Федеральное государственное бюджетное учреждение науки Институт проблем передачи информации им. А.А. Харкевича Российской академии наук

На правах рукописи

Крещук Алексей Андреевич

Разработка каскадных сигнально-кодовых конструкций для систем многоантенных передачи и приёма

05.13.17 – Теоретические основы информатики

ДИССЕРТАЦИЯ

на соискание ученой степени

кандидата технических наук

Научный руководитель

доктор технических наук

Зяблов Виктор Васильевич

Москва – 2015

Оглавление

Введение

Актуальность темы исследования. Современные стандарты беспроводной связи, такие как LTE, WiMAX и WiFi, предусматривают использование нескольких приёмных и передающих антенн для увеличения пропускной способности. Эти стандарты предусматривают использование каскадной конструкции, внутренними кодами которой являются пространственно-временные коды (то есть коды для многоантенных систем, построенные над бесконечными полями), а внешними — известные коды над конечными полями.

Современные сигнально-кодовые конструкции для систем многоанетных передачи и приёма, также называемые пространственно-временными кодами, начали своё развитие в 90х годах прошлого века. Первой такой конструкцией являются коды, предложенные С. Аламоути в 1998 году. Данная конструкция позволяла эффективно использовать две передающие антенны для уменьшения вероятности ошибки в канале, и при этом обладала низкой сложностью приёма. Она была обобщена в 1999 В. Тарох, Х. Джафархани и А. Р. Кальдербанком для большего числа антенн. Кроме того, было доказано, что предложенные сигнально-кодовые конструкции являются оптимальными в классе ортогональных пространственно-временных кодов. Дальнейшее развитие теории кодирования привело к появлению пространственно-временных кодов, имеющих более высокую скорость, но декодируемых с полиномиальной по количеству антенн сложностью. Одним из таких кодов был Golden код, предложенный в 2005 году J.-C. Belfiore, G. Rekaya и E. Viterbo. Данный код так же предназначен для систем, имеющий две передающие антенны, но имеет вдвое большую скорость передачи данных, чем конструкция Аламоути.

На практике пронстравенно-временные коды используют в составе каскадных конструкций. В 1973 году Э. Л. Блохом и В. В. Зябловым были предложены линейные обобщённые каскадные коды. Использование обобщённых каскадных конструкций может позволить повысить корректирующую способность всей си-

стемы. В 2009 году L. Luzzi, G. R.-B. Othman, J.-C. Belfiore и E. Viterbo предложили обобщённую каскадную конструкцию для многоантенных систем передачи и приёма. Однако предложенная ими конструкция имела малую длину, и потому не позволяла достичь малых вероятностей ошибки на блок.

Таким образом актуальной является задача построения обобщённых каскадных конструкций для систем многоантенных передачи и приёма, обладающей высокой корректирующей способностью при низкой сложности кодирования и декодирования.

Цели и задачи диссертационной работы: Цель диссертационной работы состоит в разработке обобщённых каскадных кодов, внутренними кодами которых являются пространственно-временные коды, а внешними — произведения кодов Рида-Соломна и коды с обобщённой локализацией ошибок, а также разработка улучшенных алгоритмов декодирования полученных сигнально-кодовых конструкций; исследовании вероятности неправильного приёма для данной конструкции в каналах многоантенной передачи и приёма с независимыми релеевскими замираниями.

Для достижения поставленных целей необходимо решить следующие задачи:

1. Адаптировать алгоритмы декодирования пространственно-временных кодов Golden и DAST для декодирования внутренних кодов обобщённых каскадных конструкций.

2. Предложить обобщённую каскадную конструкцию с внутренними пространственно-временными Golden или DAST кодами, внешними кодами которых являются произведения кодов Рида-Соломона или коды с обобщённой локализацией ошибок, и исследовать её корректирующую способность.

Научная новизна.

1. Исследованы вероятностные характеристики обобщённых каскадных кодов с различными внутренними пространственно-временными кодами с различным количеством приёмных и передающих антенн. Полученные результаты позволяют быстро выбирать параметры обобщённых каскадных конструкций в соответствии для работы в заданном канале.

2. Разработан новый алгоритм декодирования произведений кодов. Его использование позволяет увеличить корректирующую способность кодов-произведений при незначительном увеличении сложности.

3. Предложены и исследованы новые пространственно-временные коды, свободные от перестановок, построенные на базе матриц Адамара. Разработаны алгоритмы построения кодов с заданным расстоянием, длиной и числом передающих антенн.

Теоретическая и практическая значимость. Исследовано применение произведений кодов Рида-Соломона и кодов с обобщённой локализацией ошибок в качестве внешних кодов предложенных обобщённых каскадных систем. Предложенная методика выбора параметров кодов с обобщённой локализацией ошибок позволяет не только сократить время подбора параметров каскадной системы, но и за разумной время построить целое семейство сигнально-кодовых конструкций для целого диапазона различных каналлов. Предложенный новый алгоритм декодирования произведений кодов улучшает их корректирующую способность при малом увеличении сложности.

Предложеная метрика надёжности для пространственно-временных кодов, декодируемых при помощи сферического декодера, позволяет использовать их в каскадных и обобщённых каскадных конструкциях, декодируемых по обобщённому минимальному расстоянию.

Предложена сигнально-кодовая конструкция, достигающая вероятности неправильного приёма 10^{-8}, при отношении сигнал-шум 13 дБ на бит, при использовании двух передающих и двух приёмных антенн.

Полученные вероятностные характеристики обобщённых каскадных систем с внутренними пространственно-временными кодами позволяют упростить проектирование и настройку конкретных конструкций под требования заказчика. Разработаные алгоритмы кодирования и декодирования предложенных сигнально-кодовых конструкций позволяют использовать их в реальных системах.

Положения, выносимые на защиту:

1. Построены верхняя граница мощности предложенных кодов, свободных от перестановок. Построены коды, лежащие на предложенной верхней границе. Построена нижняя граница мощности кодов, свободных от перестановок, основанная на границе Гилберта.

2. Показана эффективность предложенной метрики надёжности принятых сообщений для внесения стираний.

3. Показано, что использование предложенной обобщённой каскадной конструкции даёт выигрыш в 0.5 дБ по сравнению с каскадной конструкцией с тем же внутренним и внешним кодом Рида-Соломона в некоторых условиях.

4. Показано, что предложенный декодер произведения кодов имеет вероятность неправльного декодирования на два порядка меньшую, чем известный ранее итеративный в некоторых условиях. Построена нижняя граница корректирующей способности итеративного декодера.

Апробация результатов. Основные результаты диссертации докладывались на следующих конференциях: XIII International Symposium on Problems of Redundancy in Information and Control Systems (2012); XIV International Symposium on Problems of Redundancy in Information and Control Systems (2014); XIV International Workshop on Algebraic and Combinatorial Coding Theory (2014); The 8th International Symposium on Turbo Codes & Iterative Information Processing (2014); Конференциях молодых ученых и специалистов

ИППИ РАН «Информационные технологии и системы» (2010–2015). Кроме того, основные результаты докладывались на семинарах по теории кодирования в ИППИ РАН.

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

Личный вклад автора. Личное участие автора в получении результатов, изложенных в диссертации. Постановка изложенных в диссертации задач была сделана научным руководителем аспиранта д.т.н. В.В. Зябловым. Доказательства и обоснования полученных в диссертации результатов, математические выкладки, численные расчеты выполнены лично автором. В совместных публикациях научному руководителю В.В. Зяблову принадлежат постановки задач и указания основных направлений исследований, а основные результаты, выкладки и численные расчеты выполнены диссертантом.

В работе [3] соавтору принадлежит постановка задачи, а основной результат был получен диссертантом. В работе [10] соавтору Е. Рябинкину принадлежит техническая поддержка в проведении компьютерного моделирования на кластере. В работе [1] соавтору А.А. Давыдову принадлежат результаты, связанные с кодами, свободными от повторений, а также алгоритм А построения кодов, свободных от перестановок.

Структура и объем диссертации. Диссертация состоит из введения, 3 глав, заключения, библиографии и 1 приложения. Общий объем диссертации 96 страниц, включая 16 рисунков. Библиография включает 51 наименований на 5 страницах. Приложение изложено на 5 страницах.

Глава 1

Системы с многими приёмными и передающими антеннами

1.1. Введение

В данной работе представлена новая сигнально-кодовая конструкция для систем многоантенной передачи и приёма (МАПП, англ. MIMO – Multiple Input Multiple Output). Такие системы содержат несколько приёмных и передающих антенн, а коэффициенты передачи между каждой парой антенн статистически независимы. Одновременное использование нескольких антенн позволяет увеличить скорость передачи и уменьшить вероятность ошибки при приёме. Такие системы также называют системами с пространственным разнесением, по аналогии с системами с временным или частотным разнесением. В [11] системы с разнесением описаны более подробно. Для эффективной передачи по нескольким антеннам недостаточно использовать только пространственное разнесение. Сигнально-кодовые конструкции, использующие одновременно пространственное и временное разделение, называются пространственно-временными кодами.

Термин пространственно-временные коды был предложен в марте 1998 года [12], хотя задача построения сигнально-кодовой конструкции для систем многоантенной передачи и приёма была известна давно. В октябре того же года была предложена [13] оптимальная ортогональная конструкция для случая двух передающих антенн. В 1999 году была предложен [14] алгоритм построения ортогональных пространственно-временных кодов для произвольного числа передающих антенн, который, однако, не позволял получить коды с максимально возможным разнесением. Также были предложены метрики расстояния, определяющие вероятность ошибочного приёма. В каналах с большим отношением сигнал-шум такой метрикой является минимальное детерминантное расстояние.

Ортогональные коды имеют простой декодер и подходят для систем с одной приёмной антенной, однако неортогональные коды имеют более высокую скорость. В 2003 году был предложен [15] способ построения неортогональных пространственных кодов, минимальное детерминантное расстояние которых не становится бесконечно малым при увеличении порядка модуляции. В 2005 году [16] был предложен Golden код, обдающий лучшим минимальным детерминантным расстоянием. Данный код подходит для систем с двумя передающими и не менее чем двумя приёмными антеннами. В 2009 году был предложен [17] обобщённый каскадный код, внутренний код которого является Golden кодом.

Другие пространственно-временные коды и смежные проблемы исследовались в работах [15, 18–29]. В работах [30–32] приводится обзор различных кодовых конструкция для систем многоантенной передачи и приёма.

Существующие сигнально-кодовые конструкции для систем МАПП имеют невысокую длину кода. Их удобно использовать в каскадных конструкциях, но при отсутствии внещнего кода его применение ограничено. Рассматриваемая в работе конструкция [6] позволяет строить коды, обладающие большим Евклидовым кодовым расстоянием, растущим пропорционально квадратному корню из длины кода. Квадрат Евклидова расстояние, часто используемый как критерий “качества” кода, в предложенной сигнально кодовой конструкции пропорционален длине кода.

Рассматриваемая система многоантенной передачи и приёма содержит один передатчик с N антеннами, один приёмник с M антеннами и канал с N входами и M выходами. Сигналы с разных передающих антенн интерферируют, поэтому на каждую приёмную антенну приходит линейная комбинация сигналов, отправленных с каждой передающей антенны. При этом шум не зависит от коэффициентов затухания между каждой парой антенн, и имеет одинаковую мощность для всех приёмных антенн. Опишем эту модель канала математически.

1.1.1. Модель канала

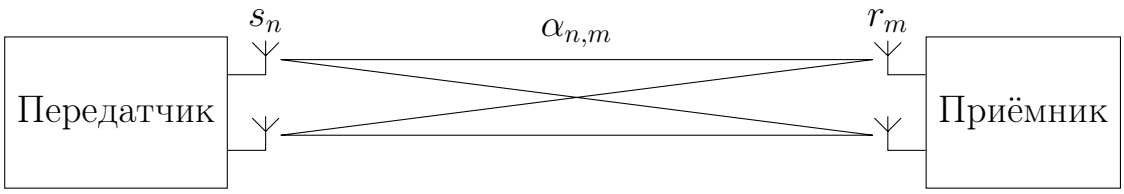

Рис. 1.1. Канал передачи данных.

