-МПП-кода при передаче по ДСК с входной вероятностью ошибки p_t. Результаты были получены для заданных заданных значений скоростей кода $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$, количества слоев $\ell = 3, 4, ..., 7$ и соответствующих значений длин кода-компонента n_0.

На рис. 2.19 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_*$ Г-МПП-кода со скоростью $R \approx 0,25$ с различным количеством слоев ℓ при различных значениях входной вероятности p_t. Как

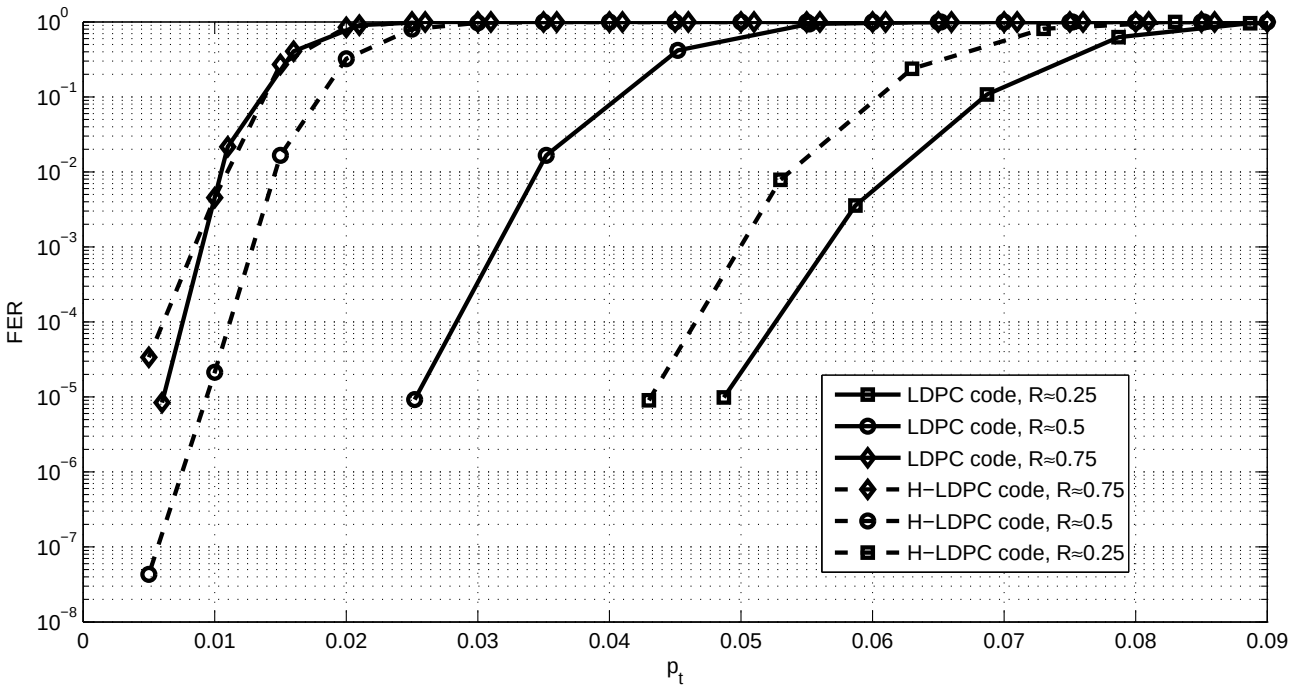

Рис. 2.18. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_M$ в зависимости от входной вероятности стираний p_t для Г-МПП-кодов и Х-МПП-кодов с различной скоростью R

видно, вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_t для Г-МПП-кода с $\ell = 5$.

На рис. 2.20 представлены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_*$ Г-МПП-кода со скоростью $R \approx 0,5$ с различным количеством слоев ℓ при различных значениях входной вероятности p_t. В данном случае вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_t для Г-МПП-кода с $\ell = 5$.

На рис. 2.21 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_*$ Г-МПП-кода со скоростью $R \approx 0,75$ с различным количеством слоев ℓ при различных значениях входной вероятности p_t. Видно, что в этом случае вероятность отказа от декодирования равная 10^{-5} достигается на наибольшей входной вероятности p_t для Г-МПП-кода с $\ell = 6$.

Теперь для каждой из рассмотренных скоростей $R \approx \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$ выбирем те параметры Г-МПП-кода, при которых вероятность отказа от декодирования

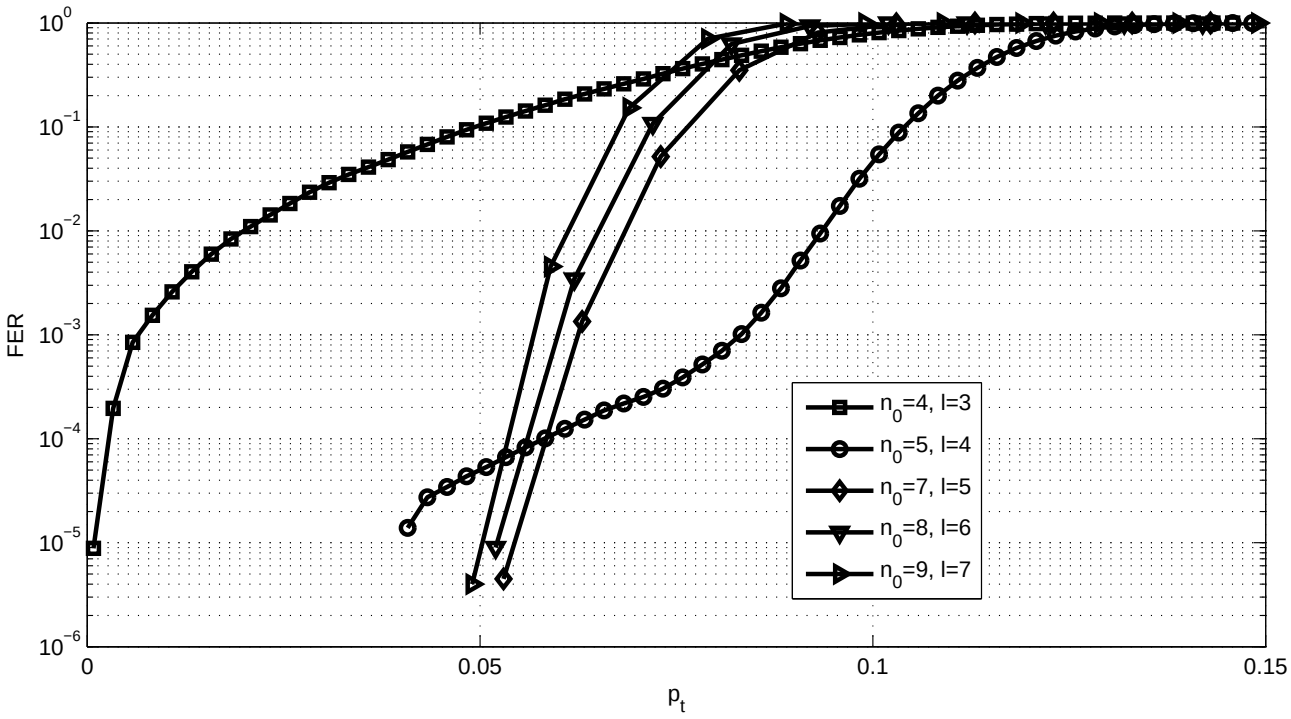

Рис. 2.19. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_*$ в зависимости от входной вероятности ошибки p_t для Г-МПП-кодов со скоростью $R \approx 0,25$ и различным количеством слоев ℓ

равная 10^{-5} достигалась при наибольших значения входной вероятности p_t. На рис. 2.22 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_*$ Г-МПП-кода с выбранными параметрами в зависимости от входной вероятности ошибки p_t.

2.3.3. Сранение алгоритмов декодирования

Сравним теперь лучшие результаты имитационного моделирования алгоритмов декодирования $\mathscr{A}_M$ и $\mathscr{A}_*$ Г-МПП-кода с различными скоростями. На рис. 2.23 приведены лучшие результаты имитационного моделирования алгоритмов декодирования $\mathscr{A}_M$ и $\mathscr{A}_*$ Г-МПП-кода с различной скоростью. Как видно из рис. 2.23 для всех рассматриваемых скоростей Г-МПП-кода вероятность отказа 10^{-5} при декодировании по алгоритму $\mathscr{A}_*$ достигается при больших значениях входной вероятности стирания p_t, чем при декодировании

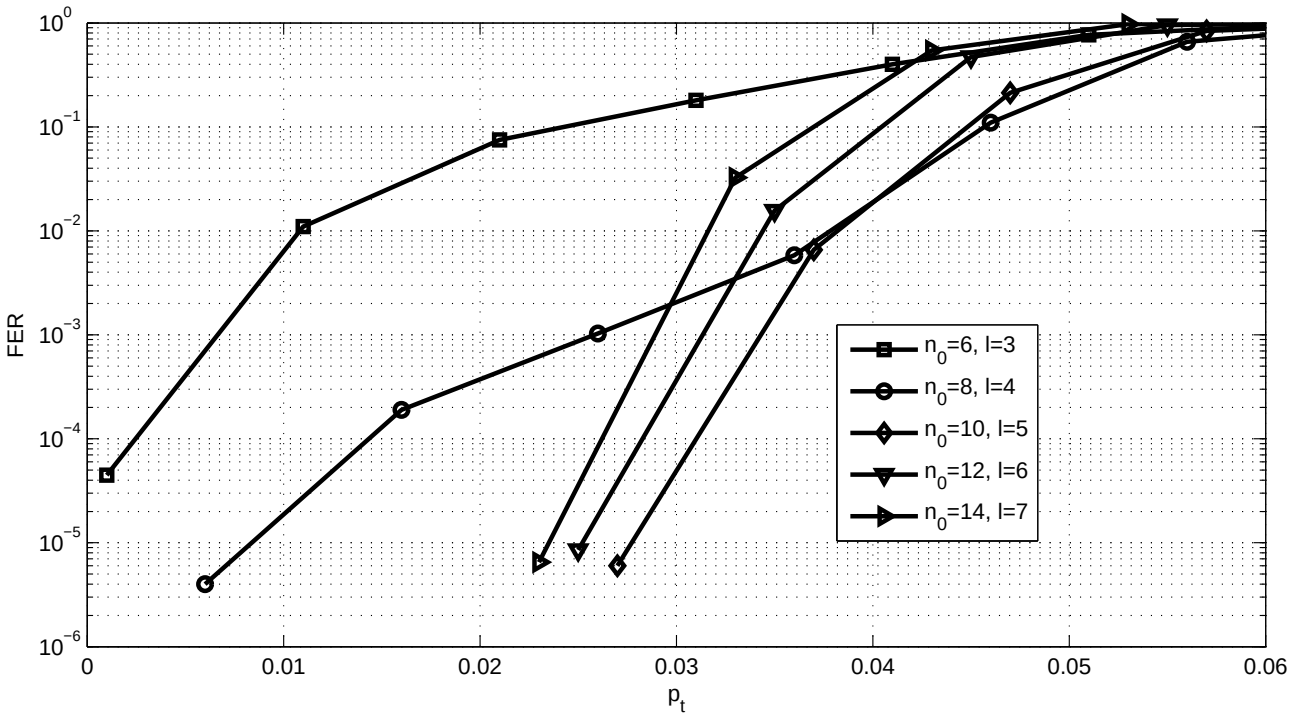

Рис. 2.20. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_*$ в зависимости от входной вероятности ошибки p_t для Г-МПП-кодов со скоростью $R \approx 0,5$ и различным количеством слоев ℓ

по алгоритму $\mathscr{A}_M$, т.е. в этом смысле алгоритм декодирования $\mathscr{A}_*$ имеет лучшие корректирующие свойства, чем $\mathscr{A}_M$. Так же можно заметить, что при увеличении скорости разница между результатами алгоритмов декодирования $\mathscr{A}_*$ и $\mathscr{A}_M$ уменьшается.

