На правах рукописи

Фролов Алексей Андреевич

Корректирующие свойства недвоичных кодов с малой плотностью проверок

05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2012

Работа выполнена в Лаборатории № 3 Федерального государственного бюджетного учреждения науки Института проблем передачи информации им. А. А. Харкевича Российскоий академии наук (ИППИ РАН).

Научный руководитель: (консультант) — *доктор технических наук,* **Зяблов Виктор Васильевич**

Официальные оппоненты: — **Бассалыго Леонид Александрович**, *доктор физико-математических наук, ИППИ РАН, главный научный сотрудник Лаборатории № 4*

Трифонов Петр Владимирович, *кандидат технических наук, доцент, ФГБОУ ВПО Санкт-Петербургский государственный политехнический университет, доцент кафедры распределенных вычислений и компьютерных сетей*

Ведущая организация: — *Федеральное государственное автономное образовательное учреждение высшего профессионального образования Санкт-Петербургский государственный университет аэрокосмического приборостроения*

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

С диссертацией можно ознакомиться в библиотеке ИППИ РАН.

Автореферат разослан «____» _____ 2012 г.

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

Общая характеристика работы

Актуальность темы. В настоящее время активное развитие вычислительной техники и информационных технологий привело к резкому увеличению объемов обрабатываемой и передаваемой информации, вследствие этого возрастают и требования к скорости передачи. В связи с этим важнейшей задачей является обеспечение высокого качества передаваемой информации (т.е. уменьшение вероятности ошибки) при высокоскоростной передаче.

Для исправления ошибок используют помехоустойчивые коды. Важнейшим обстоятельством при выборе той или иной кодовой конструкции на практике является наличие быстрых алгоритмов кодирования и декодирования. Двоичные коды с малой плотностью проверок (МПП-коды) удовлетворяют этому требованию. Однако не менее важно, чтобы алгоритмы декодирования были способны исправить большое число ошибок. Таким образом, главным вопросом является вопрос о том, насколько ухудшаются корректирующие свойства кодов при использовании простых алгоритмов декодирования. Исследованию двоичных МПП-кодов посвящено множество работ, среди которых следует особо отметить работы таких русских и зарубежных ученых, как Р. Дж. Галлагер, М. С. Пинскер, В. В. Зяблов, К. Ш. Зигангиров, А. М. Барг, Р. Таннер, Д. Спилман, Д. Маккей, Т. Ричардсон, Р. Урбанке, Д. Бурштейн, С. Л. Литсын, Ж. Земор. Доказано существование двоичных МПП-кодов, способных исправить линейно растущее с длиной кода число ошибок при сложности декодирования $O(n \log_2 n)$, где n – длина кода. Как результат, в настоящее время эти коды используются в стандартах подвижной беспроводной связи (например, LTE), цифровой телефонии; рекомендованы для использования в стандартах оптической связи, спутниковой связи, WiMAX, 802.11n.

Все исследования будем проводить для радиочастотного канала; пусть весь диапазон частот разбит на непересекающиеся частотные поддиапазоны (подканалы) при помощи технологии мультиплексирования с использованием ортогональных частот (OFDM). В связи с ограниченностью частотного ресурса дальнейшее увеличение скорости передачи возможно лишь с помощью увеличения скорости передачи в подканалах. Этого можно добиться, увеличив мощность алфавита модуляции. Из-за этого особенно интересными становятся недвоичные корректирующие коды. Недвоичные МПП-коды впервые рассмотрены в работе М. Дэви и Д. Маккея. Число работ, посвященных исследованию недвоичных МПП-кодов, сравнительно невелико. В существующих работах по этой теме приводятся результаты имитационного моделирования. Однако результатов исследований методом имитационного моделирования недостаточно.

Таким образом, необходимо исследовать корректирующие свойства недвоичных МПП-кодов теоретически и методом имитационного моделирования,

а также рассмотреть возможность применения этих кодов в современных системах связи. Так как в настоящее время пристальное внимание уделяется построению систем множественного доступа, то, в первую очередь, необходимо рассмотреть возможность применения недвоичных МПП-кодов в системах множественного доступа.

Цель диссертационной работы: исследовать корректирующие свойства недвоичных МПП-кодов теоретически и методом имитационного моделирования, а также разработать сигнально-кодовую конструкцию (СКК) на основе недвоичных МПП-кодов для системы множественного доступа.

Для достижения поставленных целей необходимо решить следующие задачи:

- Исследовать потенциальные корректирующие свойства МПП-кодов над полем $GF(q)$.
- Исследовать реализуемые корректирующие свойства МПП-кодов над полем $GF(q)$ теоретически и методом имитационного моделирования.
- Разработать СКК на основе недвоичных МПП-кодов для системы множественного доступа. Провести исследование полученной системы в канале с аддитивным белым гауссовским шумом методом имитационного моделирования.

Научная новизна. В настоящей работе впервые:

- Теоретически исследованы потенциальные и реализуемые корректирующие свойства МПП-кодов над полем $GF(q)$.
- Предложен алгоритм декодирования МПП-кодов над полем $GF(q)$ с вводом стираний.
- МПП-коды над полем $GF(q)$ использованы в СКК для системы множественного доступа.

Теоретическая и практическая ценность. Получены верхняя и нижняя границы минимального кодового расстояния для МПП-кодов над полем $GF(q)$. Улучшена асимптотическая оценка доли ошибок, гарантированно исправимых МПП-кодами над полем $GF(q)$ с помощью алгоритма, имеющего сложность $O(n \log_2 n)$. Получена нижняя оценка относительной суммарной скорости передачи для системы множественного доступа, использующей бесшумный векторный дизъюнктивный канал. Эта оценка асимптотически совпадает с верхней оценкой.