Рассмотрим канал с многими входами $c_n \in \mathbb{C}, n = \overline{1, N}$ и выходами $r_m \in \mathbb{C}, m = \overline{1, M}$ определяемый следующим выражением:

$$r_m = \sum_{n=1}^{N} \alpha_{n,m} c_n + \eta_m, \tag{1.1}$$

где $\alpha_{n,m} \in \mathbb{C}$ — коэффициент передачи канала, а $\eta_m \in \mathbb{C}$ — шум. В данной работе $\alpha_{n,m}$ и η_m — независимые гауссовские случайные величины с нулевым средним, при чём средняя мощность $\alpha_{n,m}$ равна 1. Данный канал изображён на рис. 1.1. Физическое обоснование представленной модели канала приведено в [30].

В данной работе рассматривается случай, когда коэффициенты передачи канала известны на приёмнике, но не на передатчике.

Так же, как и в случае алгебраических кодов, мы будем использовать символы, переданные за T временных отсчётов, для передачи одного кодового слова. При этом мы предполагаем стационарность канала на времени передачи одного кодового слова. Таким образом мы можем описать канал следующим выражением:

$$r_{t,m} = \sum_{n=1}^{N} \alpha_{n,m} c_{t,n} + \eta_{t,m}, \quad m = 1, \ldots, M, \quad t = 1, \ldots, T \tag{1.2}$$

Такой канал называется Релеевским каналом или каналом с Релеевскими замираниями. Подмножество передаваемых слов называется пространственно-временным кодом.

Для описания свойств данного канала, нам необходимо представить (1.2) в матричной форме. Когда мы описывать критерии проектирования кодов, мы будем использовать более естественную матричную форму, в которой кодовые слова являются матрицами размера $T \times N$. Однако, для описания алгебраической структуры кода и алгоритма декодирования мы приведём другое представление канала, в котором кодовые слова являются столбцами высоты NT.

В простом матричном представлении канала мы вводим следующие матрицы: матрицы кодовых слов $\mathbf{C} = \|c_{t,n}\|$ размера $T \times N$, матрица коэффициентов передачи канала $\mathbf{H} = \|\alpha_{n,m}\|$ размера $N \times M$, матрица полученного слова $\mathbf{r} = \|r_{t,m}\|$ размера $T \times M$ и матрица шума $\mathcal{N} = \|\eta_{t,m}\|$ размера $T \times M$. Таким образом, выражение (1.2) можно представить в виде:

$$\mathbf{r} = \mathbf{C} \cdot \mathbf{H} + \mathcal{N} \tag{1.3}$$

При декодировании по максимуму правдоподобия необходимо минимизировать выражение [30, раздел 3.2]:

$$\min_{\mathbf{C} \in \mathcal{C}} \mathrm{Tr}[(\mathbf{r} - \mathbf{C} \cdot \mathbf{H})^{\mathrm{H}} (\mathbf{r} - \mathbf{C} \cdot \mathbf{H})], \tag{1.4}$$

где $\mathcal{C}$ — пространственно-временной код, то есть множество всех кодовых слов.

1.2. Коды без перестановок (PRF-коды)

Пусть $\mathcal{N} = \mathbf{0}$. Тогда $\mathbf{r}_1 - \mathbf{r}_2 = (\mathbf{C}_1 - \mathbf{C}_2)\mathbf{H}$. Таким образом, для различения двух разных принятых сигналов $\mathbf{r}$, необходимо и достаточно, чтобы правая часть уравнения не равнялась нулю при любом допустимом количестве приёмных антенн. В данном разделе мы рассмотрим коды, работающие при любом количестве приёмынх антенн, а потому потребуем, чтобы матрицы $\mathbf{C}_1$ и $\mathbf{C}_2$ различались на приёмнике при одной приёмной антенне. При этом $M = 1$, $\mathbf{r}$ – столбец длины T, $\mathcal{N}$ – столбец длины N. Очевидно, что при $\mathcal{N} = 0$ передача невозможна. Потребуем, чтобы, когда все коэффициенты передачи канала от-

личны от нуля, любые две кодовые матрицы различались на приёмнике. Сформулируем это рассуждения в качестве необходимого критерия выбора кода.

В качестве сигнально-кодовой конструкции используется конечный набор $\mathcal{C}$ комплексных $(T \times N)$-матриц $\mathbf{C}$, удовлетворяющий условию декодируемости:

$$\forall \mathbf{C}_1, \mathbf{C}_2 \in \mathcal{C}, \forall \alpha \in \mathbb{C}^N : \forall j, \alpha_j \neq 0 \rightarrow \mathbf{C}_1\alpha \neq \mathbf{C}_2\alpha, \tag{1.5}$$

где α_j – элементы столбца $\mathcal{N}$.

Введём понятие скорости кода для систем МАПП. Предложенный код является нелинейным. Скоростью нелинейного кода $\mathcal{C}$ длины T называется величина $v = \frac{\log_2 |\mathcal{C}|}{T}$. Данное определение учитывает равенство $s_i^t = \pm 1$.

Рассмотрим только те коды, в словах которых столбцы принадлежат некоторому упорядоченному набору ортогональных столбцов. В данной работе в качестве такого набора используются столбцы $(T \times T)$-матрицы Адамара с

$$T = 2^m \geq N.$$

Мы используем ниже конечное поле с 2^m элементами. Отметим, что рассматриваемый подход к построению сигнально-кодовой конструкции применим и в тех случаях, когда T не является степенью двойки.

Определение 1. Назовём код $\mathcal{C}$ *PRF-кодом* (Permutations and Repetitions Free code), если никакие два различных его кодовых слова не могут быть получены друг из друга перестановкой столбцов, и ни одно его слово не содержит повторяющихся столбцов.

Определение 2. Назовём код $\mathcal{C}$ *PF-кодом* (Permutations Free code), если никакие два различных его кодовых слова не могут быть получены друг из друга перестановкой столбцов.

Слова PF-кода могут иметь повторяющиеся столбцы.

Лемма 1. *Пусть столбцы слов* $\mathbf{C}$ *кода* $\mathcal{C}$ *являются столбцами* $(T \times T)$*- матрицы Адамара. Тогда для выполнения условия декодируемости* (1.5) *необходимо, чтобы код* $\mathcal{C}$ *был PF-кодом, и достаточно, чтобы код* $\mathcal{C}$ *был PRF-кодом.*

Доказательство леммы дано в разделе 1.3.

Отметим, что не всякий PF-код удовлетворяет условию (1.5). Тем не менее PF-коды могут использоваться, когда параметры передачи не позволяют построить PRF-код нужной мощности.

Таким образом, для систем МАПП мы ввели *новую сигнально-кодовую конструкцию*, задаваемую *матричным кодом* $\mathcal{C}$, и показали, что для выполнения условия декодируемости достаточно, чтобы код $\mathcal{C}$ был PRF-кодом. С некоторой потерей корректирующей способности допустимо также, чтобы код $\mathcal{C}$ был PF-кодом.

Дальнейшая *цель работы* найти *методы построения PRF- и PF-кодов* достаточно большой мощности и провести численное *моделирование* построенных кодов для оценки их эффективности.

Для решения задачи построения кодов мы вводим взаимно-однозначное *отображение матричного кода* $\mathcal{C}$ *в векторный код* $\mathcal{S}$ и затем используем естественные для векторного представления методы, оказавшиеся достаточно эффективными.

Пусть q – простое число или степень простого числа. Обозначим через F_q поле Галуа из q элементов. Пусть $F_q^* = F_q \backslash \{0\}$. Обозначим через F_q^n пространство векторов длины n над полем F_q.

Пронумеруем столбцы $(T \times T)$-матрицы Адамара $\mathcal{H}$ элементами поля F_T, взятыми в некотором фиксированном порядке. Тогда $\mathcal{H} = \|\mathbf{h}_0\mathbf{h}_1 \dots \mathbf{h}_{T-1}\|$, где $\mathbf{h}_i$ – столбец матрицы Адамара и $\{0, 1, \dots, T-1\} = F_T$. Кодовое слово $\mathbf{C}$, составленное из N столбцов матрицы Адамара, может быть записано в виде

$$\mathbf{C} = \|\mathbf{h}_{i_1}\mathbf{h}_{i_2} \dots \mathbf{h}_{i_N}\|, \quad i_1, i_2, \dots, i_N \in F_T.$$

Поставим в соответствие каждому кодовому слову $\mathbf{C}$ вектор $\mathbf{s} \in F_T^N$, компоненты которого соответствуют номерам столбцов кодового слова в матрице Адамара. Обозначим данное отображение $\mathcal{L}$. Из вышесказанного следует, что $\mathcal{L}$ – взаимно-однозначное отображение, которое может быть представлено сле-

дующим образом:

$$\mathcal{L}(\mathbf{C}) = \mathcal{T}(\|\mathbf{h}_{i_1}\mathbf{h}_{i_2}\dots\mathbf{h}_{i_N}\|) = \mathbf{s} = (i_1, i_2, \dots, i_N) \in F_T^N. \tag{1.6}$$

Векторы $\mathbf{s}$ формируют код $\mathcal{S}$.

Далее в этой работе под PF- и PRF-кодами мы подразумеваем как коды $\mathcal{C}$, слова которых являются $(T \times N)$-матрицами, так и соответствующие им коды $\mathcal{S} \subset F_T^N$.

Алгоритмы построения кодов разрабатываются для векторного представления. При этом PF- и PRF-коды строятся и как подмножества слов кода Рида-Соломона (РС-кодов), и как подмножества векторного пространства F_T^N без привязки к РС-кодам.

В разделе 1.3 рассмотрены отображения $\mathcal{L}$ и $\mathcal{L}^{-1}$. Представлена формула, по которой изменяется расстояние между кодовыми словами при использовании этих отображений. В разделе 1.4 представлен общий анализ PF- и PRF-кодов и предложены методы их построения. В разделе 1.5 эффективность предлагаемых методов проиллюстрирована на примерах построения конкретных PF- и PRF-кодов. Далее в разделе 1.6 описывается метод декодирования по максимуму правдоподобия, а также анализируются различия между декодированием PF- и PRF-кодов. В разделе 1.8 описано численное моделирование корректирующей способности некоторых кодов из раздела 1.5, и приведены результаты этого моделирования в форме графиков зависимости корректирующей способности от соотношения сигнал-шум. Там же приводится анализ этих результатов. В приложении рассмотрены подмножества поля F_{2^m} с фиксированной суммой элементов, использование которых полезно при построении PF- и PRF-кодов.

1.3. Отображение $\mathcal{L}$ и кодовые расстояния кодов $\mathcal{C}$ и $\mathcal{L}(\mathcal{C})$

Доказательство леммы 1. Покажем, что всякий PRF-код удовлетворяет условию (1.5), то есть докажем достаточность. Пусть $\mathcal{H}$ – матрица Адамара.

Домножим уравнение (1.5) на матрицу $\frac{1}{T}\mathcal{H}^T$, где T – знак транспонирования. Матрица $\frac{1}{T}\mathcal{H}^T\mathbf{C}_u$ является $(0,1)$-матрицей и содержит одну единицу в каждом столбце. Положение этой единицы определяется индексом соответствующего столбца матрицы $\mathbf{C}_u$ в матрице $\mathcal{H}$. Строка матрицы $\frac{1}{T}\mathcal{H}^T\mathbf{C}_u$ либо содержит точно одну единицу (поскольку повторяющихся столбцов в $\mathbf{C}_u$ нет), либо является нулевой. Нулевые строки соответствуют отсутствующим в $\mathbf{C}_u$ столбцам из $\mathcal{H}$. Так как различные матрицы $\mathbf{C}_u$ не могут быть получены друг из друга перестановкой столбцов, то в $\mathbf{C}_1$ имеется столбец, не встречающийся в $\mathbf{C}_2$, и поэтому существует такой номер i, что i-я строка матрицы $\frac{1}{T}\mathcal{H}^T\mathbf{C}_1$ненулевая, а i-я строка матрицы $\frac{1}{T}\mathcal{H}^T\mathbf{C}_2$ нулевая. Поскольку $\alpha_j \neq 0, \forall j$, то $(\frac{1}{T}\mathcal{H}^T\mathbf{C}_1\alpha)_i \neq 0$ (что обеспечено наличием точно одной единицы в ненулевой строке), тогда как $(\frac{1}{T}\mathcal{H}^T\mathbf{C}_2\alpha)_i = 0$, где $(\mathbf{e})_i$ – i-я компонента вектора $\mathbf{e}$. Следовательно, условие декодируемости (1.5) выполнено.