2.4. Выводы к главе

- Получена новая оценка доли гарантированно исправимых ошибок, при декодировании МПП-кода по алгоритму $\mathscr{A}_M$ 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 $\mathcal{O}\left(n \log n\right)$.
- Предложен новый алгоритм декодирования с введением стираний $\mathscr{A}_*$.

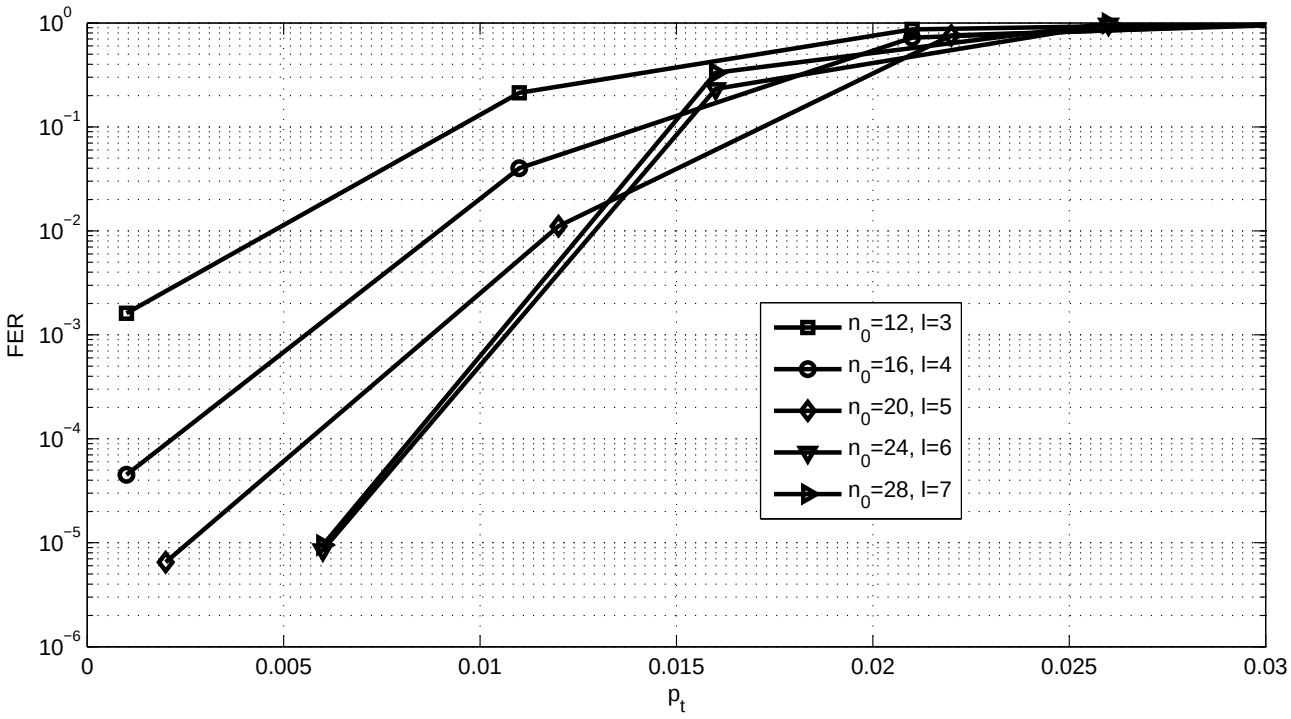

Рис. 2.21. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_*$ в зависимости от входной вероятности ошибки p_t для Г-МПП-кодов со скоростью $R \approx 0,75$ и различным количеством слоев ℓ

- Показано с помошью имитационного моделирования, что предложенный алгорит декодирования $\mathscr{A}_*$ имеет лучшие корректирующие свойства, чем алгоритм декодирования $\mathscr{A}_M$.

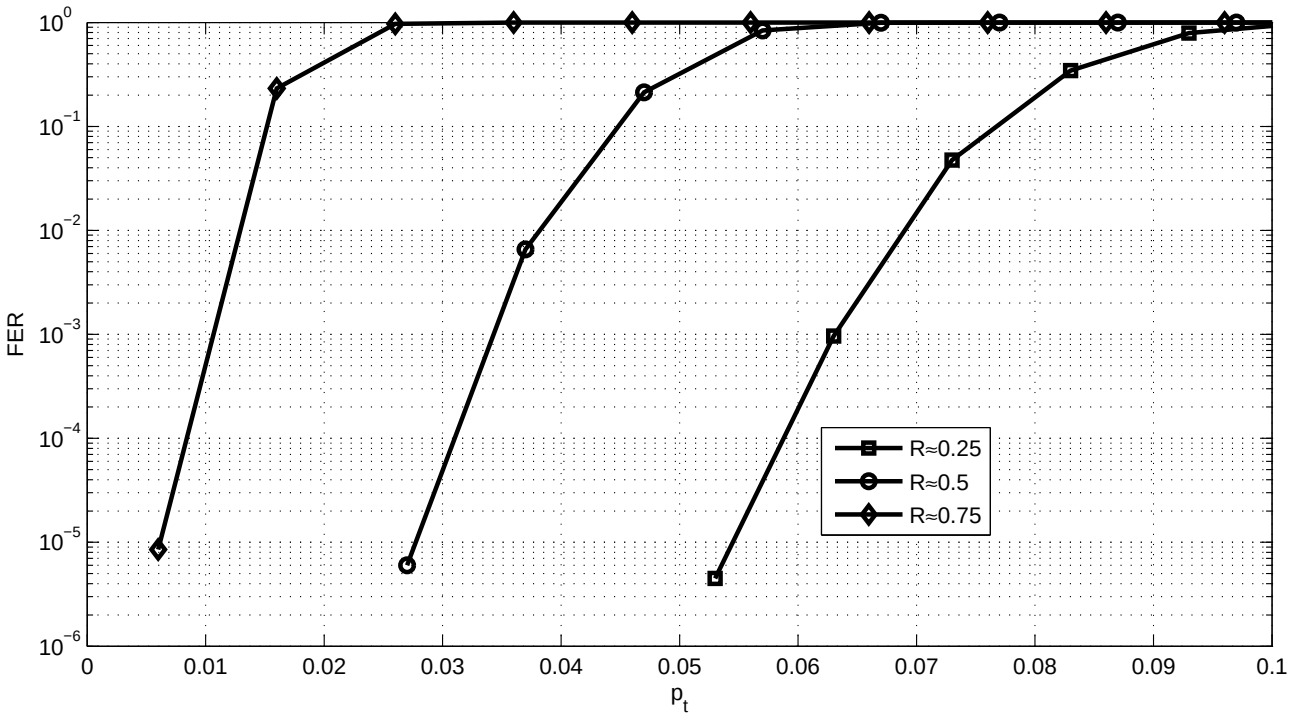

Рис. 2.22. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_*$ в зависимости от входной вероятности стираний p_t для Г-МПП-кодов с различной скоростью R

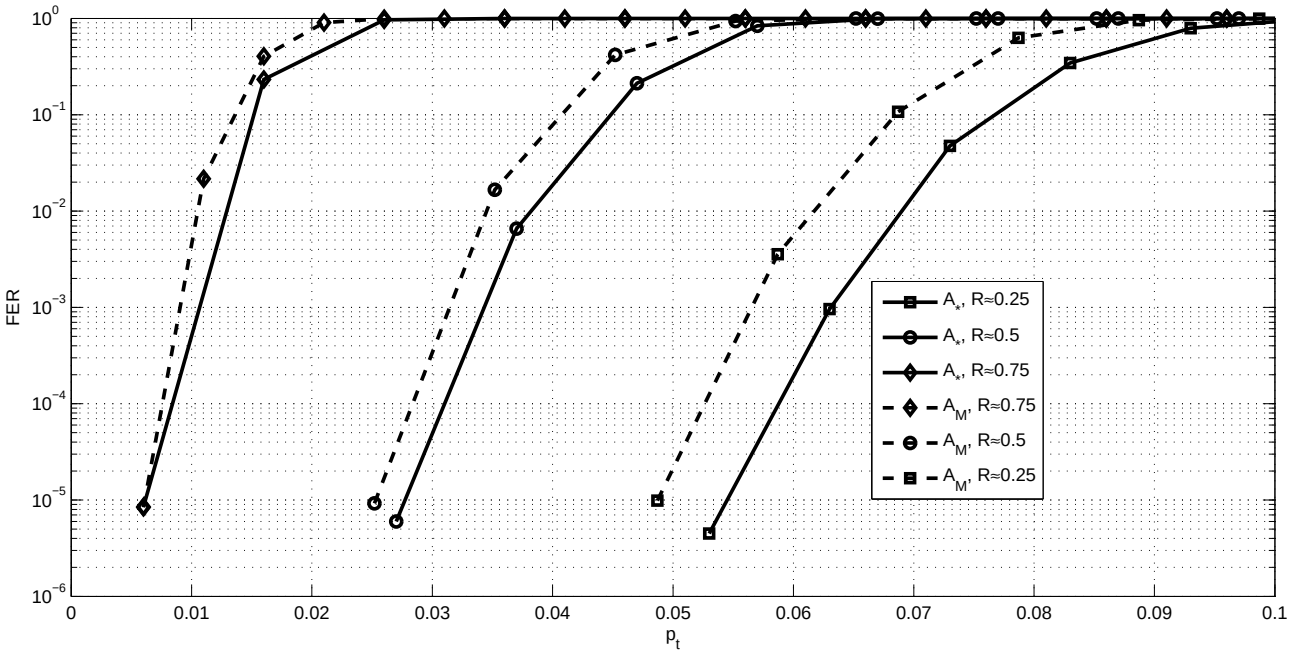

Рис. 2.23. Графики вероятности отказа от декодирования по алгоритмам $\mathscr{A}_M$ и $\mathscr{A}_*$ в зависимости от входной вероятности стираний p_t для Г-МПП-кодов с различной скоростью R

Глава 3

Построение МПП-кода со специальной контрукцией

3.1. Введение

В третьей главе предложена специальная конструкция МПП-кода и алгоритм его декодирования. Для ДСК без памяти исследуются реализуемые корректирующие свойства предложенного МПП-кода и алгоритма декодирования. Получена нижняя оценка экспоненты вероятности ошибочного декодирования предложенного МПП-кода при декодирования по предложенному алгоритму со сложностью $\mathcal{O}(n \log n)$. Также рассматриваемый алгоритм декодирования исследуется методом имитационного моделирования.