Результаты, полученные в процессе подготовки диссертационной работы, использованы в программе фундаментальных исследований Президиума РАН «Проблемы создания национальной научной распределенной информационно-вычислительной среды на основе GRID технологий и современных телекоммуникационных сетей» по направлению «Распределенная обработка данных. Информационная безопасность сетевых технологий» (№ Госрегистрации 01200965142), программе фундаментальных научных исследований ОНИТ РАН «Архитектура, системные решения, программное обеспечение стандартизация и информационная безопасность информационно-вычислительных комплексов новых поколений» по направлению № 3.1 «Обеспечение информационной безопасности распределенных информационно-вычислительных систем» (Регистрация РАН № 10002-251/ОИТВС–04/103-96/260503-208) и разработках ЗАО «Телум», что подтверждено соответствующими актами.

На защиту выносятся следующие положения:

1. Верхняя и нижняя границы минимального кодового расстояния для МПП-кодов над полем $GF(q)$.

2. Асимптотическая оценка доли ошибок, гарантированно исправимых МПП-кодами над полем $GF(q)$ с помощью алгоритма декодирования, имеющего сложность $O(n \log_2 n)$.

3. СКК для системы множественного доступа, использующей бесшумный векторный дизъюнктивный канал, нижняя оценка относительной суммарной скорости передачи, которая асимптотически совпадает с верхней.

4. СКК на основе недвоичных МПП-кодов для системы множественного доступа, использующей векторный канал с аддитивным белым гауссовским шумом, которая позволяет одновременно работать большому числу пользователей.

Апробация работы. Основные результаты диссертации докладывались на следующих конференциях: IEEE International Symposium on Information Theory (2011); XII International Symposium on Problems of Redundancy in Information and Control Systems (2009); XII International Workshop on Algebraic and Combinatorial Coding Theory (2010); конференциях молодых ученых и специалистов ИППИ РАН «Информационные технологии и системы» (2009–2011). Кроме того, основные результаты докладывались на семинарах по теории кодирования в ИППИ РАН.

Публикации. Материалы диссертации опубликованы в 10 печатных работах, из них 4 статьи [1–4] в рецензируемых журналах и 6 статей [5–10] в сборниках трудов конференций.

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.

Структура и объем диссертации Диссертация состоит из введения, обзора литературы, трех глав, заключения и библиографии. Общий объем диссертации 117 страниц, включая 64 рисунка и 8 таблиц. Библиография включает 83 наименования на 10 страницах.

Содержание работы

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

В первой главе исследуются потенциальные корректирующие свойства МПП-кодов над полем $GF(q)$. Показано, как меняются корректирующие свойства этих кодов при изменении их параметров, что важно для практического применения этих кодов.

В *разделе 1.1* приводится введение к главе 1.

В *разделе 1.2* описана структура МПП-кодов над полем $GF(q)$. Для построения проверочной матрицы такого кода рассмотрим блочную диагональную матрицу $\mathbf{H}_b$

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

на главной диагонали которой находятся b проверочных матриц $\mathbf{H}_0$ $(n_0, k_0 = R_0 n_0)$-кода над полем $GF(q)$ (далее будем использовать термин код-компонент), $m = n_0 - k_0$.

Пусть $\varphi(\mathbf{H}_b)$ обозначает матрицу, полученную из матрицы $\mathbf{H}_b$ произвольной перестановкой столбцов и умножением их на произвольные ненулевые элементы поля $GF(q)$. Тогда матрица

$$\mathbf{H} = \begin{pmatrix} \varphi_1(\mathbf{H}_b) \\ \varphi_2(\mathbf{H}_b) \\ \vdots \\ \varphi_\ell(\mathbf{H}_b) \end{pmatrix}_{\ell bm \times bn_0}$$

размера $\ell bm \times bn_0$, составленная из ℓ таких матриц, как слоев, является разреженной проверочной матрицей МПП-кода над полем $GF(q)$.

Определим ансамбль МПП-кодов над полем $GF(q)$ следующим образом:

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

Отметим, что в отличие от определения ансамбля для двоичных кодов здесь добавляется умножение на константы, не равные нулю. Ясно, что длина кода $n = bn_0$.

Для скорости кода $C \in \mathscr{E}(b)$ справедливо соотношение $R \geqslant 1-\ell\,(1-R_0)$, равенство достигается в случае полного ранга матрицы $\mathbf{H}$.

В *разделе 1.3* получена нижняя оценка минимального кодового расстояния для ансамбля $\mathscr{E}(b)$ МПП-кодов над полем $GF(q)$. Основной результат этого раздела сформулирован в виде теоремы 1.2.

Теорема 1.2. Если существует хотя бы один положительный корень (относительно переменной δ) уравнения

$$F_1\left(\delta, n_0\right) = 0, \tag{1}$$

тогда в ансамбле $\mathscr{E}(b)$ существуют коды $\{C_i\}_{i=1}^{N(b)}$ $\left(\lim\limits_{b\to\infty} \frac{N(b)}{|\mathscr{E}(b)|} = 1\right)$, такие что $d\left(C_i\right) \geqslant \left(\delta_0 - \varepsilon\right) n$, где ε – сколь угодно малое положительное число; δ_0 – наименьший положительный корень уравнения (1), а

$$\begin{aligned} F_1\left(\delta, n_0\right) &= \left(\ell - 1\right) H_q\left(\delta\right) + \\ &+ \ell \max_{s>0} \left(\delta \log_q\left(s\right) - \frac{1}{n_0} \log_q\left(g_0\left(s, n_0\right)\right) \right), \end{aligned}$$

где $H_q(x) = -x\log_q(x) - (1-x)\log_q(1-x) + x\log_q(q-1)$ – функция q-ичной энтропии, а $g_0\left(s, n_0\right)$ – производящая функция весов кодовых слов компонентного кода.