Из вышесказанного следует также, что для выполнения условия (1.5) код $\mathcal{C}$ *необходимо* должен быть PF-кодом. Для доказательства достаточно взять столбец α, все компоненты которого одинаковы. Если матрица $\mathbf{C}_2$ получена из $\mathbf{C}_1$ перестановкой столбцов, то, очевидно, условие (1.5) нарушается. □

Заметим, что доказательство леммы 1 несложно обобщить на любой ортогональный набор столбцов.

Напомним, что один столбец кодового слова $\mathbf{C} \in \mathcal{C}$ передаётся по одной передающей антенне. Таким образом, каждый элемент кодового слова $\mathcal{L}(\mathbf{C})$ соответствует одной антенне.

Требование декодируемости накладывает некоторые ограничения на код $\mathcal{L}(\mathcal{C})$. PRF-код $\mathcal{C}$ не должен содержать кодовых слов с одинаковым набором столбцов. Для кода $\mathcal{L}(\mathcal{C})$ это ограничение означает отсутствие кодовых слов, содержащий одинаковый набор элементов. Отсутствие повторяющихся столбцов в словах кода $\mathcal{C}$ приводит к отсутствию повторяющихся символов в словах кода $\mathcal{L}(\mathcal{C})$.

Рассмотрим, как отображение $\mathcal{L}$ влияет на расстояние между кодовыми словами. В пространстве матриц мы будем использовать Евклидову метрику, а в пространстве F_T^N – Хэммингову.

Заметим, что Евклидово расстояние между двумя различными столбцами $(T \times T)$-матрицы Адамара равно $\sqrt{\frac{T}{2} \cdot 2^2 + \frac{T}{2} \cdot 0^2} = \sqrt{2T}$. Возьмём два кодовых слова $\mathbf{s_1}, \mathbf{s_2} \in \mathcal{L}(\mathcal{C})$ с расстоянием Хэмминга, равным d. Тогда квадрат Евклидова расстояния $d_E^2(\mathcal{L}^{-1}(\mathbf{s}_1), \mathcal{L}^{-1}(\mathbf{s}_2))$ равен сумме квадратов расстояний между столбцами, т. е. $2Td$. Таким образом, $d_E(\mathcal{L}^{-1}(\mathbf{s}_1), \mathcal{L}^{-1}(\mathbf{s}_2)) = \sqrt{2dT}$.

Согласно [18], Евклидово расстояние является хорошей метрикой качества кода при малом отношении сигнал-шум. На корректирующую способность влияет не только минимальное кодовое расстояние, но и спектр расстояний. Квадрат Евклидова расстояния является энергетическим расстоянием между кодовыми словами. Известным выражением для этого расстояния является $d_E^2(\mathbf{C}_1, \mathbf{C}_2) = \mathrm{tr}(\mathbf{C}_1 - \mathbf{C}_2)^H(\mathbf{C}_1 - \mathbf{C}_2)$, где ^{H} - оператор эрмитова сопряжения. В [30] критерий выбора кода по Евклидову расстоянию называется trace criterion (англ. критерий следа). Мы будем пользоваться именно этим критерием при выборе сигнально-кодовой конструкции.

Суммируя всё сказанное выше, мы будем строить PF- и PRF-коды длины N над полем F_T с «хорошим» спектром Хэммингових расстояний.

1.3.1. PRF-код с манипуляцией знака

Введём ещё одну сигнально-кодовую конструкцию, являющуюся модификацией представленных PRF-кодов. Выберем некоторый PRF-код $\mathcal{C}$, слова которого составлены из столбцов матрицы Адамара (алгоритмы его построения описаны в главе 1.4). Пусть передаваемая информация представлена натуральным числом $a \leq |\mathcal{C}|$ и вектором $\mathbf{b} = (b_1, \ldots, b_N), b_i = \pm 1$. Опишем процедуру кодирования:

Выберем слово $\mathbf{C}_a \in \mathcal{C}$. Результатом кодирования является матрица $\overline{\mathbf{C}}_{a\mathbf{b}} = \mathbf{C}_a \mathrm{diag}(b_1, \ldots, b_N)$.

Назовём полученный код $\overline{\mathbf{C}}_{ab}$ PRF-кодом с манипуляцией знака. Такой код является PRF-кодом, а значит он удовлетворяет условию (1.5).

Нужно заметить, что при замене условия декодируемости (1.5) на более строгое, гарантирующее возможность передачи данных, если $\exists j : a_j \neq 0$, коды со скоростью больше 1 не могут существовать. В этом легко убедиться, представив данное состояние канала, как обычный SISO (Single Input Single output – одна передающая и одна приёмная антенна) канал.

Построение PF-кодов с манипуляцией знака также возможно, но осложняется невозможностью независимого изменения фазы равных между собой столбцов.

1.4. Некоторые подходы к построению кодов, свободных от перестановок

1.4.1. Основные понятия и определения.

Линейный код над полем F_q длины n размерности k с минимальным расстоянием d обозначим как $[n, k, d]_q$-код. Нелинейный код над полем F_q длины n мощности M с минимальным расстоянием d обозначим как $(n, M, d)_q$-код.

Определение 3. 1. Будем называть *PF-кодом* совокупность слов, каждое из которых не является перестановкой другого. PF-код $(n, M, d)_q$ обозначим через $(n, M, d)_q^{PF}$-код. Максимально возможную мощность PF-кода при заданных параметрах n, d, q обозначим через $M_q^{PF}(n, d)$. *Максимальным PF-кодом* назовем код мощности $M_q^{PF}(n, d)$.

2. PF-код, в словах которого нет совпадающих символов, назовем *PRF-кодом*. PRF-код $(n, M, d)_q$ обозначим через $(n, M, d)_q^{PRF}$-код. Максимально возможную мощность PRF-кода при заданных параметрах n, d, q обозначим через $M_q^{PRF}(n, d)$. *Максимальным PRF-кодом* назовем код мощности $M_q^{PRF}(n, d)$.

3. Рассмотрим подкоды $[n, n-d+1, d]_q$-РС-кода. Подкод называется *PF-подкодом* или *PRF-подкодом*, если он является, соответственно, PF-кодом или PRF-кодом.

   Обозначим через $\overline{M}_q^{PF}(n,d)$ и $\overline{M}_q^{PRF}(n,d)$ максимально возможные мощности, соответственно, PF-подкода и PRF-подкода. *Максимальным PF-подкодом* и *максимальным PRF-подкодом* назовем подкоды мощности $\overline{M}_q^{PF}(n,d)$ и $\overline{M}_q^{PRF}(n,d)$, соответственно.

Заметим, что PRF-код является кодом, свободным от повторений (Repetition Free code). Такие коды рассмотрены в [33],[34]. Но в этих работах перестановки символов в кодовом слове не запрещены.

Пусть $a = (a_1, a_2, ..., a_n)$ является n-вектором над полем F_q.

Если $\sum_{i=1}^{n} a_i = s \in F_q$, тогда вектор a называется $(n,s)_q$-*вектор*.

Если *все компоненты* $(n,s)_q$-вектора *различны*, тогда вектор называется $(n,s)_q^{RF}$-*вектор* или просто *RF-вектор* (Repetition Free vector). Таким образом, для $(n,s)_q^{RF}$-вектора a справедливо

$$\sum_{i=1}^{n} a_i = s \in F_q,\ a_i \neq a_j \text{ при } i \neq j.$$

Пусть $u = (u_1, u_2, ..., u_n)$ является n-вектором над полем F_q. В соответствии с [35, Раздел 5.6] назовем *композицией* вектора u следующий q-вектор над алфавитом $\{0, 1, ..., n\}$:

$$\mathrm{comp}(u) = \mathrm{comp}(u_1, u_2..., u_n) = (v_0, v_1, ..., v_{q-1}) = (v_0(u), v_1(u), ..., v_{q-1}(u)),$$

где $v_i = v_i(u)$ равно числу компонент u_j, равных i. Очевидно, $\sum_{i=0}^{q-1} v_i(u) = n$.

Композицией 2-го порядка n-вектора u над F_q назовем следующий $(n+1)$-вектор над алфавитом $\{0, 1, ..., q-1\}$:

$$\mathrm{comp}^{(2)}(u) = \mathrm{comp}(\mathrm{comp}(u)) = \mathrm{comp}(v_0(u), v_1(u), ..., v_{q-1}(u)) =$$
$$(V_0, V_1, ..., V_n) = (V_0(u), V_1(u), ..., V_n(u)),$$

где $V_i = V_i(u)$ равно числу компонент $v_j(u)$, равных i. Очевидно, $\sum_{i=0}^{n} V_i(u) = q$.

Симметрическая группа n-й степени S_n мощности $n!$ (состоящая из всех подстановок n-й степени) разбивает пространство векторов F_q^n на непересекающиеся орбиты. Далее рассматриваются именно такие орбиты. Значения параметров n и q ясны из контекста.

Длина (мощность) орбиты лежит в диапазоне $1 \ldots n!$ Количество и длина орбит зависят от значений n и q.

Обозначим через $O^w(a) = O^w(a_1, a_2, \ldots, a_n)$ орбиту, содержащую слово (word) $a = (a_1, a_2, \ldots, a_n)$, где $a_i \in F_q$. Слово $a = (a_1, a_2, \ldots, a_n)$ назовем генератором орбиты. Любое слово орбиты может быть ее генератором. Если $\sum_{i=1}^{n} a_i = s \in F_q$, тогда орбита $O^w(a_1, a_2, \ldots, a_n)$ называется также $(n, s)_q$-*орбитой*, и ее генератор $(a_1, a_2, \ldots, a_n)$ является $(n, s)_q$-*вектором*.

Обозначим через $O(v) = O(v_0, v_1, ..., v_{q-1})$ орбиту, генератор которой имеет композицию $v = (v_0, v_1, ..., v_{q-1})$. Все слова орбиты имеют одинаковую композицию, и орбита содержит все слова с этой композицией. Указанную композицию будем называть *композиция орбиты*. Длина орбиты $O(v_0, v_1, ..., v_{q-1})$ равна количеству n-векторов над F_q с композицией $(v_0, v_1, ..., v_{q-1})$, т. е.

$$|O(v_0, v_1, ..., v_{q-1})| = \binom{n}{v_0, v_1, ..., v_{q-1}} = \frac{n!}{v_0! v_1! ... v_{q-1}!}. \tag{1.7}$$

Назовем *структурой орбиты* композицию 2-го порядка ее генератора. Обозначим через $O^{(2)}(V) = O^{(2)}(V_0, V_1, ..., V_n)$ орбиту, генератор которой имеет композицию 2-го порядка $V = (V_0, V_1, ..., V_n)$. Пусть $T(V_0, V_1, ..., V_n)$ – множество орбит со структурой $(V_0, V_1, ..., V_n)$. Количество орбит $N_O(V_0, V_1, ..., V_n)$ в этом множестве равно количеству q-векторов над алфавитом $\{0, 1, ..., n\}$ с композицией $(V_0, V_1, ..., V_n)$, т. е.

$$N_O(V_0, V_1, ..., V_n) = \frac{q!}{V_0! V_1! ... V_n!}. \tag{1.8}$$

Учитывая (1.7), длина любой орбиты из множества $T(V_0, V_1, ..., V_n)$ равна

$$|O^{(2)}(V_0, V_1, ..., V_n)| = \frac{n!}{(0!)^{V_0}(1!)^{V_1}\dots(n!)^{V_n}} = \frac{n!}{\prod\limits_{i=0}^{n}(i!)^{V_i}}. \tag{1.9}$$

По существу, соотношение (1.9) является соотношением (1.7), в котором сгруппированы одинаковые сомножители.