3.2. Структура МПП-кода со специальной конструкцией

Рассмотрим построение проверочной матрицы $\mathbf{H}$ МПП-кода со специальной конструкцией. 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 $\mathbf{H}_1$:

$$\mathbf{H}_{b_1} = \left(\underbrace{\begin{array}{cccc} \mathbf{H}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_1 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_1 \end{array}}_{b_1} \right),$$

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

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

где $\pi\left(\mathbf{H}_{b_1}\right)$, 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 $\mathscr{E}_G\left(n_0, \ell, b_0\right)$ и случайную перестановку π, определим ансамбль $\mathscr{E}_L\left(n_0, \ell, b_0, n_1, 1, b_1\right)$ СЛ-Г-МПП-кодов.

3.3. Асимптотическая оценка экспоненты вероятности ошибочного декодирования

Нижняя оценка эксопненты вероятности ошибочного декодирования по максимуму правдоподобия лучших линейных кодов была получена в работе [2]. В работах [34] и [24] были получены верхняя и нижняя оценки экспоненты вероятности ошибочного декодирования Г-МПП-кода по максимуму правдоподобия, сложность которого составляет $\mathcal{O}(2^n)$. В работе [24] показано, что нижняя оценка экспоненты вероятности ошибочного декодирования Г-МПП-кода с фиксированной скоростью R по максимуму правдоподобия при $\ell \to \infty$ достигает нижнюю оценку экспоненты вероятности ошибочного декодирования лучших линейных кодов по максимуму правдоподобия, полученную в работе [2].

В данном параграфе рассматривается ансамбль СЛ-Г-МПП-кодов. Предложен алгоритм декодирования этих кодов с малой сложностью. Впервые показано, что при передаче по ДСК без памяти в ансамбле СЛ-Г-МПП-кодов существуют коды, при декодировании которых по предложенному алгоритму со сложностью $\mathcal{O}(n \log_2 n)$ вероятность ошибочного декодирования убывает экспоненциально для всех скоростей меньше пропускной способности канала.

3.3.1. Описание алгоритма 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 $\mathbf{H}_2$ Г-МПП-кода.

Рассмотрим алгоритм декодирования $\mathscr{A}_C$, состоящий из следующих двух шагов:

- последовательно декодируем по максимуму правдоподобия каждый из b_1 линейных блоковых кодов $\mathbf{H}_1$ из $\ell+1$ слоя проверочной матрицы $\mathbf{H}$;

- затем полученную на предыдущем шаге последовательность декодируем по мажоритарному алгоритму $\mathscr{A}_M$, используя проверочную матрицу Г-МПП-кода $\mathbf{H_2}$.

Стоит отметить, что алгоритм $\mathscr{A}_C$ не яляется интеративным, т. е. каждую принятую последовательность декодируем только один раз сначала по максимуму прадоподобия, используя линейный коды $\mathbf{H}_1$, затем полученную последовательность декодируем по мажоритарному алгоритму, используя Г-МПП-код $\mathbf{H}_2$.

З а м е ч а н и е 3.1. Аналогичный алгоритм декодирования для каскадной конструкции с вутренними линейными кодами и внешним Г-МПП-кодом рассматривался в [1], где была получена нижняя оценка экспоненты ошибочного декодирования каскадной конструкции и показано, что для всех скоростей меньше пропускной спсобности канала существует каскадный код с вероятностью ошибки, убывающей экспоненциально. Но для МПП-кода данный алгоритм предлагается впервые.

3.3.2. Формулировка основного результата

При рассмотрении вероятности ошибочного декодирования P ограничемся только случаем ДСК без памяти с вероятностью ошибки при передаче каждого символа p_t.

Оценку вероятности будем представлять ввиде:

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

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

В самом общем виде оценка на $E_0\left(R_1, p_t\right)$ для лучших линейных кодов была получена Р. Г. Галлагером [2], откуда следует, что существуют коды, для которых $E_0\left(R_1, p_t\right) > 0$ для $R_1 < \mathscr{C}$, где $\mathscr{C}$ – пропускная способность ДСК без памяти с вероятностью ошибки p_t [21]. В § 2.2 было доказано, что в ансамбле $\mathscr{E}_G\left(n_0, \ell, b_0\right)$ Г-МПП-кодов существует Г-МПП-код, который исправляет любую комбинацию ошибок кратности до $\lfloor \omega_t n \rfloor$ при декодировании по мажоритарному алгоритму $\mathscr{A}_M$. Учитывая два этих факта, сформулируем следующую теорему:

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:

$$E\left(R_1, n_1, \omega_t, p_t\right) = \min_{\omega_t \leq \beta \leq \beta_0} \left\{ \beta E_0\left(R_1, p_t\right) + E_2\left(\beta, \omega_t, p_t\right) - \frac{1}{n_1} H\left(\beta\right) \right\}, \quad (3.1)$$

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

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

при этом n_1 *удовлетворяет следующим условиям:*

$$\frac{-\ln\beta_0}{E_0(R_1, p_t)} \leq n_1 \leq \frac{1}{R_1}\log_2\log_2(n). \tag{3.2}$$

Тогда из (3.1) следует, что если $R \to \mathscr{C}$ так, что $R_1 < \mathscr{C}$ и $R_2 < 1$, то можно подобрать такое n_1, удовлетворяющее условию (3.2), что $E(R_1, n_1, \omega_t, p_t) > 0$, если $\omega_t > 0$ для $\forall R_2 < 1$.

3.3.3. Доказательство основного результата

Доказательство состоит из двух частей. В первой части доказано, что если выполняется левое неравенство условия (3.2), то в ансамбле СЛ-Г-МПП-кодов существует код, экспонента вероятности ошибочного декодирования по алгоритму $\mathscr{A}_C$ которого ограничена снизу (3.1), при передаче по ДСК без памяти.

Затем во второй части показано, что при выполнении правого неравенства условия (3.2) сложность алгоритма декодирования $\mathscr{A}_C$ составляет порядка $\mathcal{O}(n\log n)$.

Существование СЛ-Г-МПП-кода с заданными свойствами

Л е м м а 3.1. *Если в ансамбле* $\mathscr{E}_G(n_0, \ell, b_0)$ *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* $\mathscr{A}_M$*, а 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 $\mathscr{E}_L(n_0, \ell, b_0, n_1, 1, b_1)$ *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 *вероятность ошибочного декодирования ограничена сверху:*

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

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 2.1, доказанной в § 2.2, Г-МПП-код 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:

$$P = \sum_{i=\lfloor \omega_t b_1 \rfloor}^{b_1} \left(\begin{array}{c} b_1 \\ i \end{array} \right) P_2 \left(W \geq W_0 | i \right) P_1^i \left(n_1, R_1, p \right) \left(1 - P_1 \left(n_1, R_1, p \right) \right)^{b_1 - i}, \quad (3.3)$$

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

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

а $P_2 \left(W \geq W_0 | i \right)$ – 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 $P_2 \left(W \geq W_0 | i \right)$ можно записать следующим образом:

$$P_2 \left(W \geq W_0 | i \right) = \sum_{j=\left\lfloor \frac{\omega_t n}{2} \right\rfloor}^{i n_1} \left(\begin{array}{c} i n_1 \\ j \end{array} \right) p^j (1-p)^{i n_1 - j}.$$

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

$$E_2\left(\beta, \omega_t, p\right) = \begin{cases} \frac{1}{2}\left(\omega_t \ln \frac{\omega_t}{p} + \left(2\beta - \omega_t\right) \ln \frac{2\beta - \omega_t}{1-p}\right) - \beta \ln 2\beta, \ \beta < \beta_0 \\ 0, \ \beta \geq \beta_0 \end{cases}, \quad (3.4)$$

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 (3.4) сумму (3.3) можно записать следующим образом:

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

Рассмотрим каждую сумму отдельно:

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

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

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:

$$P_1\left(n_1, R_1, p\right) \leq \beta_0 \Rightarrow n_1 \geq \frac{-\ln \beta_0}{E_0\left(R_1, p\right)}. \tag{3.5}$$

Теперь оценим сумму P':

$$P' \leq \left\lceil \left(\beta_0 - \omega_t\right) b_1 \right\rceil \max_{\omega_t \leq \beta \leq \beta_0} \left\{ \left(\begin{array}{c} b_1 \\ \beta b_1 \end{array} \right) P_2\left(W \geq W_0 | \beta b_1\right) P_1^{\beta b_1} \left(1 - P_1\right)^{(1-\beta) b_1} \right\}.$$

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

$$E'\left(R_1, n_1, \omega_t, p\right) = \min_{\omega_t \leq \beta \leq \beta_0} \left\{ E_2\left(\beta, \omega_t, p\right) + \beta E_0\left(R_1, p\right) - \frac{1}{n_1} H\left(\beta\right) \right\}. \tag{3.6}$$

Заметим, что если в правой части (3.6) минимум достигается при β_0, то в соотвествии с (3.4) $E' = E''$. Следовательно, $E' \leq E''$.

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

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

где $E\left(R_1, n_1, \omega_t, p\right) = \min\left\{E'\left(R_1, n_1, \omega_t, p\right), E''\left(R_1, n_1, p\right)\right\} = E'\left(R_1, n_1, \omega_t, p\right)$, при этом n_1 удовлетворяет условию (3.5). ▲

Сложность алгоритма декодирования

Л е м м а 3.2. *Сложность алгоритма $\mathscr{A}_C$ декодирования СЛ-Г-МПП-кода длины n составляет порядка $\mathcal{O}(n \log n)$, если длина линейного кода* $n_1 \leq \frac{1}{R_1} log_2 log_2 (n)$.

Д о к а з а т е л ь с т в о. 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 § 2.2 было показано, что сложность алгоритма $\mathscr{A}_M$ декодирования Г-МПП-кода 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:

$$n_1 \leq \frac{1}{R_1} \log_2 \log_2 (n) . \tag{3.7}$$

▲

3.3.4. Анализ численных значений оценки

Рассмотрим зависимость минимально необходимой длины линейного кода n_1, при которой выполняется условие (3.5), 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 Г-МПП-кода, что $R = R_1 + R_2 - 1$. Данная зависимость приведена на рис. 3.1.