В *разделе 1.4* получена верхняя оценка минимального кодового расстояния для МПП-кодов над полем $GF(q)$. Основной результат этого раздела сформулирован в виде теоремы 1.3.

Теорема 1.3. Пусть $C \in \mathscr{E}(b)$ и пусть $d(C) = d$, тогда

$$R(C) \leqslant \min_{\left\lceil \frac{d}{n_0} \right\rceil \leqslant b' \leqslant b} \left[1 - \frac{\ell\tau}{\ell + \tau - 1} \left(1 - R^*\left(\tau n, d\right) \tau\right) \right],$$

где $R^*\left(\tau n, d\right)$ – любая верхняя граница скорости линейного кода, $\tau = \frac{b'}{b}$, $b' \in \mathbb{N}$.

Асимптотическая форма верхней границы дается в теореме 1.4.

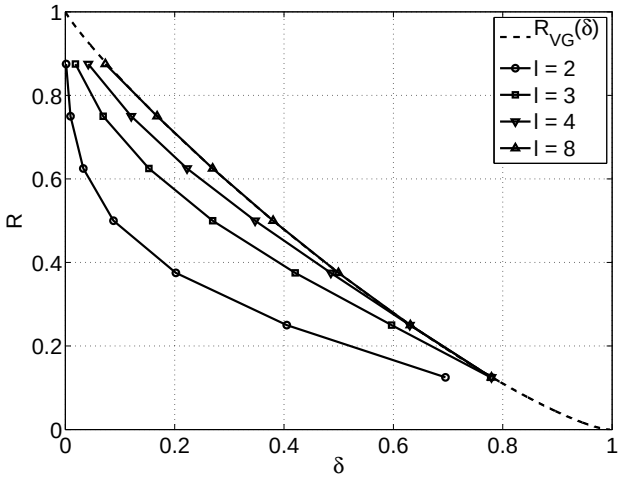

Рис. 1. Нижние границы при $q = 256$

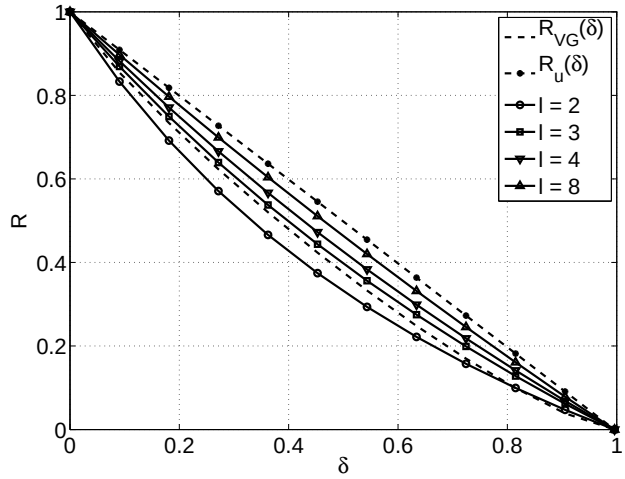

Рис. 2. Верхние границы при $q = 256$

Теорема 1.4. Пусть $\{C_b\}_{b=1}^{\infty}, C_b \in \mathscr{E}(b)$ – это последовательность МПП-кодов над полем $GF(q)$ с относительным кодовым расстоянием $\delta(C_b) = \frac{d(C_b)}{n(C_b)} = \delta$, тогда

$$\begin{aligned} R(\delta) &= \lim_{b\to\infty}(R(C_b)) \leqslant \\ &\leqslant \min_{\frac{q}{q-1}\delta\leqslant\tau\leqslant 1}\left[1 - \frac{\ell\tau}{\ell+\tau-1}\left(1 - R^*\left(\frac{\delta}{\tau}\right)\tau\right)\right]. \end{aligned}$$

В *разделе 1.5* приводится анализ результатов, полученных при $q = 64, q = 256, q = 1024$. Результаты для $q = 256$ приводятся на рис. 1 и рис. 2. На рис. 1 приведено сравнение нижних границ, построенных для МПП-кодов с разным числом слоев ($\ell = 2, 3, 4, 8$). В качестве компонентного кода выбран код Рида–Соломона. Для сравнения приведена также граница Варшамова–Гилберта ($R_{VG}(\delta)$). На рис. 2 приведено сравнение верхних границ, построенных для МПП-кодов с разным числом слоев ($\ell = 2, 3, 4, 8$), в качестве функции R^* использована первая граница Мак-Элиса–Родемича–Рамсея–Велча. Для сравнения приведены также граница Варшамова–Гилберта и верхняя граница для линейных кодов ($R_u(\delta)$), полученная из границ Плоткина, Бассалыго–Элайеса и первой границы Мак-Элиса–Родемича–Рамсея–Велча.

В *разделе 1.6* приводятся выводы к главе 1.

Выводы к главе 1

- Получена нижняя граница минимального кодового расстояния для МПП-кодов над полем $GF(q)$. Эта граница улучшается с увеличением числа слоев (ℓ). При $\ell \geqslant 8$ эта граница проходит очень близко к границе Варшамова–Гилберта и начинает отходить от нее лишь на высоких скоростях.

- Получена верхняя граница минимального кодового расстояния для МПП-кодов над полем $GF(q)$. Эта граница лучше всех известных верхних границ для линейных кодов. Она улучшается с увеличением числа слоев. При $\ell = 2$[1] и $q \geqslant 32$ эта граница лежит ниже границы Варшамова–Гилберта, т.е. МПП-коды с такими параметрами хуже лучших из известных линейных кодов. При $q \geqslant 1024$ не достаточно и трех слоев.

Результаты первой главы опубликованы в работах [3, 10].