Лемма 2. *PF-код $(n, M, d)_q^{PF}$ может включать не более одного слова из каждой орбиты группы S_n независимо от структуры орбиты.*

1.4.2. RF-орбиты, RF-подмножества и RF-векторы

Далее во всей работе $n \leq q$.

Рассмотрим орбиту с генератором $(a_1, a_2, \dots, a_n)$. Если все компоненты a_i *различны* и $\sum\limits_{i=1}^{n} a_i = s \in F_q$, тогда орбита называется $(n, s)_q^{RF}$*-орбитой* или просто *RF-орбитой* (Repetitions Free orbit). Будем обозначать ее также через O_{RF}. Из сказанного в 1.4.1 следует, что независимо от s структура $(n, s)_q^{RF}$-орбиты имеет вид

$$V_0 = q - n, V_1 = n, V_2 = V_3 = \dots = V_n = 0. \tag{1.10}$$

Для заданных q и n общее количество RF-орбит и длина RF-орбиты равны, соответственно,

$$N_{O_{RF}} = \binom{q}{n},\ |O_{RF}| = n!. \tag{1.11}$$

Лемма 3. *Все слова $(n, M, d)_q^{PRF}$-кода принадлежат RF-орбитам группы S_n. При этом из каждой RF-орбиты PRF-код может включать не более одного слова.*

Леммы 2 и 3 являются базовыми для построения PF- и PRF-кодов.

Следствие 1. *При любом расстоянии d для максимально возможной мощности $(n, M, d)_q^{PRF}$-кода справедливо*

$$M_q^{PRF}(n, d) \leq \binom{q}{n}.$$

Доказательство. Используется лемма 3 и соотношение (1.11). □

Назовем n-подмножество поля F_q, состоящее из *различных* элементов, *RF-подмножеством* (Repetitions Free subset). RF-подмножество, сумма элементов которого равна s, будем называть также $(n,s)_q^{RF}$-*подмножеством*. Такое подмножество имеет вид

$$\{a_1, a_2, ..., a_n\} \subset F_q,\ \sum_{i=1}^{n} a_i = s,\ a_i \neq a_j \text{ при } i \neq j.$$

Обозначим через $N_{n,q}^{(s)}$ общее число $(n,s)_q^{RF}$-подмножеств.

Если любым образом упорядочить элементы $(n,s)_q^{RF}$-подмножества, то получим $(n,s)_q^{RF}$-вектор, который можно рассматривать как генератор $(n,s)_q^{RF}$- орбиты. Таким образом, между $(n,s)_q^{RF}$-подмножествами и $(n,s)_q^{RF}$-орбитами существует взаимно-однозначное соответствие. Поэтому величины $N_{n,q}^{(s)}$ играют важную роль при построении и исследовании PF- и PRF-кодов. Пусть $F_q = \{e_0, e_1, \ldots, e_{q-1}\}$. Тогда

$$\sum_{i=0}^{q-1} N_{n,q}^{(e_i)} = \binom{q}{n}. \tag{1.12}$$

1.4.3. Коды $(n, M, 2)_{2^m}^{PF}$ и $(n, M, 2)_{2^m}^{PRF}$ как подкоды $[n, n-1, 2]_{2^m}$-РС-кода.

Далее во всей работе рассматриваются $(n, M, 2)_{2^m}^{PF}$- и $(n, M, 2)_{2^m}^{PRF}$-коды над полем F_{2^m} с расстоянием $d = 2$. Элементы поля F_{2^m} будем обозначать числами так, что

$$F_{2^m} = \{0, 1, ..., 2^{m-1}\}. \tag{1.13}$$

При этом двоичное m-разрядное представление числа совпадает с векторным представлением элемента над некоторым базисом. Поскольку здесь мы используем только сложение элементов, базис не имеет значения.

Полезные соотношения, связанные с величинами $N_{n,2^m}^{(s)}$, получены в приложении с использованием спектра весов двоичного кода Хэмминга и его смежных классов. Введем обозначения:

$A_{w,2^m}$ – число слов веса w в двоичном $[2^m-1, 2^m-1-m, 3]_2$-коде Хэмминга с m проверочными символами,

$\overline{A}_{w,2^m}$ – число слов веса w в смежном классе $[2^m-1, 2^m-1-m, 3]_2$-кода Хэмминга.

Все слова $[n, n-1, 2]_{2^m}$-РС-кода могут быть получены добавлением проверки на четность к информационному $(n-1)$-вектору. Отсюда вытекает следующая лемма.

Лемма 4. *Рассматривается $[n, n-1, 2]_{2^m}$-РС-код и его смежные классы.*

1. *Код содержит все $(n, 0)_{2^m}$-векторы и только эти векторы. Группа S_n разбивает код на непересекающиеся $(n, 0)_{2^m}$-орбиты.*

2. *Пусть смежный класс имеет ненулевой синдром $s \in F_{2^m}$. Тогда смежный класс содержит все $(n, s)_{2^m}$-векторы и только эти векторы. Группа S_n разбивает этот смежный класс на непересекающиеся $(n, s)_{2^m}$- орбиты.*

Назовем орбиту, вложенную в РС-код, *кодовой орбитой*. Вложенная в код RF-орбита называется *кодовой RF-орбитой*.

Из лемм 2 – 4 вытекает следующая теорема.

Теорема 1. *Рассматривается $[n, n-1, 2]_{2^m}$-РС-код.*

1. *Максимальный PF-подкод включает одно и только одно слово из каждой кодовой орбиты независимо от ее структуры. Максимальная мощность $\overline{M}_{2^m}^{PF}(n, 2)$ равна общему числу кодовых орбит.*

2. *Максимальный PRF-подкод включает одно и только одно слово из каждой кодовой RF-орбиты. Слов из орбит с другой композицией такой под-*

код не содержит. Максимальная мощность $\overline{M}_{2^m}^{PRF}(n,2)$ *равна общему числу кодовых RF-орбит.*

Лемма 5. *В* $[n, n-1, 2]_{2^m}$*-PC-коде с* $n \leq 2^m$*,* $m \geq 3$*, существуют кодовые орбиты, представленные в таблице* 1.1*, где* O_1 *является RF-орбитой.*

Доказательство. Длины всех орбит в таблице 1.1 рассчитаны по формуле (1.9).

Структура RF-орбиты O_1 имеет вид (1.10) независимо от того, кодовая она или нет. Аналогично, для генератора RF-орбиты всегда необходимо условие $a_i \neq a_j$ при $i \neq j$. Наконец, равенство $a_1 + \ldots + a_n = 0$ для генератора *кодовой* RF-орбиты должно выполняться по лемме 4(1). Из свойств генератора и определения величины $N_{n,q}^{(s)}$ следует $N_{O_1} = N_{n,2^m}^{(0)}$. Далее используется соотношение (1) следствия 3, см. приложение.

Для орбит O_2 – O_9 и O_{8+t} используется лемма 4(1). С учетом свойств поля F_{2^m} все генераторы орбит O_2 – O_9 и O_{8+t} имеют нулевую сумму элементов. Структура орбиты определяется видом генератора. Количество орбит O_2, O_3, O_4, O_{8+t} вытекает из (1.8) поскольку никаких ограничений на элементы генератора не указано. Для орбит O_5 и O_6 элемент a можно выбрать 2^m способами. Затем используем лемму 12(2), см. приложение. Для орбит O_7 и O_8 пару элементов a, b можно выбрать $\binom{2^m}{2}$ способами. Далее используем лемму 12(3). Наконец, для орбиты O_9 пару элементов a, b можно выбрать $2^m(2^m-1)$ способами, поскольку элементы a и b неравноправны. Затем снова применяем лемму 12(3). □

Теорема 2. *Максимальный PRF-подкод* $[n, n-1, 2]_{2^m}$*-PC-кода имеет мощность*

$$\overline{M}_{2^m}^{PRF}(n,2) = N_{n,2^m}^{(0)} = A_{n-1,2^m} + A_{n,2^m}. \tag{1.14}$$

При этом все слова максимального PRF-подкода могут быть получены непосредственно из слов веса $n-1$ *и* n *двоичного* $[2^m-1, 2^m-1-m, 3]_2$*-кода Хэмминга.*

Орбита	Ненулевые компоненты структуры орбиты	Генератор орбиты	Количество орбит N_{O_j}	Длина орбиты $\lvert O_j\rvert$
$O_1 = O_{RF}$	$V_0 = 2^m - n, V_1 = n$	$(a_1, a_2, \ldots, a_n)$ $a_1 + a_2 + \ldots + a_n = 0$ $a_i \neq a_j$ при $i \neq j$	$N^{(0)}_{n,2^m} =$ $A_{n-1,2^m} + A_{n,2^m}$	$n!$
O_2	$V_0 = 2^m - 1, V_n = 1$	$(\underbrace{a, ..., a}_{n}),\ n = 2p$	2^m	1
O_3	$V_0 = 2^m - 2, V_p = 2$	$(\underbrace{a, ..., a}_{p}, \underbrace{b, ..., b}_{p})$ p – четное	$\binom{2^m}{2}$	$\binom{n}{p}$
O_4	$V_0 = 2^m - p, V_2 = p$	$(a_1, a_1, a_2, a_2, ..., a_p, a_p)$	$\binom{2^m}{p}$	$2^{-p}n!$
O_5	$V_0 = 2^m - 4,$ $V_1 = 3, V_{n-3} = 1$	$(\underbrace{a, ..., a}_{n-3}, b, c, d)$ $a + b + c + d = 0,\ n = 2p$	$2^m \cdot \frac{1}{3}\binom{2^m-1}{2}$	$\frac{n!}{(n-3)!}$
O_6	$V_0 = 2^m - 5,$ $V_1 = 4, V_{n-4} = 1$	$(\underbrace{a, ..., a}_{n-4}, b, c, d, e)$ $b + c + d + e = 0$ $n = 2p \geq 6$	$2^m \cdot \frac{1}{2^m-3}\binom{2^m-1}{4}$	$\frac{n!}{(n-4)!}$
O_7	$V_0 = 2^m - 4, V_1 = 2,$ $V_{p-1} = 2$	$(\underbrace{a, ..., a}_{p-1}, \underbrace{b, ..., b}_{p-1}, c, d)$ p – четное $a + b + c + d = 0$	$\binom{2^m}{2}(2^{m-1} - 1)$	$\frac{n!}{(p-1)!(p-1)!}$
O_8	$V_0 = 2^m - 6, V_1 = 4,$ $V_{p-2} = 2$	$(\underbrace{a, ..., a}_{p-2}, \underbrace{b, ..., b}_{p-2}, c, d, e, f)$ p – четное $c + d + e + f = 0,\ n \geq 8$	$\binom{2^m}{2}\ (2^{m-1} - 1 +$ $\frac{1}{3}\binom{2^m-1}{2}(2^{m-2} - 2))$	$\frac{n!}{(p-2)!(p-2)!}$
O_9	$V_0 = 2^m - 5, V_1 = 3,$ $V_{p-1} = 1, V_{p-2} = 1$	$(\underbrace{a, ..., a}_{p-1}, \underbrace{b, ..., b}_{p-2}, c, d, e)$ p – четное $a + c + d + e = 0,\ n \geq 8$	$\binom{2^m}{3}(2^m - 4)$	$\frac{n!}{(p-1)!(p-2)!}$
O_{8+t}	$V_0 = 2^m - p + t - 1,$ $V_2 = p - t, V_{2t} = 1$	$(\underbrace{b, ..., b}_{2t}, a_1, a_1, ..., a_{p-t}, a_{p-t})$ $n = 2p,\ t = 2, 3, \ldots, p-1$	$\binom{2^m}{p-t}(2^m - p + t)$	$\frac{1}{(2t)!}2^{t-p}n!$

Таблица 1.1. Некоторые кодовые орбиты $[n, n-1, 2]_{2^m}$-РС-кода, $n \leq 2^m$

Доказательство. В соответствии с теоремой 1(2), максимальный PRF-подкод включает точно одно слово из каждой кодовой RF-орбиты. Далее используется лемма 5 и орбиты O_1 таблицы 1.1.