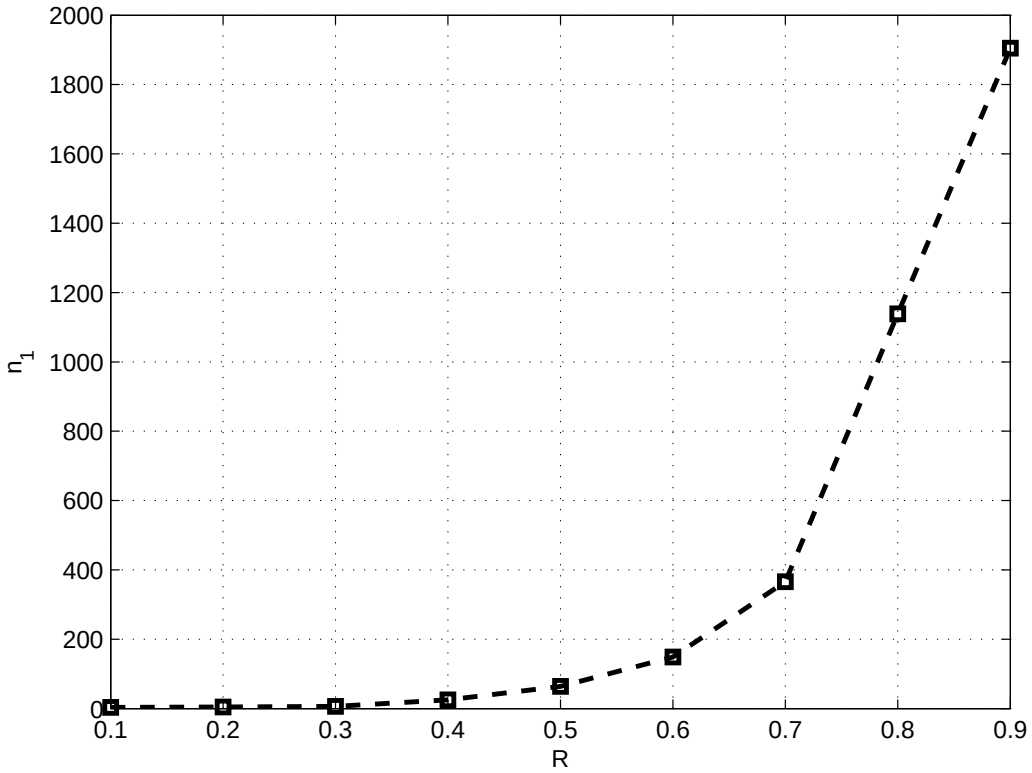

Рис. 3.1. Зависимость минимально необходимой длины n_1 при фиксированной вероятности ошибки $p = 0,001$ от скорости R СЛ-Г-МПП-кода

В соответствии с рис. 3.1 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. 3.2.

Как видно на рис. 3.2 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 Г-МПП-кода, что $R = R_1 + R_2 - 1$. Обозначим полученное значение следующим образом:

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

На рис. 3.3 представлен график зависимости $E(R, p)$ от вероятности ошибки p при фиксированной $n_1 = 2000$ и $R = 0,5$.

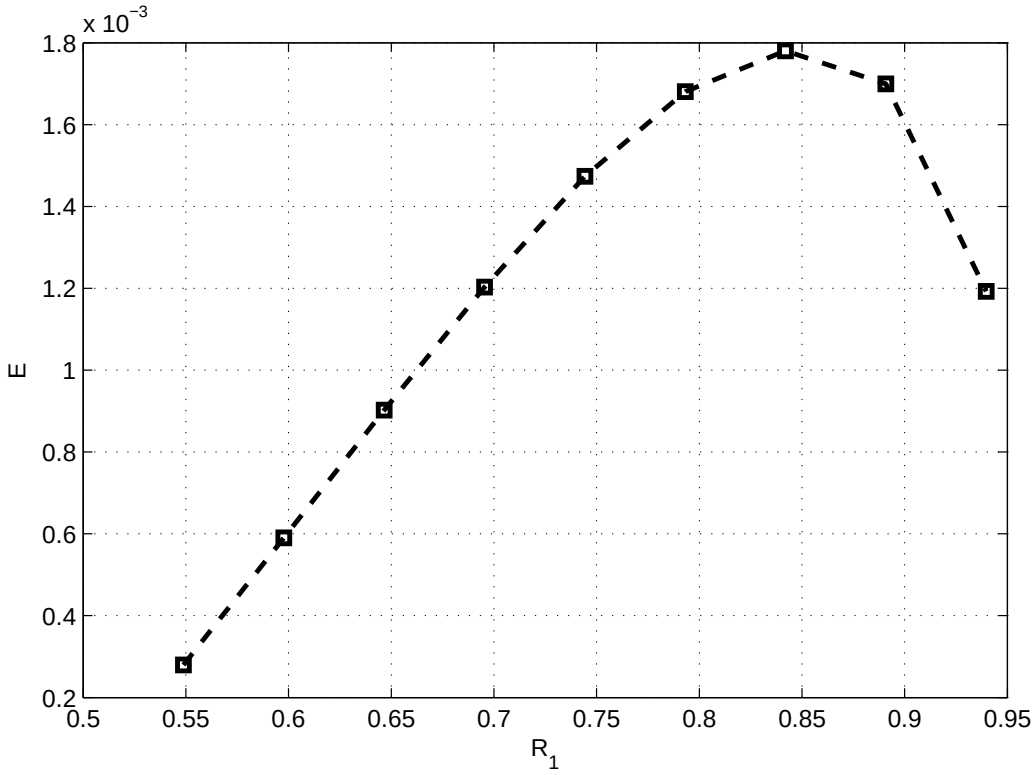

Рис. 3.2. Зависимость $E(R_1, n_1, \omega_t, p)$ от скорости R_1 при фиксированной скорости $R = 0,5$, длине линейного кода $n_1 = 2000$ и вероятности ошибки на бит $p = 0,001$

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. 3.4).

Теперь найдем зависимость $E(R, p)$ от скорости R СЛ-Г-МПП-кода при заданных $n_1 = 2000$ и $p = 0,001$ (см. рис. 3.5).

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. 3.6)

Как видно из рис. 3.6 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 – $\mathcal{O}\left(2^{Rn}\right)$.

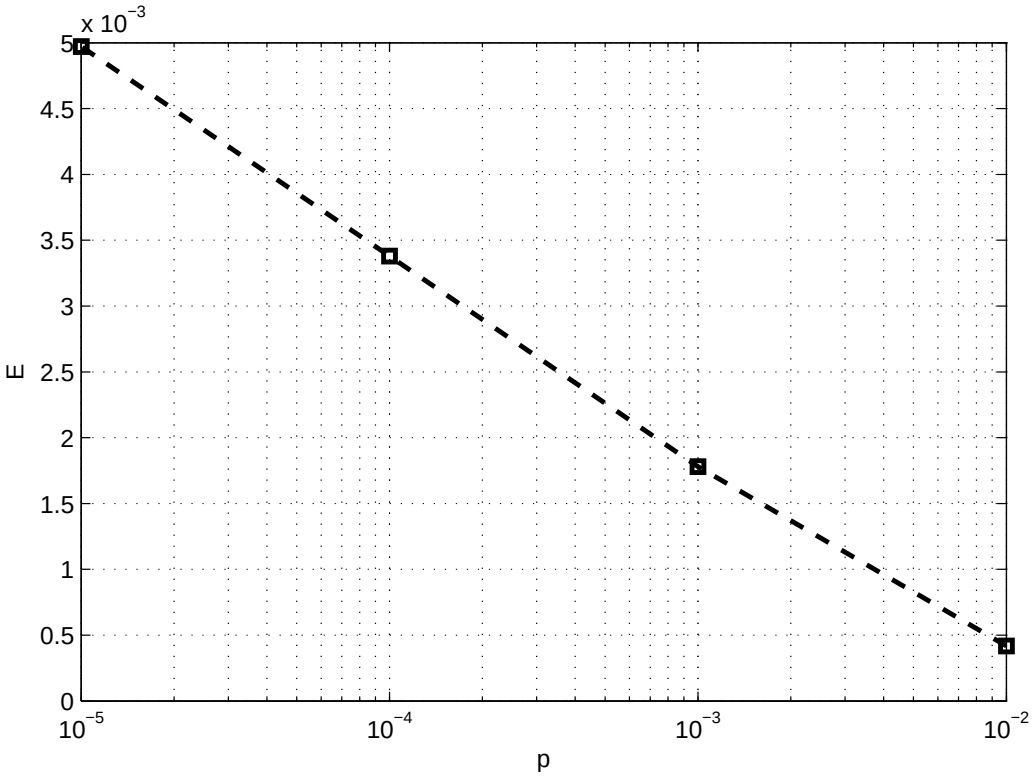

Рис. 3.3. Зависимость $E\,(R, p)$ от скорости p при фиксированной $n_1 = 2000$ и $R = 0,5$

3.4. Имитационное моделирования алгоритма декодирования МПП-кода со специальной контрукцией

В данном параграфе приведены результаты имитационного моделирования для некоторых параметров СЛ-Г-МПП-кода при декодировании по алгоритму $\mathscr{A}_C$. Рассматривались СЛ-Г-МПП-коды, в качестве линейных кодов у которых были выбраны коды БЧХ (31, 21) и (63, 39).

В качестве модели канала был выбран ДСК без памяти с вероятностью перехода в ошибку (входной вероятностью ошибки) p_t. Для каждого значения p_t испытания проводились до тех пор, пока не будет накоплено не менее 20 отказов от декодирования СЛ-Г-МПП-кода. Имитационное моделирование останавливалось, если вероятность отказа от декодирования заданного СЛ-Г-МПП-кода была меньше 10^{-5}.

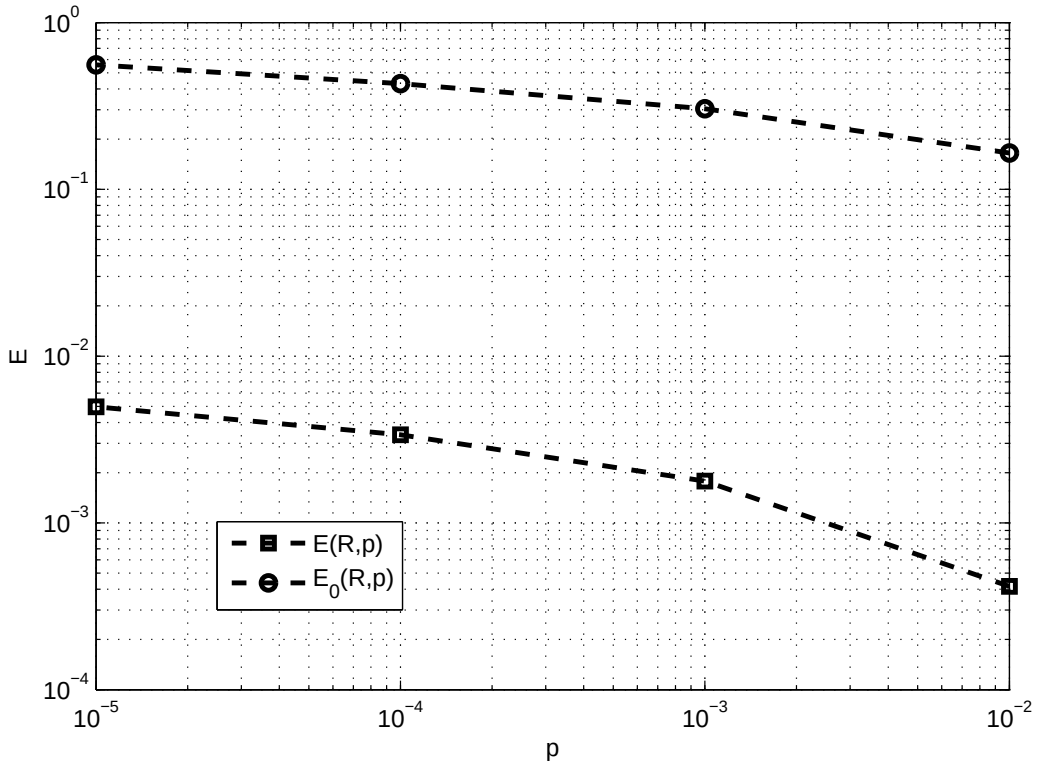

Рис. 3.4. Зависимость $E(R,p)$ при фиксированной $n_1 = 2000$ и $E_0(R,p)$ от вероятности p при скорости кода $R = 0,5$

3.4.1. Анализ результатов имитационного моделирования

Рассмотрим вероятность ошибки на бит после декодирования БЧХ кодов (31,21) и (63, 39) по максимуму правдопадобия в зависимости от входной вероятности ошибки p_t (см. рис. 3.7).