Во второй главе исследуются реализуемые корректирующие свойства МПП-кодов над полем $GF(q)$. Современные системы связи требуют высокой скорости передачи и при этом высокой надежности, следовательно, нужны длинные коды с хорошими корректирующими свойствами при простом декодировании. В связи с этим получена асимптотическая оценка доли гарантированно исправимых ошибок при декодировании с помощью алгоритма, имеющего наименьшую из известных сложность. Кроме того, предложены новые относительно просто реализуемые алгоритмы декодирования. Эффективность этих алгоритмов показана с помощью имитационного моделирования.

В *разделе 2.1* приводится введение к главе 2.

Раздел 2.2 посвящен асимптотической оценке доли ошибок, исправляемых МПП-кодами над полем $GF(q)$. Этот раздел состоит их четырех параграфов.

В *параграфе 2.2.1* приводится описание мажоритарного алгоритма декодирования $\mathscr{A}$, который является обобщением двоичного мажоритарного алгоритма.

В *параграфе 2.2.2* в виде теоремы 2.5 формулируется основной результат главы 2.

Теорема 2.5. Если существует по крайней мере один положительный корень (относительно переменной ω) уравнения (2), то в ансамбле $\mathscr{E}(b)$ существуют коды (с вероятностью $p_b : \lim\limits_{b\to\infty} p_b = 1$), которые могут исправить любую комбинацию ошибок веса не более $\lfloor \frac{\omega_\alpha n}{2} \rfloor$ при сложности декодирования $O(n \log_2 n)$, причем

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

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

$$h(\omega) + \omega \log_2 (q-1) - \ell F_2(\alpha, \omega, n_0) = 0, \qquad (2)$$

где $h(\omega) = -\omega \log_2 \omega - (1-\omega)\log_2(1-\omega)$ – двоичная энтропия, а функция

[1] при таком выборе мы получаем класс кодов на двудольных графах, в который входят коды на двудольных графах–расширителях(в англоязычной литературе используется термин “expander codes”)

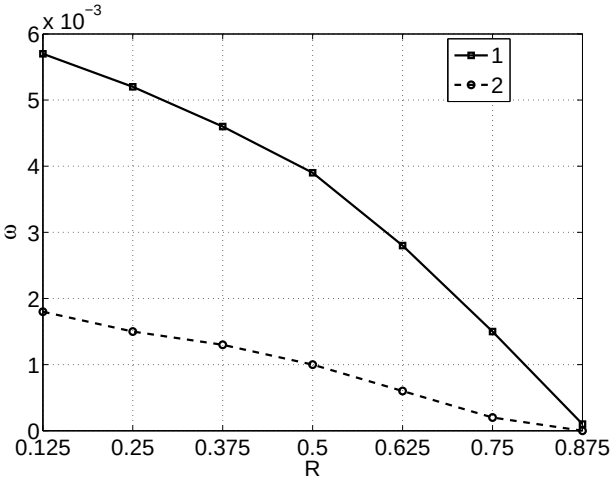

Рис. 3. Сравнение зависимостей доли гарантированно исправимых ошибок от R при $q = 128$

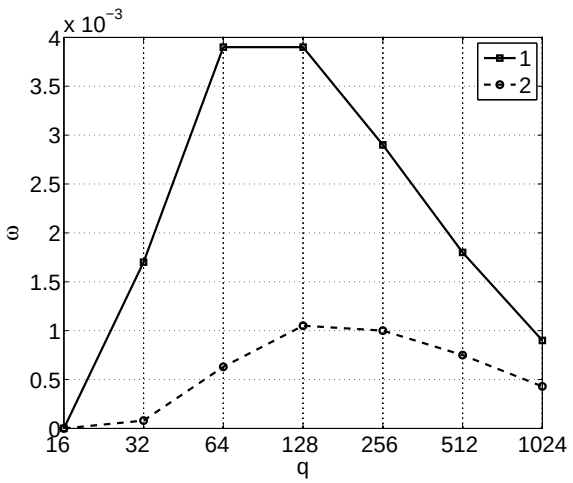

Рис. 4. Сравнение зависимостей доли гарантированно исправимых ошибок от q при $R = 0,5$

$F_2(\alpha, \omega, n_0)$ определяется следующим образом:

$$\begin{aligned} F_2(\alpha,\omega,n_0) &= h(\omega) + \omega\log_2(q-1) - \frac{1}{n_0}h(\alpha\omega n_0) + \\ &+ \max_{s>0}\left\{\omega\log_2(s) - \frac{1}{n_0}\log_2(g_0(s,n_0)) - \right. \\ &- \left.\alpha\omega\log_2\left(\frac{g_1(s,n_0)}{g_0(s,n_0)}\right)\right\}, \end{aligned}$$

где $\alpha > \frac{1}{2} + \varepsilon_2$, ε_2 – сколь угодно малая положительная величина.

Поиск максимума ведется по всем положительным s таким, что

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

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

В *параграфе 2.2.3* дается доказательство основного результата.

В *параграфе 2.2.4* приводится анализ полученных результатов. На рис. 3 и рис. 4 показано сравнение полученной оценки (зависимость помечена цифрой 1) доли гарантированно исправимых ошибок и лучшей из существующих оценок (зависимость помечена цифрой 2). Видно, насколько полученная оценка лучше.

Раздел 2.3 посвящен исследованию реализуемых корректирующих свойств МПП-кодов над полем $GF(q)$ методом имитационного моделирования.

В *параграфе 2.3.1* приводится описание двух алгоритмов декодирования: алгоритма декодирования с вводом стираний ($\mathscr{A}_*$) и алгоритма распростране-

ния доверия[2] ($\mathscr{A}_{BP}$). Эти алгоритмы больше, нежели алгоритм $\mathscr{A}$ подходят для практического применения. Оба алгоритма являются итеративными.