Упорядочим (в произвольном порядке) указанные в лемме 9(1) $(n,0)^{RF}_{2^m}$ - подмножества, построенные на основе слов веса $n-1$ и n двоичного $[2^m-1, 2^m-1-m, 3]_2$-кода Хэмминга. В результате получим $(n,0)^{RF}_{2^m}$-векторы, которые могут рассматриваться как слова максимального PRF-кода. □

Следствие 2. *Для* $n \in \{2^m-2, 2^m-1, 2^m\}$ *максимальный PRF-подкод* $[n, n-1, 2]_{2^m}$*-PC-кода имеет мощность*

$$\overline{M}^{PRF}_{2^m}(2^m,2) = \overline{M}^{PRF}_{2^m}(2^m-1,2) = 1,\ \overline{M}^{PRF}_{2^m}(2^m-2,2) = 0.$$

Доказательство. Используются теорема 2 и лемма 10, см. приложение. □

PF- или PRF-код построен, если структуры и генераторы всех орбит, представители которых образуют код, определены.

Из леммы 5 и теоремы 2 следует, что *задача построения максимального PRF-подкода* $[n, n-1, 2]_{2^m}$*-PC-кода решена* и точное значение максимальной мощности $\overline{M}^{PRF}_{2^m}(n,2)$ получено.

Учитывая лемму 5 и теоремы 1 и 2, максимальный PF-подкод $[n, n-1, 2]_{2^m}$-PC-кода можно построить следующим образом.

Алгоритм А. *Построение максимального PF-подкода* $[n, n-1, 2]_{2^m}$*- PC-кода.*

1. В таблице 1.1 выделить орбиты O_j, которые присутствуют в PC-коде при заданном значении n. Множество номеров таких орбит обозначим как J_n. (RF-орбиты O_1 всегда присутствуют.) Подсчитать суммарное количество M выделенных кодовых орбит и количество Σ слов в этих орбитах:

$$M = \sum_{j \in J_n} N_{O_j}, \quad \Sigma = \sum_{j \in J_n} N_{O_j} \cdot |O_j|.$$

2. Проверить равенство

$$\Sigma = 2^{m(n-1)}. \tag{1.15}$$

Если (1.15) выполняется, выйти из алгоритма, полагая, что

$$\overline{M}_{2^m}^{PF}(n,2) = M.$$

Если (1.15) не выполняется, перейти к шагу 3.

3. Основываясь на технике построения таблицы 1.1 и доказательстве леммы 5, найти допустимую при заданных параметрах структуру орбиты O_{new}, которая не использована на выполненных шагах. Определить длину $|O_{\text{new}}|$ этой орбиты и количество $N_{O_{\text{new}}}$ таких орбит. Скорректировать $\Sigma = \Sigma + N_{O_{\text{new}}} \cdot |O_{\text{new}}|$, $M = M + N_{O_{\text{new}}}$. Перейти к шагу 2.

Заметим,что при выполнении (1.15) выделенные орбиты содержат весь РС-код. В этом случае максимальный PF-подкод построен, и его мощность $\overline{M}_{2^m}^{PF}(n,2)$ равна общему числу кодовых орбит M.

Эффективность алгоритма А проиллюстрирована в разделе 1.5.1, где приведены практически интересные примеры построения максимальных PF-подкодов $[n, n-1, 2]_8$-РС-кода. Шаг 3 алгоритма в этих примерах не понадобился.

1.4.4. Коды $(n, M, 2)_{2^m}^{PF}$ и $(n, M, 2)_{2^m}^{PRF}$ как подмножества пространства $F_{2^m}^n$.

В общем случае, когда мы не ограничены подкодами РС-кода, оказываются полезными следующие алгоритмы.

Алгоритм В. *Построение PRF-кода как объединения PRF-кодов, полученных из кода Рида-Соломона и его смежных классов.*

Пусть $n \geq 4$. Обозначим искомый $(n, M, 2)_{2^m}^{PRF}$-код через $\mathcal{C}$.

1. На основе леммы 11, см. приложение, построить $(n, N_{n,2^m}^{(s)}, 2)_{2^m}^{PRF}$-коды, сумма элементов каждого слова которых равна s, для всех $s = 0, 1, \ldots, 2^m -$

1. Введём некоторый упорядочивание элементов поля F_q. Пример такого упорядочивания представлен в начале развела 1.4.3. Переупорядочить все слова полученных кодов с $s \neq 0$ по убыванию составляющих элементов, а слова кода с $s = 0$ – по возрастанию элементов. Обозначим полученные PRF-коды как $\mathcal{C}_s$-коды.

2. Сформировать код $\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1$. По построению код имеет расстояние 2. Положить $s' = 2$.

3. Получить код $\mathcal{C}^*_{s'}$, выполнив над словами кода $\mathcal{C}_{s'}$ некоторые перестановочные операции, одинаковые для всех слов. В качестве примера таких операций укажем циклический сдвиг влево или вправо на определенное число позиций, перестановку некоторых (фиксированных для данного s') пар элементов. Методом проб и ошибок найти операции, обеспечивающие расстояние 2 в объединенном коде $\mathcal{C} \cup \mathcal{C}^*_{s'}$. Положить $\mathcal{C} = \mathcal{C} \cup \mathcal{C}^*_{s'}$. Если операции найти не удается, код $\mathcal{C}$ не меняется.

4. Если $s' = 2^m - 1$, выйти из алгоритма. Иначе положить $s' = s' + 1$ и перейти к шагу 3.

Эффективность алгоритма B проиллюстрирована в 1.5.2, где построен практически интересный максимальный $(4, M, 2)_8^{PRF}$-код мощности $M = \binom{8}{4}$, см. пример 1. В этом примере перестановочные операции обеспечивающие расстояние 2 в объединенном коде $\mathcal{C} \cup \mathcal{C}^*_{s'}$, найдены для всех s'.

Полезен также следующий жадный алгоритм.

Алгоритм C. *Построение PRF-кода с «хорошим» спектром расстояний.* Обозначим искомый $(n, M, 2)_{2^m}^{PRF}$-код через $\mathcal{V}$.

1. В пространстве $F_{2^m}^n$ построить все RF-орбиты группы S_n. (Это можно сделать, например, перечислив все сочетания из 2^m элементов по n.) Обозначим эти орбиты $O_1, O_2, \ldots, O_{M_0}, M_0 = \binom{2^m}{n}$. Пусть
$O_i = \{c_{i,1}, c_{i,2}, \ldots, c_{i,n!}\}$, где $c_{i,j}$ – некоторый n-вектор из орбиты O_i.

2. В орбите O_1 выбрать случайным образом вектор $c_{1,j}$ и положить

$$\mathcal{V} = \{v_1\},\ v_1 = c_{1,j},\ M = 1,\ i = 2.$$

3. Вычислить для *каждого* вектора $c_{i,j}$ орбиты O_i спектр расстояний от построенного на предыдущих шагах кода $\mathcal{V} = \{v_1, v_2, \ldots, v_M\}$:

$$\mathrm{spec}(c_{i,j}, \mathcal{V}) = (s_1, s_2, \ldots, s_n),\ s_u = |\{k : v_k \in \mathcal{V},\, d(c_{i,j}, v_k) = u\}|,$$

где $d(c, v)$ – расстояние Хэмминга между векторами c и v.

4. Если нет ни одного спектра $\mathrm{spec}(c_{i,j}, \mathcal{V})$, для которого $s_1 = 0$, положить $i = i + 1$ и перейти к шагу 6. (Представитель орбиты O_i в этом случае не включается в код $\mathcal{V}$.)

Если спектр с $s_1 = 0$ существует, перейти к шагу 5.

5. Выбрать все векторы $c_{i,j}$, в спектре которых $s_1 = 0$. Из этих векторов выбрать вектор с наименьшим значением s_2. Если таких векторов больше одного, выбрать среди них векторы с минимальным значением s_3 и так далее до s_n. Если осталось больше одного вектора, выбрать один из них произвольно. Обозначим выбранный вектор через $c_{i,t}$. Положить

$$M = M + 1,\ v_M = c_{i,t},\ \mathcal{V} = \mathcal{V} \cup \{v_M\},\ i = i + 1.$$

Перейти к шагу 6.

6. Если $i > M_0$, выйти из алгоритма. В противном случае перейти к шагу 3.

Эффективность алгоритма С проиллюстрирована в 1.5.2, где в примере 2 построен максимальный $(4, 70, 2)_8^{PRF}$-код с лучшим, чем в примере 1, спектром расстояний. Для всех орбит в этом примере существовал вектор $c_{i,j}$, в спектре которого $s_1 = 0$. Поэтому код $\mathcal{V}$ получился максимальным.

В принципе, $(n, M, 2)_{2^m}^{PF}$- код может иметь большую мощность, чем $(n, M, 2)_{2^m}^{PRF}$- код, поскольку требования к PF-коду слабее. Для построения PF-кода как подмножества пространства $F_{2^m}^n$ представляется разумным взять в

качестве стартового набора PRF-код, полученный алгоритмом B или C. Затем к коду следует приписать ряд представителей орбит, допускающих повторение элементов. При этом, разумеется, необходимо следить за сохранением кодового расстояния 2.

Эффективность такого подхода проиллюстрирована в 1.5.2, где построен $(4, M, 2)_8^{PF}$-код мощности 114, тогда как максимальный $(4, M, 2)_8^{PRF}$-код имеет мощность 70.

1.5. Примеры построения $(n, M, 2)_8^{PF}$ и $(n, M, 2)_8^{PRF}$ кодов

В данном разделе $n = 4, 8$ и $m = 3$.

1.5.1. Коды $(n, M, 2)_8^{PF}$ и $(n, M, 2)_8^{PRF}$ как подкоды $[n, n-1, 2]_8$-РС-кода

В теоремах 3 и 4 используется алгоритм A, см. 1.4.3.

Теорема 3. *1. Пусть орбиты O_1, O_2, O_3 заданы в таблице* 1.1. *РС-код $[4, 3, 2]_8$ разбивается на* 50 *следующих $(4, 0)_8$-орбит симметрической группы S_4:* 14 *RF-орбит O_1,* 8 *орбит O_2 и* 28 *орбит O_3 с $p = 2$.*

2. Максимальный PF-подкод $[4, 3, 2]_8$-РС-кода содержит 50 *слов, т. е.*

$$\overline{M}_8^{PF}(4, 2) = 50.$$

3. Максимальный PRF-подкод $[4, 3, 2]_8$-РС-кода содержит $N_{4,8}^{(0)} = \frac{1}{4}\binom{8}{4}$ слов, т. е.

$$\overline{M}_8^{PRF}(4, 2) = 14.$$

Доказательство. В пунктах 1 и 2 используется алгоритм A.

1. Длина и количество орбит указаны в таблице 1.1. Мы полагаем $J_4 = \{1, 2, 3\}$. Для $N_{4,8}^{(0)}$ используем лемму 12(i). Учитывая длину орбит, записанную в таблице 1.1, получаем, что всего в 50 указанных орбитах содержится $\Sigma = \sum\limits_{j=1}^{3} N_{O_j} \cdot |O_j| = 8^3$ кодовых слов, т. е. весь $[4, 3, 2]_8$-РС-код.

2. В соответствии с теоремой 1(1), максимальный PF-подкод включает точно одно слово из каждой кодовой орбиты, независимо от ее структуры.

3. Следует из теоремы 2 и леммы 12(i).