Как видно из рис. 3.7 БЧХ (63,39) имеет меньшую вероятность ошибки на бит после декодирования по максимуму правдопадобия, чем БЧХ (31,21). Стоит отметить, что в соотвествии с описанием алгоритма $\mathscr{A}_C$ полученная вероятность ошибки на бит после декодирования по максимуму правдоподобия является входной вероятностью ошибки для мажоритарного алгоритма $\mathscr{A}_M$ декодирования Г-МПП-кода с $\mathbf{H}_2$. Из рис. 3.7 следует, что декодирование кодов БЧХ (31,21) и БЧХ (63,39) по максимуму правдоподобия улучшаю канал, т.е уменьшают вероятность ошибки на бит при входной вероятности ошибки $p_t \leq 0,1$.

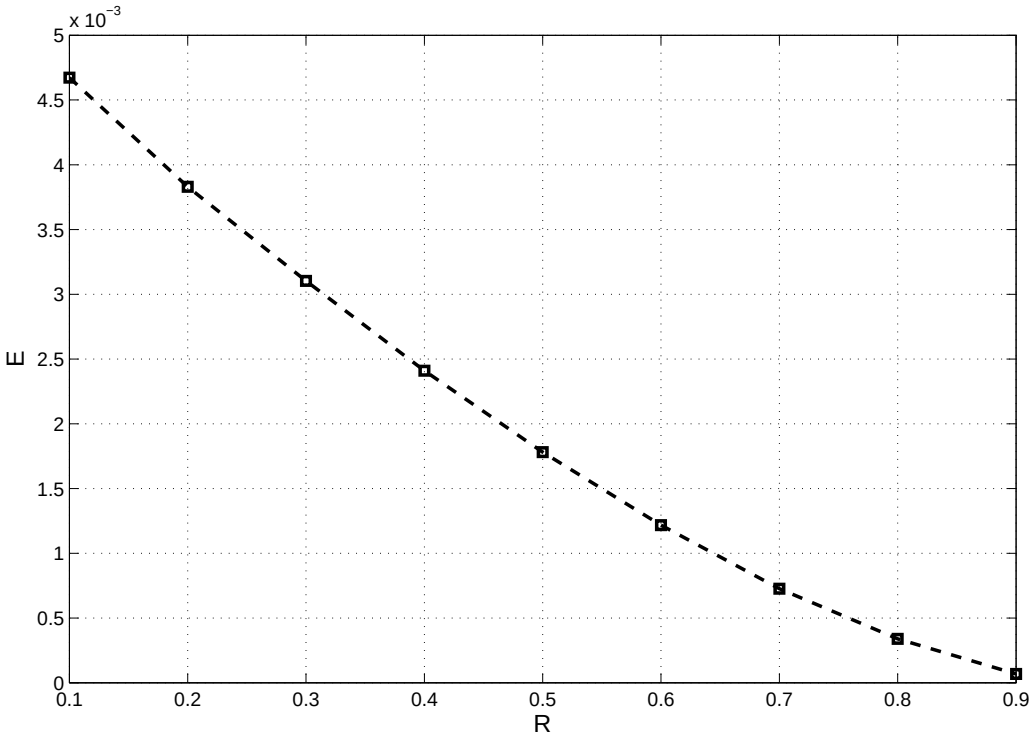

Рис. 3.5. $E\,(R, p)$ от скорости R при фиксированной $n_1 = 2000$ и $p = 0,001$

Рассмотрим результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_C$ СЛ-Г-МПП-кода с БЧХ кодом (31,21) для различных скоростей кода R и количества слоев ℓ Г-МПП-кода. На рис. 3.8 представлены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_C$ СЛ-Г-МПП-кода со скоростью $R \approx 0,25$ и с БЧХ кодом (31,21) для различного количества слоев ℓ Г-МПП-кода. Вероятность отказа от декодирования 10^{-5} достигается при наибольшей входной вероятности ошибки p_t для СЛ-Г-МПП-кода с Г-МПП-кодом с $\ell = 5$.

На рис. 3.9 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_C$ СЛ-Г-МПП-кода со скоростью $R \approx 0,5$ и с БЧХ кодом (31,21) для различного количества слоев ℓ Г-МПП-кода. Вероятность отказа от декодирования 10^{-5} достигается при наибольшей входной вероятности ошибки p_t для СЛ-Г-МПП-кода с Г-МПП-кодом с $\ell = 6$.

Рассмотрим результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_C$ СЛ-Г-МПП-кода с БЧХ кодом (63,39) для различных скоро-

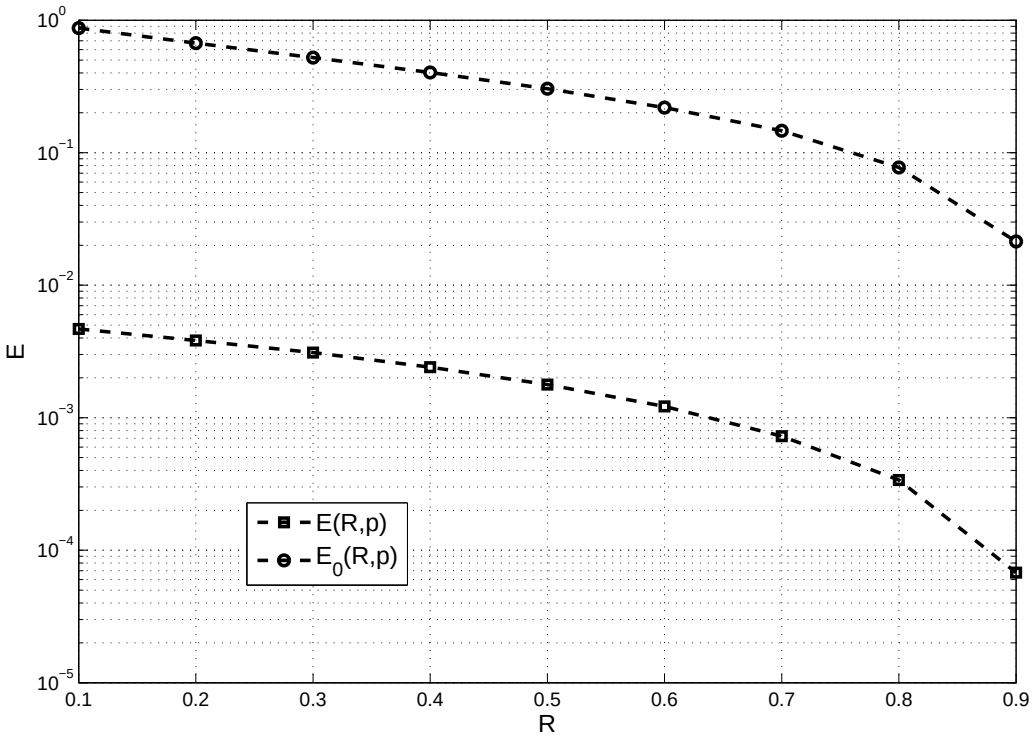

Рис. 3.6. Зависимость $E\,(R,p)$ при фиксированной $n_1 = 2000$ и $E_0\,(R,p)$ от скорости R при вероятности ошибки $p = 0,001$

стей кода R и количества слоев ℓ Г-МПП-кода. На рис. 3.10 представлены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_C$ СЛ-Г-МПП-кода со скоростью $R \approx 0,25$ и с БЧХ кодом (63,39) для различного количества слоев ℓ Г-МПП-кода. Вероятность отказа от декодирования 10^{-5} достигается при наибольшей входной вероятности ошибки p_t для СЛ-Г-МПП-кода с Г-МПП-кодом с $\ell = 7$.

На рис. 3.11 приведены результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_C$ СЛ-Г-МПП-кода со скоростью $R \approx 0,5$ и с БЧХ кодом (63,39) для различного количества слоев ℓ Г-МПП-кода. Вероятность отказа от декодирования 10^{-5} достигается при наибольшей входной вероятности ошибки p_t для СЛ-Г-МПП-кода с Г-МПП-кодом с $\ell = 6$.

Сравним результаты имитационного моделирования алгоритма декодирования СЛ-Г-МПП-кода с БЧХ кодом (31,21) и (63,39) при передаче по ДСК с входной вероятностью ошибки p_t. Для каждой скорости $R \approx \frac{1}{4}, \frac{1}{2}$ выбирем

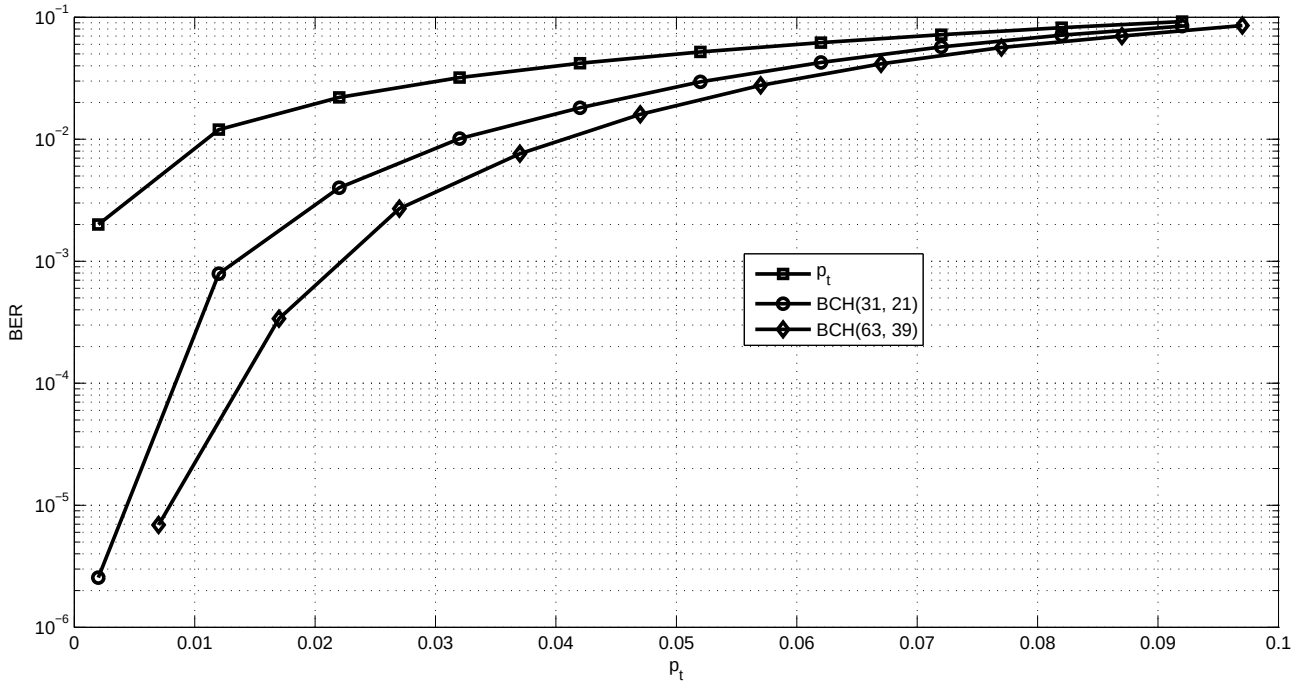

Рис. 3.7. Графики вероятности ошибки на бит после декодирования БЧХ кодов (31,21) и (63, 39) по максимуму правдопадобия в зависимости от входной вероятности ошибки p_t

такие параметры СЛ-Г-МПП-кода, что вероятность отказа от декодирования равная 10^{-5} достигалась при наибольшем значении входной вероятности p_t. На рис. 3.12 приведены графики вероятности отказа от декодирования СЛ-Г-МПП-кодов с БЧХ кодом (31,21) и (63,39) с выбранными параметрами в зависимости от входной вероятности ошибки p_t.