Алгоритм $\mathscr{A}_*$ был предложен в работе [2] и является алгоритмом декодирования с жестким решением. Он был разработан для применения в случае наличия ошибок и стираний в слове на входе декодера. Однако в работе [2] показано, что он эффективнее алгоритма $\mathscr{A}$ в случае, если во входном слове присутствуют только ошибки. Главное отличие этого алгоритма от мажоритарного состоит во вводе стираний на места символов, подозрительных на ошибки. На каждой итерации подозрительные символы заменяются стираниями, и далее в пределах этой итерации выполняется только исправление стираний. Стирания, которые были введены и не были исправлены, после итерации удаляются. Эти две операции повторяются до тех пор, пока не случится такого, что в процессе итерации мы не исправили ни одного стирания.

Алгоритм $\mathscr{A}_{BP}$ для МПП-кодов над полем $GF(q)$ предложен М. Дэви и Д. Маккеем и является модифицированной версией алгоритма распространения доверия для двоичного случая. Это алгоритм с мягким решением, на входе алгоритма априорные распределения для каждого из символов принятого слова, на выходе – апостериорные. Он гораздо эффективнее алгоритма $\mathscr{A}_*$, однако в то же самое время и гораздо медленнее последнего, несмотря на все улучшения, сделанные в последнее время (использование многомерного преобразования Фурье, работа с логарифмами вероятностей).

В *параграфе 2.3.2* рассмотрен q-ичный симметричный канал (qСК).

Исследована зависимость корректирующих свойств МПП-кодов над полем $GF(q)$ от числа слоев (ℓ) при разных скоростях. Получено, что алгоритм $\mathscr{A}_{BP}$ лучше работает при малом числе слоев ($\ell = 3$ при $R = 0,25$ и $R = 0,5$; $\ell = 4$ при $R = 0,75$). Для алгоритма $\mathscr{A}_*$ результат такой – $\ell = 6$ при $R = 0,25$ и $R = 0,5$; $\ell = 7$ при $R = 0,75$.

Приведено сравнение лучших вариантов алгоритмов $\mathscr{A}_*$ и $\mathscr{A}_{BP}$ при разных скоростях (число слоев различно и выбрано наиболее подходящим для соответствующих алгоритмов). Показано, что при всех скоростях алгоритм $\mathscr{A}_{BP}$ оказывается лучше алгоритма $\mathscr{A}_*$, несмотря на то, что алгоритм $\mathscr{A}_{BP}$ применяется здесь в жесткой форме.

Показано, что корректирующие свойства (доля исправимых ошибок при условии, что вероятность ошибки на блок равна 10^{-4}) МПП-кодов над полем $GF(q)$ улучшаются с увеличением длины кода (использован алгоритм $\mathscr{A}_{BP}$).

Приведено сравнение разных декодеров ($\mathscr{A}_{BP}$ при $q = 2, 8, 64$) в q-ичном симметричном канале при $q = 64$ (рис. 5). Параметры кодов – $R = 0,5$; $\ell = 3$; $n_0 = 6$; длина $n = 510$ в случае декодера над $GF(64)$, длины в остальных случаях подбираются так, чтобы количество бит оставалось таким же, т.е. $n = 1020$ в случае декодера над $GF(8)$ и $n = 3060$ в случае декодера над

[2] в англоязычной литературе используется термин “belief propagation”

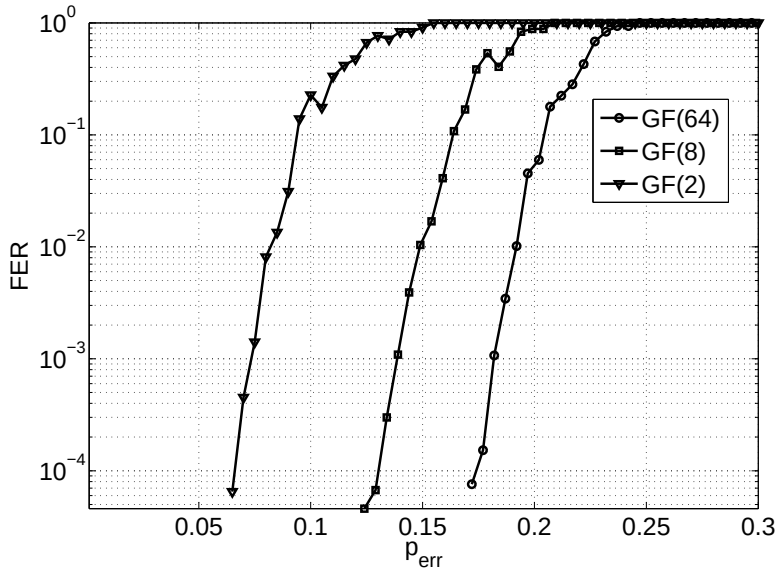

Рис. 5. Вероятность ошибки на блок, qСК при $q = 64$

$GF(2)$ (длины заданы в символах соответствующих полей).

В *параграфе 2.3.3* приведено сравнение недвоичных МПП-кодов с двоичными в канале с аддитивным белым гауссовским шумом (АБГШ) при разных модуляциях. Параметры кодов – $R = 0,5$; $\ell = 3$; $n_0 = 6$; длина $n = 1020$ в случае декодера над $GF(8)$ и $n = 3060$ в случае декодера над $GF(2)$ (длины заданы в символах соответствующих полей).

На рис. 6 показано сравнение при использовании фазовой манипуляции(ФМн) с $M = 8$. При малых E_b/N_0[3] лучше оказывается двоичный код. Это можно объяснить так: входные символы записаны в коде Грэя, поэтому доля битовых ошибок оказывается меньше (примерно в $\log_2 q$ раз), чем доля символьных. Однако в случае больших E_b/N_0 выигрывает недвоичный код.

На рис. 7 показано сравнение при использовании частотно-позиционной модуляции(ЧПМ) с $M = 8$. В этом случае МПП-код над $GF(8)$ оказывается гораздо лучше двоичного.

В *разделе 2.4* приводятся выводы к главе 2.