□

Теорема 4. *1. Пусть орбиты $O_1 - O_9$ и O_{8+t} заданы в таблице* 1.1. *PC-код $[8, 7, 2]_8$ разбивается на* 835 *следующих $(8, 0)_8$-орбит симметрической группы S_8: одну RF-орбиту O_1,* 8 *орбит O_2,* 28 *орбит O_3,* 70 *орбит O_4,* 56 *орбит O_5,* 56 *орбит O_6,* 84 *орбиты O_7,* 84 *орбиты O_8,* 224 *орбиты O_9,* 168 *орбит O_{8+2} и* 56 *орбит O_{8+3}. При этом для всех орбит с параметром p полагаем $p = 4$.*

2. Максимальный PF-подкод $[8, 7, 2]_8$-PC-кода содержит 835 *слов, т. е.*

$$\overline{M}_8^{PF}(8, 2) = 835.$$

3. Максимальный PRF-подкод $[8, 7, 2]_8$-PC-кода содержит 1 *слово и является также максимальным $(8, M, 2)_8^{PRF}$-кодом, т. е.*

$$\overline{M}_8^{PRF}(8, 2) = M_8^{PRF}(8, 2) = 1.$$

Доказательство. В пунктах 1 и 2 используется алгоритм А.

1. Длина и количество орбит указаны в таблице 1.1. Мы полагаем $J_8 = \{1, 2, \ldots, 11\}$. Для $N_{8,8}^{(0)}$ используем (9). Учитывая длину орбит, записанную в таблице 1.1, получаем, что всего в 835 указанных орбитах содержится $\Sigma = \sum_{j=1}^{11} N_{O_j} \cdot |O_j| = 8^7$ кодовых слов, т. е. весь $[8, 7, 2]_8$ код РС.

2. В соответствии с теоремой 1(1), максимальный PF-подкод включает точно одно слово из каждой кодовой орбиты, независимо от типа орбиты.

3. Используются следствия 1 и 2.

□

1.5.2. Коды $(n, M, 2)_8^{PF}$ и $(n, M, 2)_8^{PRF}$ как подмножества пространства F_8^n

Максимальный $(4, 70, 2)_8^{PRF}$-код

Пример 1. Для построения максимального $(4, 70, 2)_8^{PRF}$-кода используется алгоритм B, см. 1.4.4.

По лемме 12(1) $N_{4,8}^{(0)} = 14$. По следствию 3 и лемме 13, см. приложение, $N_{4,8}^{(s)} = 8$ для всех $s \neq 0$.

Коды $\mathcal{C}_0$ и $\mathcal{C}_1$ имеют вид:

$\mathcal{C}_0 = \{0123, 0145, 0167, 0246, 0257, 0347, 0356, 1247,$

$1256, 1346, 1357, 2345, 2367, 4567\},$

$\mathcal{C}_1 = \{7530, 7521, 7431, 7420, 6531, 6520, 6430, 6421\}.$

Коды $\mathcal{C}_{s'}^*$ имеют вид:

$\mathcal{C}_2^* = \{7261, 7360, 7342, 7140, 6352, 6150, 5241, 5340\},$

$\mathcal{C}_3^* = \{7136, 7026, 7235, 7015, 6234, 6014, 5024, 5134\},$

$\mathcal{C}_4^* = \{6507, 6417, 5427, 2107, 5436, 3106, 3205, 3214\},$

$\mathcal{C}_5^* = \{1765, 0764, 3754, 0731, 2654, 0621, 1532, 0432\},$

$\mathcal{C}_6^* = \{5276, 4376, 4075, 2073, 4165, 2163, 1052, 1043\},$

$\mathcal{C}_7^* = \{6735, 6724, 5714, 3712, 5604, 3602, 3501, 2401\}.$

Для получения кодов $\mathcal{C}_{s'}^*$ из кодов $\mathcal{C}_{s'}$ использованы следующие перестановочные операции:

$s' = 2 \to$ перестановка 2-го и 3-го элементов,

$s' = 3 \to$ перестановка 2-го и 4-го элементов,

$s' = 4 \to$ циклический сдвиг влево на одну позицию,

$s' = 5 \to$ циклический сдвиг вправо на одну позицию,

$s' = 6 \to$ циклический сдвиг вправо на две позиции,

$s' = 7 \to$ перестановка 1-го и 2-го и 3-го и 4-го элементов.

Расстояние 2 объединенного кода $\mathcal{C} \cup \mathcal{C}_{s'}^*$ на каждом шаге 3 алгоритма B с $s' = 2, 3, \ldots, 7$ проверено на компьютере.

Искомый $(4, M, 2)_8^{PRF}$-код имеет вид $\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \bigcup\limits_{s'=2}^{7} \mathcal{C}_{s'}^*$. Его мощность $M = 14 + 7 \cdot 8 = 70$.

Пример 2. Еще один вариант $(4, 70, 2)_8^{PRF}$-кода, код $\mathcal{V}$, получен на компьютере с помощью жадного алгоритма С, см 1.4.4.

$\mathcal{V} = \{$3210, 4102, 5021, 2601, 1720, 0314, 1053, 0136, 1307, 0541, 6140, 4017, 1065, 7510, 6701, 2430, 5203, 0623, 3072, 0452, 2046, 7204, 0265, 2570, 7026, 4350, 6034, 3407, 5630, 0375, 0763, 4506, 7405, 0647, 5760, 3124, 1532, 6312, 2173, 4251, 1246, 2714, 6125, 2157, 7162, 5413, 3461, 7341, 3615, 5371, 1673, 1564, 4715, 1476, 7651, 4523, 6243, 3742, 5326, 5237, 2367, 5642, 4275, 6427, 2756, 3654, 3547, 4736, 7635, 6574$\}$.

Обозначим через $D = \{d_1, d_2, \ldots, d_n\}$ спектр расстояний (n, M, d)-кода, где d_i – число расстояний i между кодовыми словами. Очевидно, $d_i = 0$ для $i < d$.

Теорема 5. *Коды* $(4, 70, 2)_8^{PRF}$ *примеров* 1 *и* 2 *являются максимальными PRF-кодами, т. е.*

$$M_8^{PRF}(4, 2) = 70.$$

Спектр расстояний указанных кодов следующий: $D = \{0, 234, 712, 1469\}$ *для примера* 1 *и* $D = \{0, 95, 900, 1420\}$ *для примера* 2.

Доказательство. По следствию 1 указанные коды $\mathcal{C}$ имеют максимально возможную мощность. Спектр расстояний вычислен непосредственно. □

Код $(4, 114, 2)_8^{PF}$

Лемма 6. *В пространстве* F_8^4 *существуют орбиты группы* S_4*, указанные в таблице* 1.2.

Доказательство. Длина орбит следует из (1.9). Элемент a для орбиты $O_{aaab}^{(s)}$ может быть выбран произвольно, что ведет к существованию 8 орбит. Для любого фиксированного ненулевого δ в поле F_8 существует 4 пары различных элементов a, b таких, что $a + b = \delta$. Поэтому существуют 4 орбиты $O_{aabb}^{(\delta)}$. □

Таблица 1.2. Некоторые орбиты группы S_4 в пространстве F_8^4

Орбита	Ненулевые компоненты структуры орбиты	Генератор орбиты	Количество орбит	Длина орбиты
$O^{(s)}_{aaab}$	$V_0 = 6, V_1 = 1,$ $V_3 = 1$	$\{a, a, a, b\}$ $a + b = s, \quad s \neq 0$	8	4
$O^{(\delta)}_{aabb}$	$V_0 = 6, V_2 = 1$	(a, a, b, b) $a + b = \delta, \quad \delta \neq 0$	4	6

Лемма 7. *Для любого фиксированного ненулевого $s \in F_8$ расстояние между любыми двумя словами множества $\bigcup\limits_{a=0}^{7} O^{(s)}_{aaab}$ не меньше, чем 2.*

Доказательство. Множество $\bigcup\limits_{a=0}^{7} O^{(s)}_{aaab}$ вложено в смежный класс $[4, 3, 2]_8$-РС-кода с образующим $(0, 0, 0, s)$. □

Лемма 8. *Для любого набора ненулевых элементов $\delta_j \in F_8$ расстояние между любыми двумя словами множества $\bigcup\limits_j \bigcup\limits_i O^{(\delta_j)}_{a_i a_i b_i b_i}$, не меньше, чем 2.*

Доказательство. Множество $\bigcup\limits_j \bigcup\limits_i O^{(\delta_j)}_{a_i a_i b_i b_i}$ вложено в $[4, 3, 2]_8$-РС-код. □

Конструкция D. Запишем ненулевые элементы поля F_8 следующим образом

$\{s_1, s_2, s_3, s_4, \delta_1, \delta_2, \delta_3\}$. Пусть $\mathcal{C}$ является 70-множеством, полученным в примере 1. Построим четыре 8-множества T_j.

$$T_1 = \bigcup_{a_i=0}^{7} b_{1,i} a_i a_i a_i, \quad T_2 = \bigcup_{a_i=0}^{7} a_i b_{2,i} a_i a_i, \quad T_3 = \bigcup_{a_i=0}^{7} a_i a_i b_{3,i} a_i,$$

$$T_4 = \bigcup_{a_i=0}^{7} a_i a_i a_i b_{4,i}, \quad b_{j,i} = a_i + s_j, \quad j = 1, 2, 3, 4, \quad i = 0, 1, \ldots, 7.$$

Для каждого ненулевого элемента δ_k запишем 4 элемента поля $\{a_{k,1}, a_{k,2}, a_{k,3}, a_{k,4}\}$ таких, что $a_{k,u} \neq a_{k,v} + \delta_k$, если $u \neq v$. Далее построим три

4-множества D_k.

$$D_k = \bigcup_{h=1}^{4} a_{k,h}a_{k,h}b_{k,h}b_{k,h}, \quad b_{k,h} = a_{k,h} + \delta_k, \quad k = 1, 2, 3.$$

Построим $(4, 114, 2)_8$-код $\mathcal{U}$ следующим образом.

$$\mathcal{U} = \mathcal{C} \cup \bigcup_{j=1}^{4} T_j \cup \bigcup_{k=1}^{3} D_k.$$

Теорема 6. *1. Код $\mathcal{U}$ конструкции D является $(4, 114, 2)_8^{PF}$-кодом.*

2. Справедлива оценка

$$M_{PF}(4, 2, 8) \geq 114. \tag{1.16}$$

Доказательство. Мощность кода 114 следует непосредственно из конструкции. Свойство PF основано на лемме 2. Минимальное расстояние 2 внутри следующих подмножеств кода: $\mathcal{C}$, T_j, $\bigcup_{k=1}^{3} D_k$ следует из теоремы 5 и лемм 7 и 8.

Минимальное расстояние 2 между подмножествами непосредственно следует из их структуры. В частности, поскольку все слова подмножества $\mathcal{C}$ состоят из различных элементов, а в словах из T_j и D_k только два несовпадающих элемента, расстояние между $\mathcal{C}$ и T_j и между $\mathcal{C}$ и D_k не менее 2. Расстояние между словами различных подмножеств T_j, например, между словами $b_{1,i}a_ia_ia_i$ и $a_ib_{2,i}a_ia_i$, также не менее 2, даже если элементы a_i совпадают. Наконец, поскольку $s_j \neq \delta_k$, $s_j, \delta_k \neq 0$, $b_{1,i} = a_i + s_1$, и $b_{k,h} = a_{k,h} + \delta_k$, то расстояние между словами из подмножеств T_j и D_k, например, между словами $b_{1,i}a_ia_ia_i$ и $a_{k,h}a_{k,h}b_{k,h}b_{k,h}$, не менее 2. В самом деле, если $b_{k,h} = a_i$, то $a_{k,h} \neq a_i$ и $a_{k,h} = b_{k,h} + \delta_k \neq a_i + s_1 = b_{1,i}$.

Оценка (1.16) следует из существования рассмотренного кода. □

1.6. Декодирование

Для декодирования будем использовать метод максимального правдоподобия. Сначала вычислим значение функции правдоподобия на всех возможных

кодовых словах s_i^t. Затем осуществим отображение $\mathcal{L}$ и определим значение функции правдоподобия для всех кодовых слов $\mathbf{c}$. Таким образом мы получаем декодер с мягким выходом.