Теперь рассмотрим экспоненту $E_*(R, p_t)$ вероятности ошибочного декодирования по алгоритму $\mathscr{A}_C$, полученную в результате имитационного моделирования:

$$E_*(R, p_t) = \frac{-\ln P_*(R, p_t)}{n},$$

где $P_*(R, p_t)$ – вероятность отказа от декодирования, полученная в результате имитационного моделирования. Заметим, что асимптотическая оценка, полученная в § 3.3, экспоненты вероятности ошибки декодирования в действительности является оценкой экспоненты суммы вероятностей ошибки и отказа от декодирования.

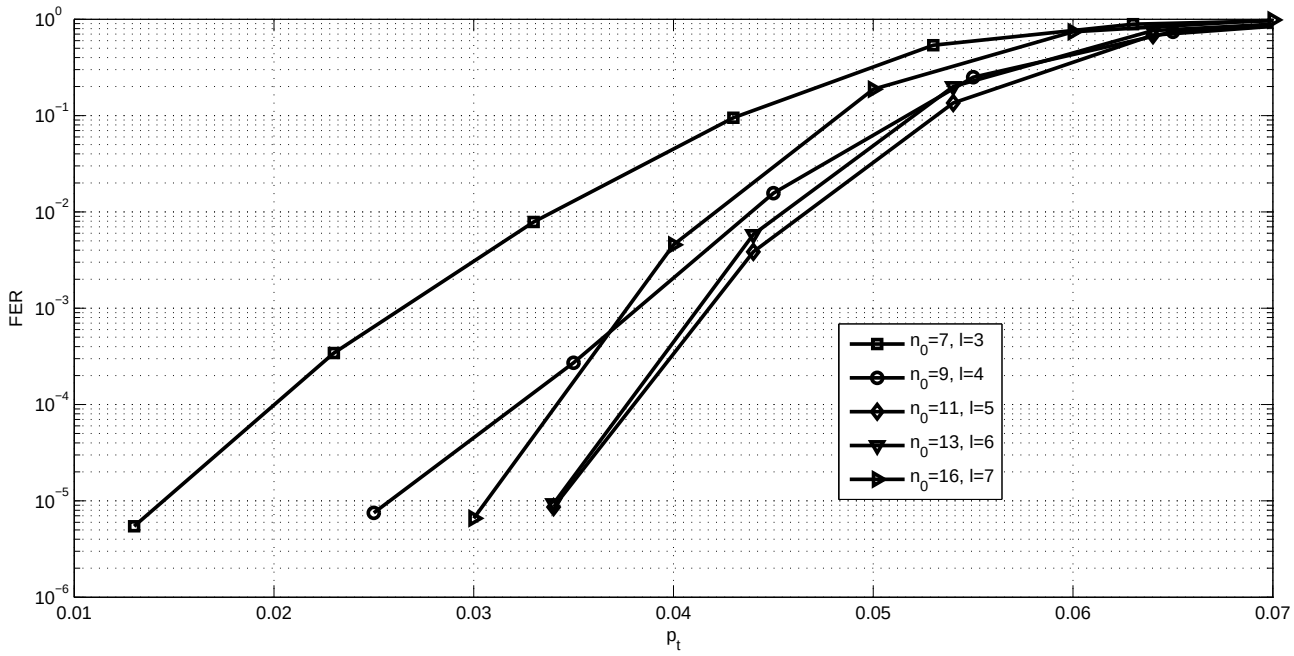

Рис. 3.8. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_C$ СЛ-Г-МПП-кода со скоростью $R \approx 0,25$ с БЧХ кодом (31,21) и различным количеством слоев Г-МПП-кода в зависимости от входной вероятности ошибки p_t

Рассмотрим результаты имитационного моделирования алгоритма декодирования $\mathscr{A}_C$ СЛ-Г-МПП-кода с БЧХ(63,39) и скоростью $R \approx 0,5$. Сравним экспоненту вероятности ошибочного декодирования, полученную в результате имитационного моделирования, и максимальное значение нижней оценки экспоненты вероятности ошибочного декодирования $E(R, p_t)$, введенную ранее (см. рис. 3.13).

Из рис. 3.13 видно, что при $p_t < 0,038$ экспонента вероятности ошибки, полученная в результате имитационного моделировани, заметно превосходит теоретическую экспоненту вероятности ошибки, но при $p_t > 0,038$ экспонента вероятности ошибки $E_*(R, p_t)$ становится меньше нижней оценки $E(R, p_t)$. Это можно объяснить тем, что полученная оценка является асимптотической, т.е. при $n \to \infty$. А в имитационном моделировании рассматривались достаточно короткие коды длины $n \approx 2000$ с короткими БЧХ кодами, которые были выбраны в качестве линейных. Также из полученной оценки

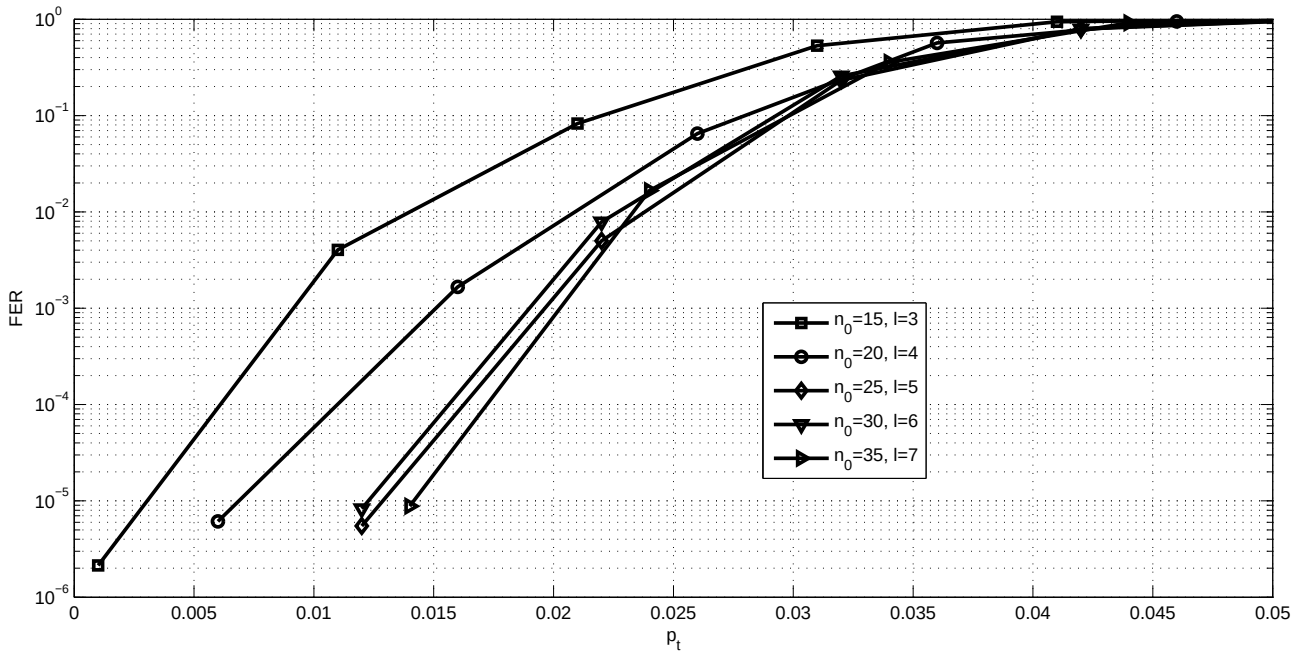

Рис. 3.9. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_C$ СЛ-Г-МПП-кода со скоростью $R \approx 0,5$ с БЧХ кодом (31,21) и различным количеством слоев Г-МПП-кода в зависимости от входной вероятности ошибки p_t

можно заключить, что в ансамбле СЛ-Г-МПП-кодов есть коды лучше, чем рассмотренные при имитационном моделировании.

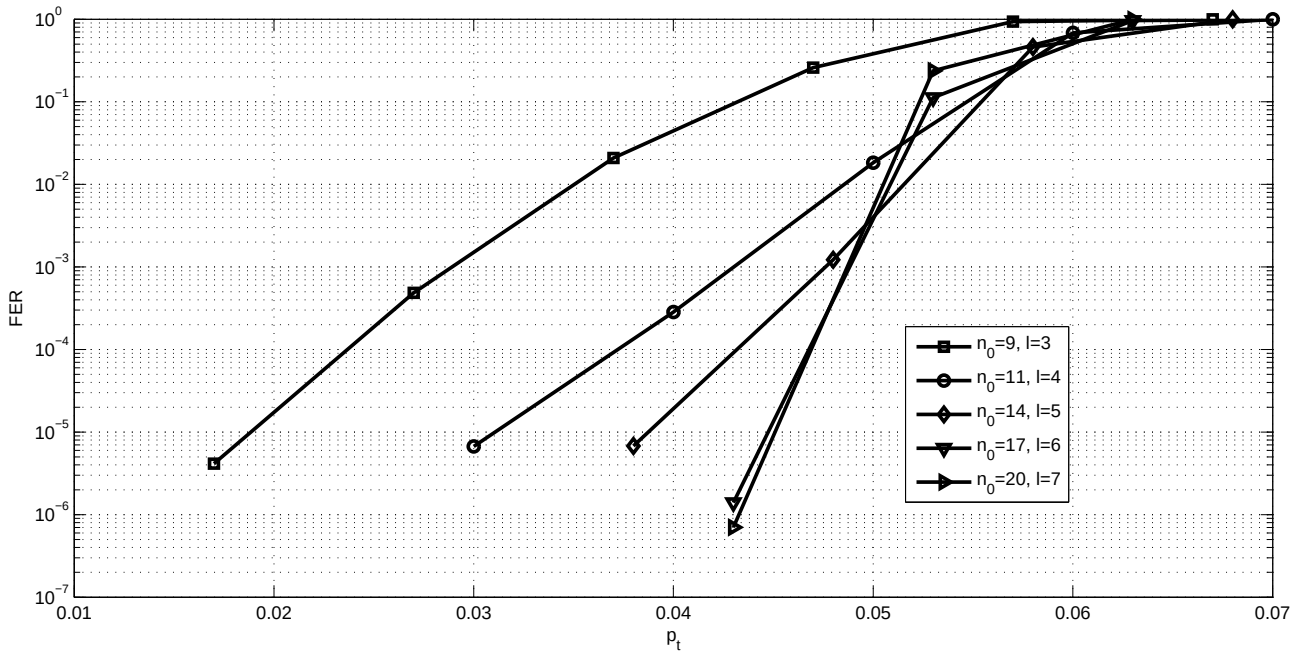

Рис. 3.10. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_C$ СЛ-Г-МПП-кода со скоростью $R \approx 0,25$ с БЧХ кодом (63,39) и различным количеством слоев Г-МПП-кода в зависимости от входной вероятности ошибки p_t

3.5. Выводы к главе

- Предложена специальная конструкция МПП-кода (СЛ-Г-МПП-код) и алгоритм декодирования $\mathscr{A}_C$;
- Получена нижняя оценка экспоненты вероятности ошибочного декодирования СЛ-Г-МПП-кода по алгоритму $\mathscr{A}_C$ со сложностью $\mathcal{O}(n \log n)$;
- Показано, что для всех скоростей меньше пропускной способности существует СЛ-Г-МПП-код, при декодировании которого по алгоритму $\mathscr{A}_C$ со сложностью $\mathcal{O}(n \log n)$ вероятность ошибки убывает экспоненциально.