Выводы к главе 2

- Улучшена асимптотическая оценка доли ошибок, гарантированно исправимых МПП-кодами над полем $GF(q)$ с помощью алгоритма декодирования, имеющего сложность $O(n \log_2 n)$.

- Предложен алгоритм декодирования с вводом стираний, способный работать в канале с ошибками и стираниями. Этот алгоритм работает лучше мажоритарного алгоритма при условии наличия только ошибок в принятом слове.

[3] под E_b/N_0 понимается отношение сигнал/шум на информационный бит

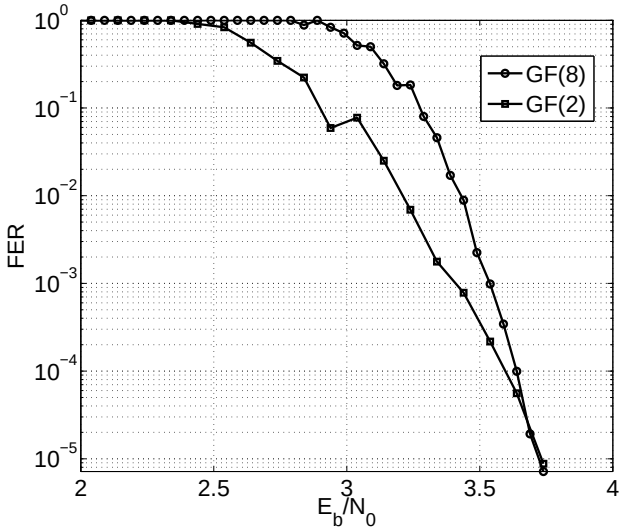

Рис. 6. Вероятность ошибки на блок, АБГШ, ФМн

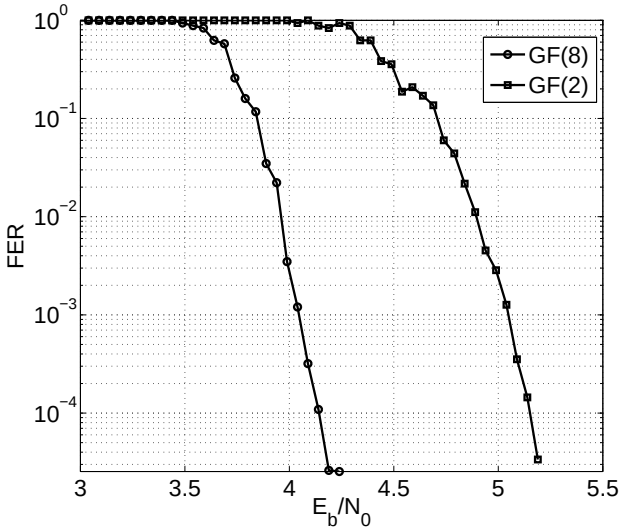

Рис. 7. Вероятность ошибки на блок, АБГШ, ЧПМ

- Проведено исследование алгоритмов $\mathscr{A}_{BP}$ и $\mathscr{A}_*$ в различных каналах при разных модуляциях. Показано, что $\mathscr{A}_{BP}$ лучше алгоритма $\mathscr{A}_*$. В то же самое время он гораздо медленнее последнего, поэтому он не подходит для приложений, где важна высокая скорость.

- Методом имитационного моделирования показано, что МПП-коды над полем $GF(q)$ гораздо более эффективны нежели двоичные в qСК и канале с АБГШ при ЧПМ.

Результаты второй главы опубликованы в работах [1, 2, 5–7, 9].

Третья глава посвящена применению недвоичных МПП-кодов в сигнально-кодовой конструкции для системы множественного доступа. Результирующая система строится на базе технологий мультиплексирования с использованием ортогональных частот (OFDM) и псевдослучайной перестройки рабочей частоты (ППРЧ). Эта система позволяет одновременно работать очень большому числу пользователей, что очень важно для таких систем как, например, LTE и WiMAX.

В *разделе 3.1* приводится введение к главе 3.

В *разделе 3.2* приводится описание СКК для системы множественного доступа, использующей бесшумный векторный дизъюнктивный канал. Обозначим число активных пользователей через S. Будем предполагать, что все пользователи используют один и тот же конечный алфавит – символы поля $GF(q)$.

Передача. Каждый пользователь кодирует передаваемую информацию q-ичным (n, k, d) кодом C (все пользователи используют один и тот же код). Рассмотрим процесс передачи сообщения i-м пользователем. Пусть передается кодовое слово c_i, каждому символу c_i ставится в соответствие двоичный

вектор длины q и веса 1, причем единица находится в позиции, соответствующей передаваемому элементу поля (предполагается, что элементы вектора занумерованы элементами поля и этот порядок фиксирован и одинаков для всех пользователей). Обозначим таким образом построенную матрицу через $\mathbf{C}_i$. Передача происходит посимвольно. Перед передачей каждого двоичного вектора в канал выполняется случайная перестановка. Перестановки, используемые каждым из пользователей, выбираются равновероятно и независимо из всего множества возможных перестановок (при передаче каждого символа используется своя перестановка).

Интервал времени за которое передается один вектор будем называть тактом. Будем предполагать, что в системе используется тактовая синхронизация (наличие блочной синхронизации не требуется).

Прием. Базовая станция последовательно принимает сообщения от всех пользователей. Рассмотрим процесс приема сообщения, пришедшего от i-го пользователя. Будем полагать, что принимающая станция засинхронизирована с передатчиком каждого из пользователей. Это означает, что приемнику известны n столбцов, которые соответствуют кодовому слову, переданному i-м пользователем. При приеме каждого столбца выполняется перестановка, обратная той, что использовал i-ый пользователь при передаче. Таким образом, получим матрицу

$$\mathbf{Y}_i = \mathbf{C}_i \vee \left(\bigvee_{m=1:S, m \neq i} \mathbf{X}_m \right),$$

где $\mathbf{C}_i$ – это матрица, соответствующая кодовому слову, переданному i-м пользователем, а матрицы $\mathbf{X}_m, m = 1 : S, m \neq i$ – это результат действия остальных пользователей. Заметим здесь, что матрицы $\mathbf{X}_m$ могут не включать целиком кодовые слова остальных пользователей.