Построим функцию правдоподобия:

$$P(s_i^t|\alpha_{ij}, r_j^t) = \frac{P(s_i^t|\alpha_{ij})}{P(r_j^t|\alpha_{ij})} P(r_j^t|\alpha_{ij}, s_i^t) = const \cdot P\left(\eta_j^t = r_j^t - \sum_{i=0}^{N} \alpha_{ij} s_i^t\right).$$

Плотность этой вероятности

$$p(s_i^t|\alpha_{ij}, r_j^t) = const \cdot exp\left(\frac{|r_j^t - \sum_{i=0}^{N} \alpha_{ij} s_i^t|^2}{2\sigma^2}\right) = const \cdot exp\left(\frac{f(s_i^t|\alpha_{ij}, r_j^t)}{2\sigma^2}\right).$$

$$f(s_i^t|\alpha_{ij}, r_j^t) = \sum_{j=0}^{N_R} \sum_{t=0}^{T} \left| r_j^t - \sum_{i=0}^{N} \alpha_{ij} s_i^t \right|^2. \tag{1.17}$$

Как было показано ранее, у PRF-кода все столбцы ортогональны, т. е. $\sum_{t=1}^{T} s_i^t s_j^t = T\delta_{ij}$, где δ_{ij} - оператор Кронекера. Поэтому можно воспользоваться подходом, описанным в [14], и переписать выражение (1.17) в виде:

$$f(s_i^t|\alpha_{ij}, r_j^t) = \sum_{i=0}^{N} \sum_{t=0}^{T} \left(\left| s_i^t - \sum_{j=0}^{N_R} \alpha_{ij}^* r_j^t \right|^2 + \left(-1 + \sum_{j=0}^{N} |\alpha_{ij}|^2 \right) \left| s_i^t \right|^2 \right) + const.$$

Так как s_i^t являются элементами матрицы Адамара, то $|s_i^t| = 1$. Внутренняя скобка не зависит от s_i^t, и функция правдоподобия принимает вид

$$f(s_i^t|\alpha_{ij}, r_j^t) = \sum_{i=0}^{N} \sum_{t=0}^{T} \left| s_i^t - \sum_{j=0}^{N_R} \alpha_{ij}^* r_j^t \right|^2 + const, \tag{1.18}$$

где x^* - оператор комплексного сопряжения.

Осуществив отображение $\mathcal{L}(s_i^t)$, мы получим значение функции правдоподобия $f(\mathbf{c})$ на всех элементах поля F_T^N. Кроме того, для PRF-кодов мы можем получить значение функции правдоподобия для отдельных символов из F_T, то есть для каждого символа кодового слова. Данный факт позволяет использовать эффективные методы декодирования, не учитывающие специфику канала передачи данных и работающие с q-ичным симметричным каналом. При этом

можно использовать итеративные алгоритмы исправления ошибок, но в данной работе они не рассматриваются.

В случае PRF-кодов с манипуляцией знака вышеуказанная процедура изменяется минимально. Формула (1.18) принимает вид:

$$f(s_i^t, b_i|\alpha_{ij}, r_j^t) = \sum_{i=0}^{N}\sum_{t=0}^{T}\left|s_i^t b_i - \sum_{j=0}^{N_R}\alpha_{ij}^* r_j^t\right|^2 + const. \tag{1.19}$$

1.7. Нижняя граница на мощность PF-кода

Мы воспользовались методом Гильберта [36] для построения нижней границы на мощности PF и PRF кодов. Вначале приведём её для PF кодов. Метод Гильберта может быть описан следующим алгоритмом.

Algorithm 1 Метод Гильберта

1: $\Omega \leftarrow F_q^n$
2: $C \leftarrow \emptyset$
3: **while** $\Omega \neq \emptyset$ **do**
4: $\quad c \in \Omega$ ▷ Выберем любой c из Ω
5: $\quad \Omega \leftarrow \Omega \backslash \{x \in F_q^n : dist_{Hamm}(c, x) < d\}$
6: $\quad \Omega \leftarrow \Omega \backslash \{x \in F_q^n : \exists \pi : c = \pi(x)\}$
7: $\quad C \leftarrow C \cup c$
8: **end while**
9: **return** C

Построим верхнюю границу на число элементов, исключённых из Ω на шаге 5:

$$D_1 \leq \sum_{i=1}^{d-1}\binom{n}{i}(q-1)^i = \sum_{i=1}^{d-1} n_i$$

$$\frac{n_{i-1}}{n_i} = \frac{i}{(n-i+1)(q-1)} \leq \frac{d-1}{(n-d+2)(q-1)} < 1$$

$$D_1 \leq \sum_{i=1}^{d-1} n_i \leq \binom{n}{d-1}(q-1)^{d-1}\frac{1}{1-\frac{d-1}{(n-d+2)(q-1)}} \tag{1.20}$$

Число элементов исключённых на шаге 6 составляет $D_2 \leq \sum_{k=d}^{n} \binom{n}{k} !k$, где $!k$ обозначает число беспорядков [37]. Для каждой перестановки $\tilde{u}$ вектора u, имеющей не более q неподвижных точек, $d_H(u, \tilde{u}) \leq d$.

$$D_2 \leq \sum_{k=d}^{n} \left\lfloor \frac{n!}{(n-k)!k!} \left(\frac{k!}{e} + \frac{1}{2} \right) \right\rfloor = \sum_{k=d}^{n} \left\lfloor \frac{1}{e} A_n^k + \frac{1}{2} C_n^k \right\rfloor \tag{1.21}$$

Теорема 7. *Существует PF-код, минимальное расстояние которого не меньше d, а мощность равна*

$$M_q^{PF} \geq \frac{q^n}{D_1 + D_2} \tag{1.22}$$

Для $d = 2$, $D_2 = n! - 1$

Для построения аналогичной границы для PRF кодов мы должны сделать замену $q_0 = q - 1 - (n - d)$ в (1.20). Действительно, новое кодовое слово должно быть словом без повторений, поэтому заменённый символ не может быть равен никакому другому символу кодового слова, кроме тех, которые также будут изменены. Поэтому,

Теорема 8. *Существует PRF-код, минимальное расстояние которого не меньше d, а мощность равна*

$$M_q^{PRF} \geq \frac{A_q^n}{D_1^{PRF} + D_2}, \tag{1.23}$$

где

$$D_1^{PRF} \leq \binom{n}{d-1} q_0^{d-1} \frac{1}{1 - \frac{d-1}{(n-d+2)q_0}} \tag{1.24}$$

Мы вычислили значение нижней границы по формуле (1.22) и сравнили результат с кодами, полученными в предыдущих разделах. Результаты сравнения приведены в таблице. Для вычисления верхней границы мы воспользовались следующими формулами.

$$M_q^{PF}(n, d) \leq \binom{q + n - 1}{n} - q(q - n) \tag{1.25}$$

$$M_q^{PRF}(n, d) \leq \binom{q}{n} \tag{1.26}$$

тип	q	D_1	(1.22), (1.23)	(1.25), (1.26)	получены	скорость
PF	8	29	78	298	281	1.02
PF	12	45	304	1269	1102	0.84
PF	16	61	780	3684	2936	0.72
PRF	8	17	42	70	70	0.77
PRF	12	33	212	495	495	0.75
PRF	16	49	606	1820	1812	0.68

Для всех приведённых кодов $n = 4$ и $d = 2$. Из таблицы видно, что мощность полученных численными методами кодов лежит вблизи верхней границы и заметно превышает нижнюю границу.

1.8. Моделирование

Для экспериментальной оценки корректирующей способности предложенной кодовой конструкции была построена модель для пакета Simulink. Данный выбор сделан в силу наличия визуальных средств проектирования и набора библиотечных функций и блоков для эмуляции канала. Кроме того, с помощью Simulink можно разрабатывать программный код для ПЛИС.

Для увеличения скорости моделирования использовался режим rapid accelerator. При этом Simulink преобразует проект в программный код на языке C, который впоследствии компилируется. Важным параметром оптимизации является разделение параметров моделирования на изменяемые во время запуска и неизменные. Первые позволяют уменьшить число пересборок исполняемого файла, последние позволяют компилятору ввести дополнительную оптимизацию. В качестве компромисса был выбран один изменяемый параметр: отношение сигнал-шум. Все остальные параметры фиксируются при сборке модели.

Для ускорения моделирования так же применялись распределённые вычисления. Была написана вспомогательная программа на языке MATLAB, которая осуществляла следующие операции:

- Вносила в модель значения всех неизменяемых параметров.
- Получала из базы данных параметры используемого кода по его идентификатору.
- Осуществляла сборку модели.
- Отправляла полученный файл и набор изменяемых параметров на центральный сервер, который затем распределял работу на несколько компьютеров.
- Собирала полученные результаты и сохраняла их в базе данных ORACLE MySQL.

Данная вспомогательная программа может быть использована с любыми моделями после минимальных модификаций. На основе полученных с её помощью данных были построены все графики, приведённые в данной работе.

Использование распределённых вычислений и компиляции модели Simulink позволило экспериментально измерить корректирующую способность кода с высокой точностью. При некоторых отношениях сигнал-шум количество информационных бит достигало 10^8. Если во время моделирования возникал сбой в работе компьютера, терялись лишь промежуточные результаты для текущего набора параметров, а после перезагрузки расчёт продолжался автоматически.

Параметры моделирования были заданы в следующих диапазонах:

- Отношение сигнал-шум изменялось от 0 до 30 дБ с шагом от 0.25 до 1 дБ.
- Количество передающих антенн N всегда равнялось 4.
- Использовались следующие сигнально кодовые конструкции
  - приведённая в разделе 1.5.2,
  - построенные алгоритму C из раздела 1.4.4 над полями F_8 и F_{16},

– построенная с помощью алгоритма А, приведённого в разделе 1.4.3, подкод кода РС $[4, 3, 2]_8$.

- Количество приёмных антенн M 1, 2 или 4.
- Моделирование велось до достижения 10^3 или 10^4 ошибок или $10^6, 10^7$ или 10^8 переданных битов.

Кроме того было проведено моделирование кода со скоростью 5/4, который был получен увеличением длины информационного слова на N битов, отвечающие за знак сигналов, отправленных с каждой передающей антенны. То есть исходное кодовое слово $\mathbf{C}$ домножалось на матрицу $diag(i_1, \ldots, i_N), i_k = \pm 1$. Приём происходил по максимуму правдоподобия.

1.8.1. Результаты моделирования

Теоретические кривые строились с помощью стандартных функций пакета MATLAB, соответствующих формулам, описанным, например, в книге [11]. На графиках они представлены сплошными линиями. Порядок разнесения для этих кривых равен 1,2,4,8,16 сверху вниз.

Важным параметром для сравнения корректирующей способности различных кодов является порядок пространственного разнесения. Он определяется как $C_d = -\lim_{\gamma\to\infty} \frac{log(P_e)}{log(\gamma)}$, где P_e - вероятность битовой ошибки при отношении сигнал-шум γ. Подробнее про порядок пространственного разнесения (в англ. diversity) можно прочитать в [30]. Максимальным значением этого параметра является произведение NM. Назовём этот порядок разнесения и коды, ему соответствующие, оптимальными. Такими кодами являются STBC коды [14].

На всех графиках результаты моделирования для каждого кода представлены в виде трёх кривых. Им соответствуют значения $M = 1, 2, 4$, при чём результат моделирования при меньшем M располагается на графике выше.