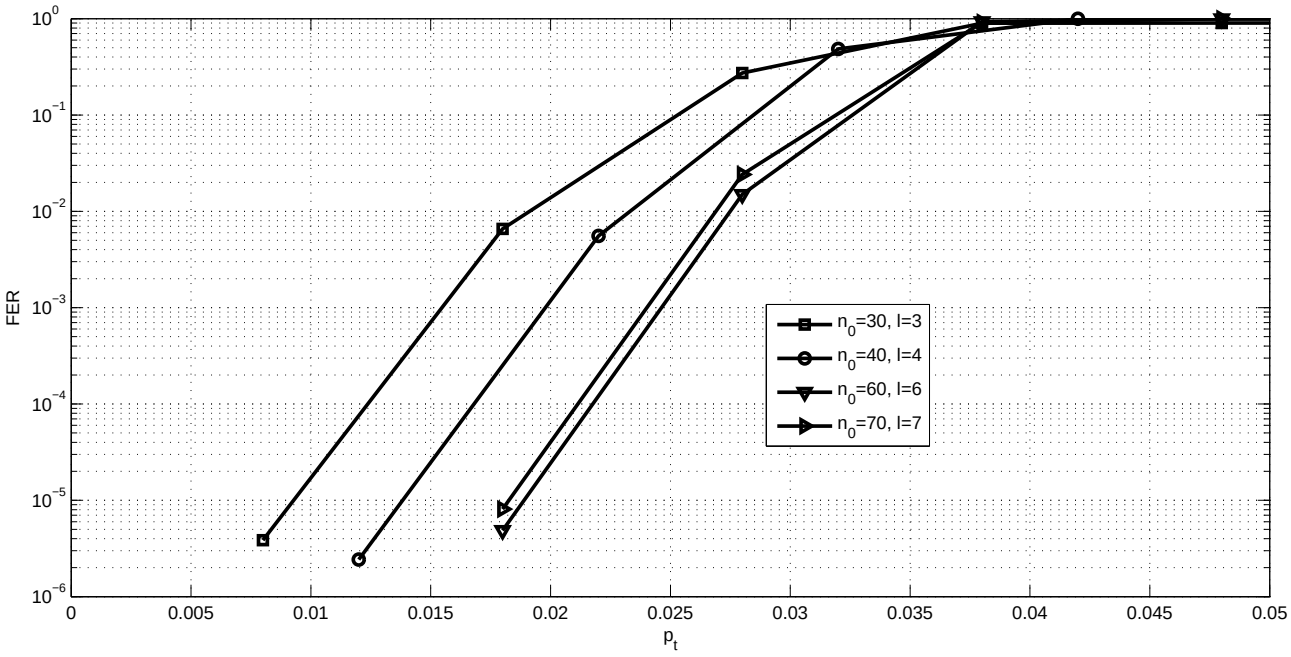

Рис. 3.11. График вероятности отказа от декодирования по алгоритму $\mathscr{A}_C$ СЛ-Г-МПП-кода со скоростью $R \approx 0,5$ с БЧХ кодом (63,39) и различным количеством слоев Г-МПП-кода в зависимости от входной вероятности ошибки p_t

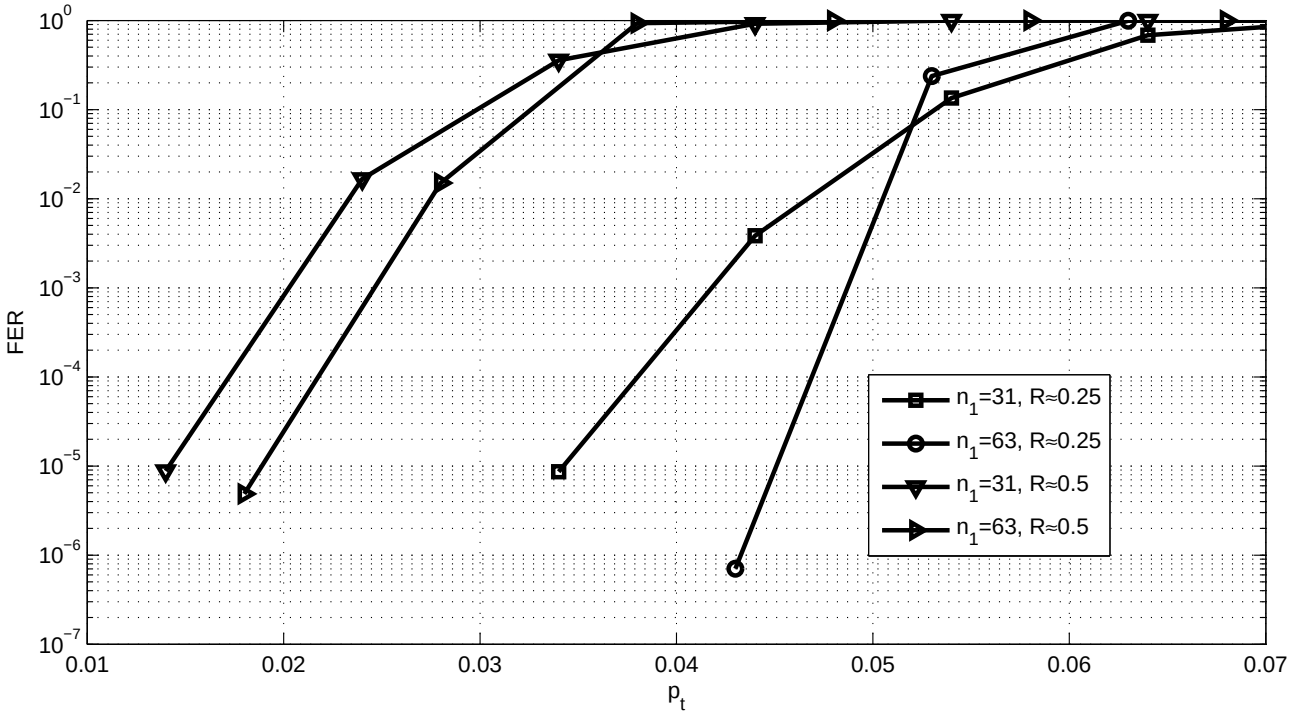

Рис. 3.12. Графики вероятности отказа от декодирования по алгоритму $\mathscr{A}_C$ СЛ-Г-МПП-кодов с различной скоростью R с БЧХ кодом (31,21) и (63,39) в зависимости от входной вероятности ошибки p_t

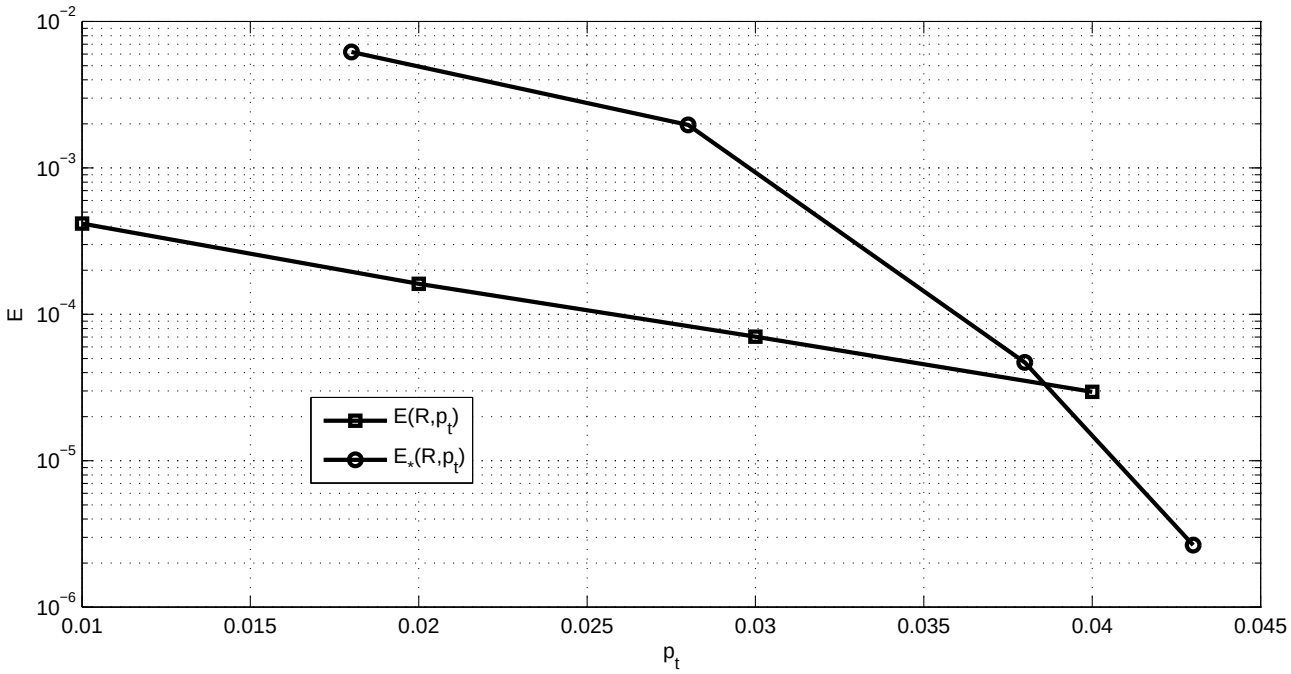

Рис. 3.13. Графики экспоненты вероятности ошибочного декодирования, полученной теоретически $E(R, p_t)$ и в результате имитационного моделирования $E_*(R, p_t)$, по алгоритму $\mathscr{A}_C$ СЛ-Г-МПП-кода со скоростью $R \approx 0,5$ в зависимости от входной вероятности ошибки p_t

Заключение

Основные результаты:

- 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 введением стираний;
- показано с помощью имитационного моделирования, что алгоритм декодирования с введением стираний лучше мажоритарного алгоритма;
- 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 для всех скоростей меньше пропускной способности существует СЛ-Г-МПП-код, при декодировании которого со сложностью $\mathcal{O}(n \log n)$ вероятность ошибки убывает экспоненциально.