Рассмотрим кодовое слово $c_t \in C$. Построим матрицу $\mathbf{C}_t$, соответствующую c_t способом, описанным выше. Предположение о том, что кодовое слово $c_t \in C$ было передано i-м пользователем, можно считать выполненным только в том случае если выполняется

$$\mathbf{C}_t \wedge \mathbf{Y}_i = \mathbf{C}_t, \tag{3}$$

где $\wedge$ означает поэлементную конъюнкцию матриц.

Для декодирования необходимо проверить выполнение условия (3) для всех кодовых слов используемого кода. В случае если список кодовых слов, которые удовлетворяют условию декодирования, состоит из одного слова, то это слово и есть слово переданное рассматриваемым пользователем, если же список состоит из нескольких слов, то принимается решение об отказе от

декодирования (в рассматриваемом случае ошибочное декодирование невозможно).

В *разделе 3.3* получена нижняя асимптотическая граница суммарной относительной скорости передачи для вышеописанной системы. Для того, чтобы получить эту оценку, построены оценки вероятности отказа от декодирования (обозначим ее через p_* и потребуем $p_* < 2^{-cn}, c > 0$), необходимых кодового расстояния и длины кода.

Скорость передачи информации от одного активного пользователя (в битах на один такт) равна

$$R_i(q, S, k, c) = \frac{k}{n(q, S, k, c)} \log_2 q.$$

Суммарная скорость передачи всех активных пользователей может быть найдена как

$$R_\Sigma(q, S, k, c) = \sum_{i=1}^{S} R_i(q, S, k, c) = S \frac{k}{n(q, S, k, c)} \log_2 q.$$

Пусть $S = \gamma q$, введем теперь асимптотическую величину

$$\rho(\gamma, k, c) = \lim_{q \to \infty} \frac{R_\Sigma\left(q, \gamma q, k, c\right)}{q},$$

характеризующую количество информации, передаваемой всеми активными пользователями в расчете на один подканал.

Теорема 3.2 При $\gamma < -\ln\left(1 - 2^{-c}\right)$ справедливо соотношение

$$\rho\left(\gamma, k, c\right) \geqslant -\gamma \left(\log_2\left(1 - e^{-\gamma}\right) + c\right).$$

Л. Вильхельмссон и К. Ш. Зигангиров показали, что при некоординированной передаче в случае равномерного распределения вероятностей символов на входе (как и в рассматриваемом случае) $\rho(\gamma, k, c) \leqslant -\gamma \log_2\left(1 - e^{-\gamma}\right)$. Предложенная конструкция позволяет обеспечить асимптотическую относительную суммарную скорость передачи сколь угодно близкую к этой верхней границе при $c = \varepsilon$.

В *разделе 3.4* приводится описание модифицированной СКК на основе недвоичных МПП-кодов для системы множественного доступа, использующей векторный канал с АБГШ.

Для борьбы с шумом необходим длинный код, декодирование которого по минимуму расстояния неприменимо на практике. В связи с этим конструкция из *раздела 3.2* в этом случае не подходит. Приведем описание отличий модифицированной СКК.

Основные отличия:

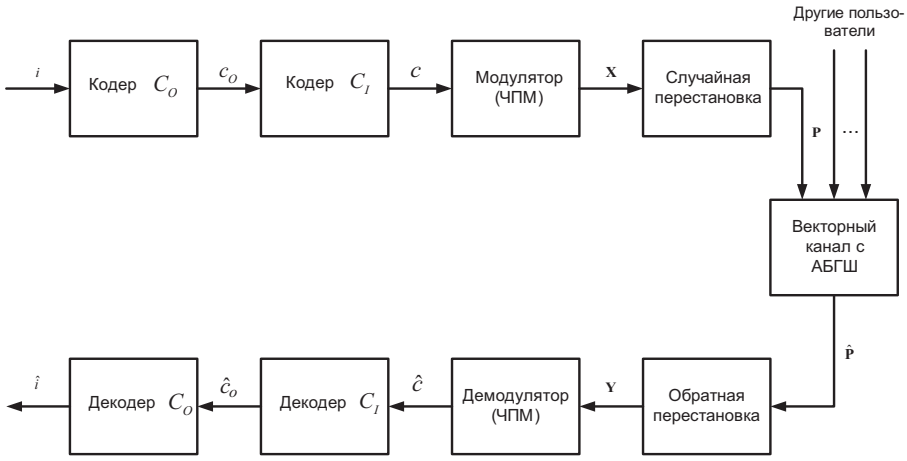

Рис. 8. Блок схема предложенной СКК

- При передаче используем ЧПМ с $M = q$;
- Для борьбы с шумом добавлен внешний МПП-код на полем $GF(Q)$, где $Q = q^k$. Таким образом код из *раздела 3.2* становится внутренним (в качестве алгоритма декодирования используем алгоритм $\mathscr{A}_{BP}$);
- Внутренний код будем декодировать по максимуму правдоподобия, а не по минимуму расстояния.

На рис. 8 приведена блок-схема предложенной системы.

В *разделе 3.5* приводится исследование вышеописанной СКК методом имитационного моделирования. Зафиксируем следующие параметры: $Q = 64$; $N = 510$; $R = 0,5$; $q = 64$, $n = 8$, $r = 0,125$ (в качестве внутреннего кода используется код с повторением над $GF(64)$). На рис. 9 приведены полученные результаты: четыре зависимости при $S = 4, 8, 12, 16$. Пусть требуется, чтобы вероятность ошибки на блок была меньше 10^{-4}, в табл. приведены значения E_b/N_0, при которых это требование выполняется. Заметим здесь, что в этом примере система эффективна даже, когда число активных пользователей составляет четверть от числа подканалов.

В *разделе 3.5* приводится выводы к главе 3.

Выводы к главе 3

- Разработана СКК для системы множественного доступа, использующей бесшумный векторный дизъюнктивный канал. Получена нижняя оценка относительной суммарной скорости передачи для таким образом построенной системы множественного доступа;
- Разработана СКК на основе недвоичных МПП-кодов для системы множественного доступа, использующей векторный канал с АБГШ. С помощью имитационного моделирования показана эффективность этой системы.

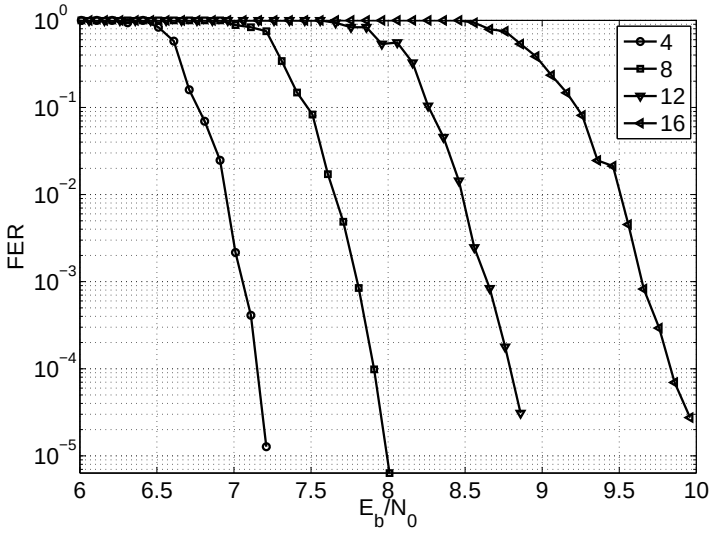

Рис. 9. Вероятность ошибки на блок от E_b/N_0

Таблица

Зависимость E_b/N_0 от S

S	4	8	12	16
E_b/N_0, дБ	7,16	7,91	8,81	9,86

Результаты третьей главы опубликованы в работах [4, 8].

В Заключении обобщены полученные в диссертационной работе результаты и сделаны выводы.

Основные результаты:

1. Построены верхняя и нижняя границы минимального кодового расстояния для МПП-кодов над полем $GF(q)$;

2. Предложен мажоритарный алгоритм декодирования МПП-кодов над полем $GF(q)$;

3. Улучшена асимптотическая оценка доли ошибок, гарантированно исправимых с помощью алгоритма, имеющего сложность $O(n \log_2 n)$;

4. Предложен алгоритм декодирования с вводом стираний, способный работать в канале с ошибками и стираниями. Этот алгоритм лучше мажоритарного алгоритма при условии наличия только ошибок в принятом слове;

5. Показано, что МПП-коды над полем $GF(q)$ гораздо более эффективны, чем двоичные, в qСК и канале с АБГШ при ЧПМ;

6. Разработана СКК для системы множественного доступа, использующей бесшумный векторный дизъюнктивный канал. Для этой системы получена нижняя оценка относительной суммарной скорости передачи;

7. Разработана модифицированная СКК на основе недвоичных МПП-кодов для системы множественного доступа, использующей векторный канал с АБГШ. Показана эффективность этой системы.

Список публикаций

1. Фролов А. А., Зяблов В. В. Асимптотическая оценка доли ошибок, исправляемых q-ичными МПП-кодами // Пробл. передачи информ. 2010. Т. 46, № 2. С. 47–65.

2. 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.

3. Фролов А. А., Зяблов В. В. Границы минимального кодового расстояния для недвоичных кодов на двудольных графах // Пробл. передачи информ. 2011. Т. 47, № 4. С. 27–42.

4. Зяблов В. В., Фролов А. А. Сигнально-кодовая конструкция для системы множественного доступа, использующей векторный канал с аддитивным белым гауссовским шумом // Информационные процессы. 2012. Т. 12, № 1. С. 98–104.

5. Frolov A., Zyablov V. The Application of Q-ary LDPC-codes for Fiber Optic Lines // Proc. of XII International Symposium on Problems of Redundancy in Information and Control Systems, Saint-Petersburg, Russia. 2009. — May. P. 121–125.

6. Зяблов В. В., Фролов А. А. Сравнение корректирующей способности МПП-кодов с кодами-компонентами разной избыточности // Информационные технологии и системы (ИТиС'09), пос. д/о Бекасово, Россия. 2009. — Дек. С. 160–163.

7. Зяблов В. В., Фролов А. А. Исследование корректирующих свойств МПП-кодов с кодом-компонентом Рида-Соломона // Информационные технологии и системы (ИТиС'10), г. Геленджик, Россия. 2010. — Сент. С. 74–78.

8. Осипов Д. С., Фролов А. А., Зяблов В. В. Сигнально-кодовая конструкция на базе q-ичных кодов для защиты от сосредоточенных помех // Информационные технологии и системы (ИТиС'11), г. Геленджик, Россия. 2011. — Окт. С. 167–173.

9. Frolov A., Zyablov V. Insertion of Erasures as a Method of Q-ry LDPC Codes Decoding // Proc. of XII International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2010), Akademgorodok, Novosibirsk, Russia. 2010. — Sept. P. 138–143.

10. Frolov A., Zyablov V. Upper and Lower Bounds on the Minimum Distance of Expander Codes // Proc. of IEEE International Symposium on Information Theory (ISIT 2011), Saint-Petersburg, Russia. 2011. — Jul./Aug. P. 1302–1306.