Литература

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

2. Галлагер Р. Г. Теория информации и надежная связь. М.: Сов. радио, 1974.

3. 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.

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

5. Зигангиров К. Ш., Лентмайер М. Математический анализ одного итеративного алгоритма декодирования низкоплотностных кодов // Пробл. передачи информ. 2000. Т. 36, № 4. С. 35–46.

6. Зигангиров К. Ш., Пусане А. Е., Зигангиров Д. К., Костелло Д. Д. О корректирующей способности кодов с малой плотностью проверок на четность // Пробл. передачи информ. 2008. Т. 44. С. 50–62.

7. 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. 95–109.

8. Зяблов В. В., Пинскер М. С. Сложность декодирования низкоплотностных кодов при передаче по каналу со стираниями // Пробл. передачи информ. 1974. Т. 10, № 1. С. 15—28.

9. Зяблов В. В., Пинскер М. С. Оценка сложности исправления ошибок низкоплотностными кодами Галлагера // Пробл. передачи информ. 1975. Т. 11, № 1. С. 23—36.

10. 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.

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

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. Зяблов В. В., Фролов А. А. Асимптотическая оценка доли ошибок, исправляемых q-ичными МПП-кодами // Пробл. передачи информ. 2010. Т. 46, № 2. С. 142–159.

18. Ковалев С. И. Декодирование низкоплотностных кодов // Пробл. передачи информ. 1991. Т. 27, № 4. С. 51–56.

19. Маргулис Г. А. Явные конструкции расширителей // Пробл. передачи информ. 1973. Т. 9, № 4. С. 71–80.

20. 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.

21. Шеннон К. Работы по теории информации и кибернетике. М.: Изд-во иностранной литературы, 1963.

22. Шридхаран А., Лентмайер М., Трухачев Д. В. и др. О минимальном расстоянии низкоплотностных кодов с проверочными матрицами, составленными из перестановочных матриц // Пробл. передачи информ. 2005. Т. 41, № 1. С. 39–52.

23. Barak O., Burshtein D. Lower bounds on the spectrum and error rate LDPC

code ensembles // Proceedings of IEEE International Symposium on Information Theory (ISIT). 2005. — sept. P. 42 –46.

24. Barak O., Burshtein D. Lower Bounds on the Error Rate of LDPC Code Ensembles // Information Theory, IEEE Transactions on. 2007. — nov. Vol. 53, no. 11. P. 4225 –4236.

25. Barg A., Mazumdar A. On the Number of Errors Correctable with Codes on Graphs // IEEE Transactions on Information Theory. 2011. — feb. Vol. 57, no. 2. P. 910–919.

26. Barg A., Mazumdar A., Zemor G. Weight distribution and decoding of codes on hypergraph // Adv. Math. Commun. 2008. Vol. 2, no. 4. P. 433–450.

27. Barg A., Zemor G. Error exponents of expander codes // IEEE Trans. Inform. Theory. 2002. — jun. Vol. 48, no. 6. P. 1725–1729.

28. Barg A., Zemor G. Distance properties of expander codes // IEEE Transactions on Information Theory. 2006. — jan. Vol. 52, no. 1. P. 78–90.

29. Barg A., Zemor G. Codes on hypergraphs // Proceedings of IEEE International Symposium on Information Theory (ISIT). 2008. — july. P. 156 –160.

30. Bazzi L., Richardson T., Urbanke R. Exact thresholds and optimal codes for the binary-symmetric channel and Gallager's decoding algorithm A // IEEE Transactions on Information Theory. 2004. — sep. Vol. 50, no. 9. P. 2010 – 2021.

31. Bhardwaj V., Pathak N., Kumar A. Structured LDPC Codes with Linear Complexity Encoding // WRI International Conference on Communications and Mobile Computing (CMC). Vol. 1. 2009. — jan. P. 200 –203.

32. Boutros J., Pothier O., Zemor G. Generalized low density (Tanner) codes // Proc. IEEE Int. Conference on Communications. Vol. 1. 1999. P. 441–445.

33. Burshtein D. On the Error Correction of Regular LDPC Codes Using the Flipping Algorithm // IEEE Transactions on Information Theory. 2008. — feb. Vol. 54, no. 2. P. 517–530.

34. Burshtein D., Barak O. Upper Bounds on the Error Exponents of LDPC Code Ensembles // Proceedings of IEEE International Symposium on Information Theory. 2006. — july. P. 401 –405.

35. Burshtein D., Miller G. Asymptotic enumeration methods for analyzing LDPC codes // IEEE Transactions on Information Theory. 2004. — june. Vol. 50, no. 6. P. 1115 – 1131.

36. Chung S.-Y., Forney J., G.D., Richardson T., Urbanke R. On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit // IEEE Communications Letters. 2001. — feb. Vol. 5, no. 2. P. 58 –60.

37. Di C., Proietti D., Telatar I. et al. Finite-length analysis of low-density parity-check codes on the binary erasure channel // IEEE Transactions on Information Theory. 2002. — jun. Vol. 48, no. 6. P. 1570 –1579.

38. Di C., Richardson T., Urbanke R. Weight Distribution of Low-Density Parity-Check Codes // Information Theory, IEEE Transactions on. 2006. — nov. Vol. 52, no. 11. P. 4839 –4855.

39. Divsalar D. Ensemble Weight Enumerators for Protograph LDPC Codes // Proceedings of IEEE International Symposium on Information Theory (ISIT). 2006. — july. P. 1554 –1558.

40. Divsalar D., Jones C., Dolinar S., Thorpe J. Protograph based LDPC codes with minimum distance linearly growing with block size // IEEE Global Telecommunications Conference (GLOBECOM). Vol. 3. 2005. — nov.-2 dec. P. 5.

41. Freundlich S., Burshtein D., Litsyn S. Approximately Lower Triangular Ensembles of LDPC Codes With Linear Encoding Complexity // IEEE Transactions on Information Theory. 2007. — april. Vol. 53, no. 4. P. 1484 –1494.

42. Gallager R. G. Low-Density Parity-Check Codes. Cambridge, MA: MIT Press, 1963.

43. Goldenberg I., Burshtein D. Upper Bound on Error Exponent of Regular LDPC Codes Transmitted Over the BEC // IEEE Transactions on Information Theory. 2009. — june. Vol. 55, no. 6. P. 2674 –2681.

44. Johnson S. A Finite-Length Algorithm for LDPC Codes Without Repeated Edges on the Binary Erasure Channel // IEEE Transactions on Information Theory. 2009. — jan. Vol. 55, no. 1. P. 27 –32.

45. Lentmaier M., Zigangirov K. Iterative decoding of generalized low-density parity-check codes // Proc. IEEE Int. Symposium on Inform. Theory. 1998. — aug. P. 149.

46. Lentmaier M., Zigangirov K. On generalized low-density parity-check codes based on Hamming component codes // IEEE Commun. Lett. 1999. — aug. Vol. 3, no. 8. P. 248–250.

47. Litsyn S., Shevelev V. On ensembles of low-density parity-check codes: asymptotic distance distributions // IEEE Transactions on Information Theory. 2002. — apr. Vol. 48, no. 4. P. 887 –908.

48. Litsyn S., Shevelev V. Distance distributions in ensembles of irregular low-density parity-check codes // IEEE Transactions on Information Theory. 2003. — dec. Vol. 49, no. 12. P. 3140 – 3159.

49. Lu J., Moura J. Linear Time Encoding of LDPC Codes // IEEE Transactions on Information Theory. 2010. — jan. Vol. 56, no. 1. P. 233 –249.

50. Luby M., Mitzenmacher M., Shokrollahi M., Spielman D. Improved low-density parity-check codes using irregular graphs // IEEE Transactions on Information Theory. 2001. — feb. Vol. 47, no. 2. P. 585 –598.

51. MacKay D. Good error-correcting codes based on very sparse matrices // IEEE Transactions on Information Theory. 1999. — mar. Vol. 45, no. 2. P. 399 –431.

52. Miladinovic N., Fossorier M. Generalized LDPC codes and generalized stopping sets // IEEE Transactions on Communications. 2008. — febr. Vol. 56, no. 2. P. 201–212.

53. Miller G., Burshtein D. Bounds on the maximum-likelihood decoding error probability of low-density parity-check codes // IEEE Transactions on Information Theory. 2001. — nov. Vol. 47, no. 7. P. 2696 –2710.

54. Paolini E., Flanagan M., Chiani M., Fossorier M. On a class of doubly-generalized LDPC codes with single parity-check variable nodes // Proceedings of IEEE International Symposium on Information Theory (ISIT). 2009. — july. P. 1983 –1987.

55. Pishro-Nik H., Fekri F. On decoding of low-density parity-check codes over the binary erasure channel // IEEE Transactions on Information Theory. 2004. — march. Vol. 50, no. 3. P. 439 – 454.

56. Pishro-Nik H., Fekri F. Performance of low-density parity-check codes with linear minimum distance // Information Theory, IEEE Transactions on. 2006. — jan. Vol. 52, no. 1. P. 292 – 300.

57. Rathi V. On the asymptotic weight distribution of regular LDPC ensembles // Proceedings of International Symposium on Information Theory (ISIT). 2005. — sept. P. 2161 –2165.

58. Rathi V. On the Asymptotic Weight and Stopping Set Distribution of Regular LDPC Ensembles // IEEE Transactions on Information Theory. 2006. — sept. Vol. 52, no. 9. P. 4212 –4218.

59. Richardson T., Shokrollahi M., Urbanke R. Design of capacity-approaching irregular low-density parity-check codes // Information Theory, IEEE Transactions on. 2001. — feb. Vol. 47, no. 2. P. 619 –637.

60. Richardson T., Urbanke R. Efficient encoding of low-density parity-check codes // IEEE Transactions on Information Theory. 2001. — feb. Vol. 47, no. 2. P. 638 –656.

61. 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.

62. 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.

63. Sipser M., Spielman D. Expander codes // IEEE Trans. Inform. Theory. 1996. — nov. Vol. 42, no. 6. P. 1710–1722.

64. Skachek V. Minimum distance bounds for expander codes // Information Theory and Applications Workshop. 2008. — feb. P. 366 –370.

65. Spielman D. Linear-time encodable and decodable error-correcting codes // IEEE Transactions on Information Theory. 1996. — nov. Vol. 42, no. 6. P. 1723–1731.

66. Stiglmayr S., Zyablov V. V. Asymptotically Good Low-Density Codes Based on Hamming Codes // Proc. XI International Symposium on Problems of Redundancy in Information and Control Systems. Saint-Petersburg, Russia: 2007. — jul. P. 98–103.

67. Tanner R. A recursive approach to low complexity codes // IEEE Trans. Inform. Theory. 1981. — sept. Vol. 27, no. 5. P. 533–547.

68. Zarrinkhat P., Banihashemi A. Threshold values and convergence properties of majority-based algorithms for decoding regular low-density parity-check codes // IEEE Transactions on Communications. 2004. — dec. Vol. 52, no. 12. P. 2087 – 2097.

69. Zemor G. On expander codes // IEEE Transactions on Information Theory. 2001. — feb. Vol. 47, no. 2. P. 835–837.

70. Zyablov V., Loncar M., 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.

71. Zyablov V., Loncar M., 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.

72. Zyablov V., Loncar M., 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.

73. 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.