Оценим эффективный порядок разнесения для PRF-кодов по графику 1.2: при $M = 1, 2$ эффективный порядок разнесения PRF-кода соответствует поло-

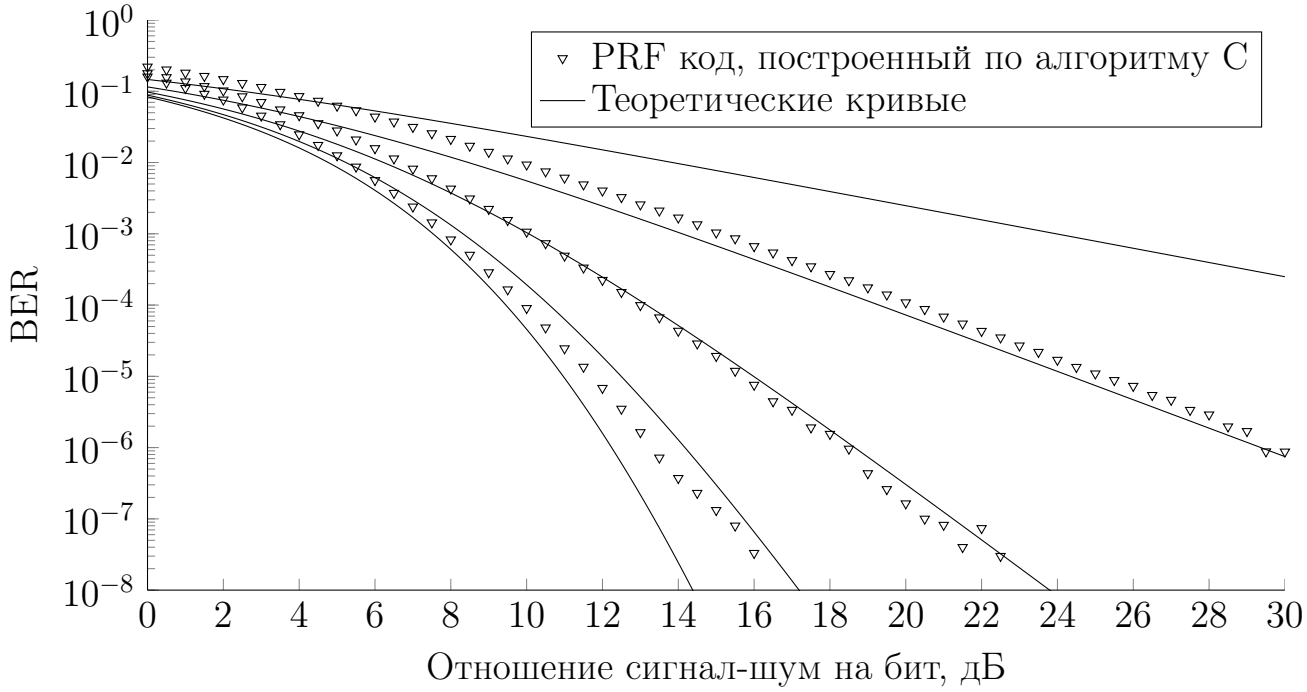

Рис. 1.2. Сравнение результатов моделирования корректирующей способности PRF-кодов и теоретической оценки для кодов, таких как [14]

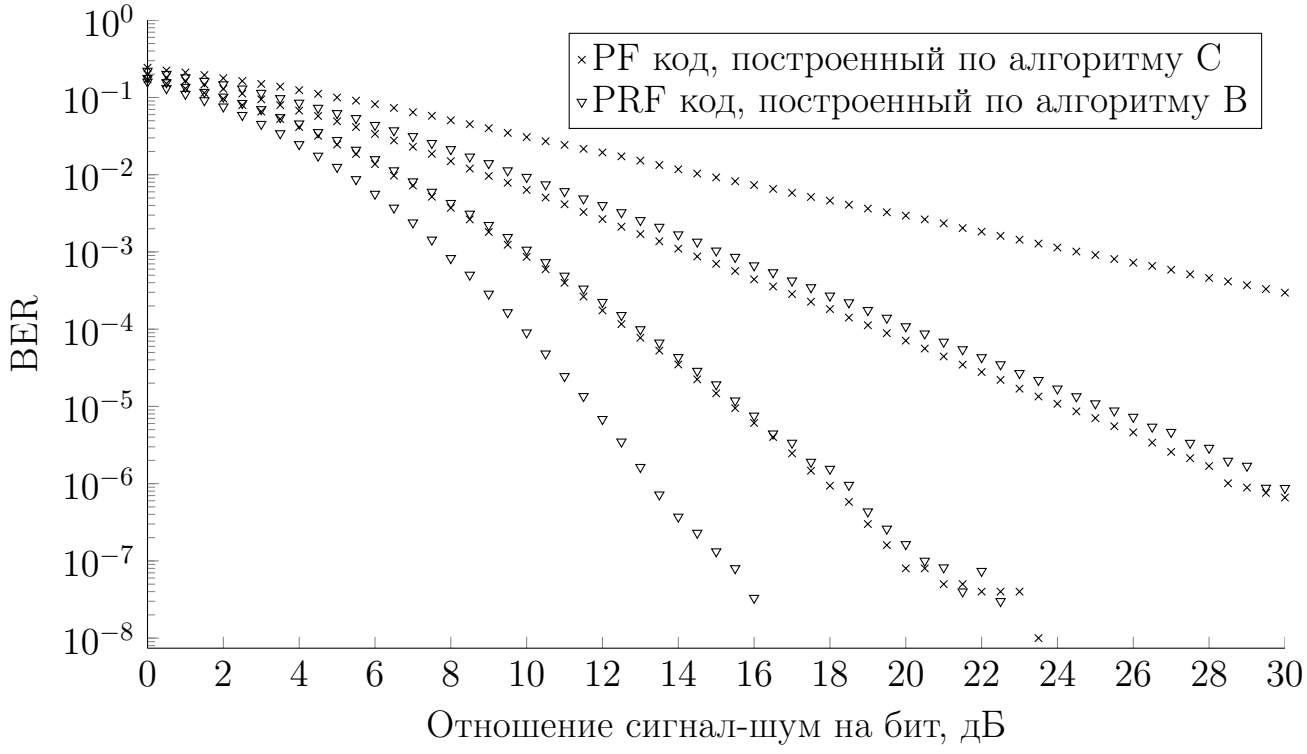

Рис. 1.3. Сравнение результатов моделирования PF- и PRF-кодов

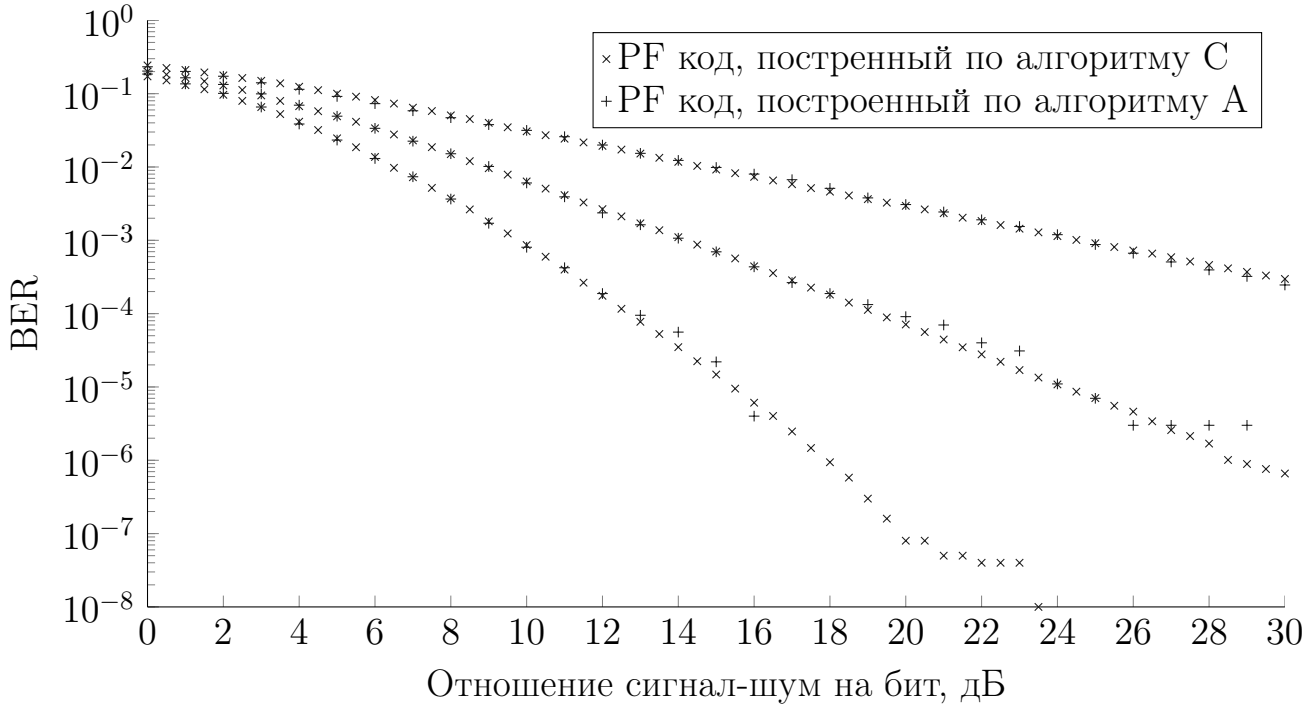

Рис. 1.4. Сравнение корректирующих способностей PF-кодов, построенных по алгоритмам A и C

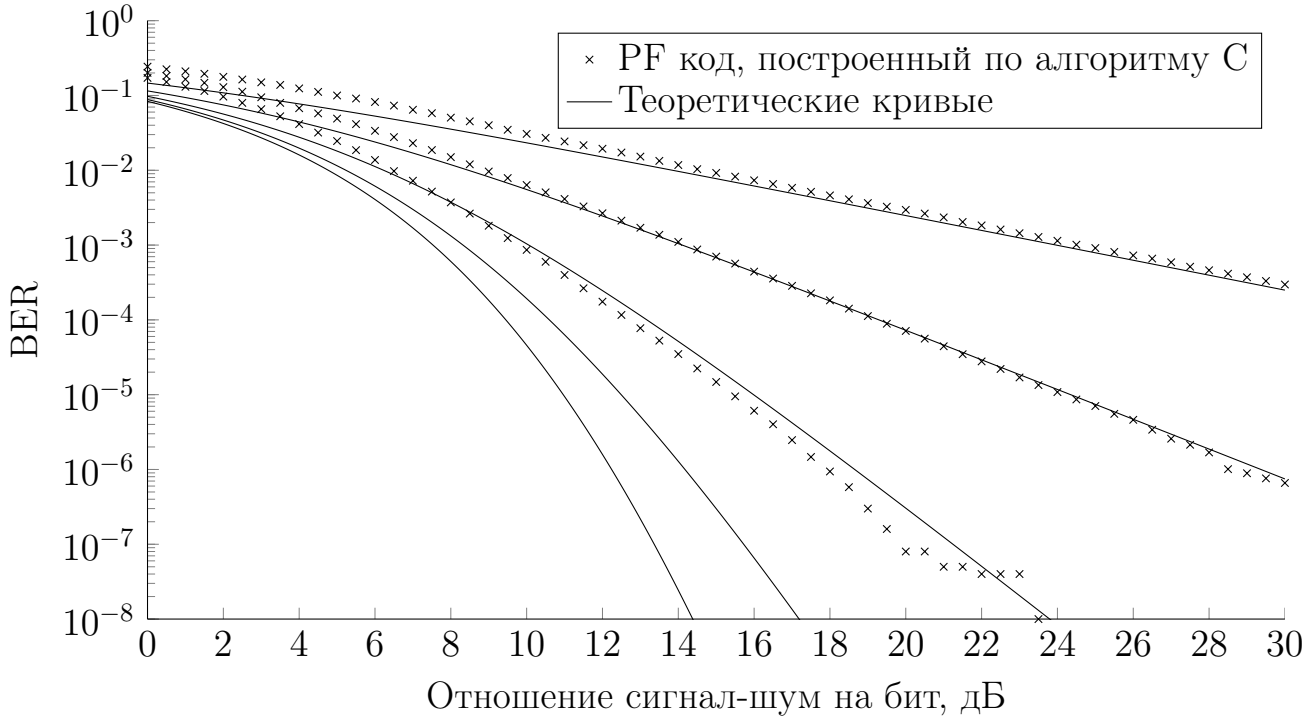

Рис. 1.5. Сравнение результатов моделирования корректирующей способности PF-кодов и теоретической оценки для оптимальных кодов

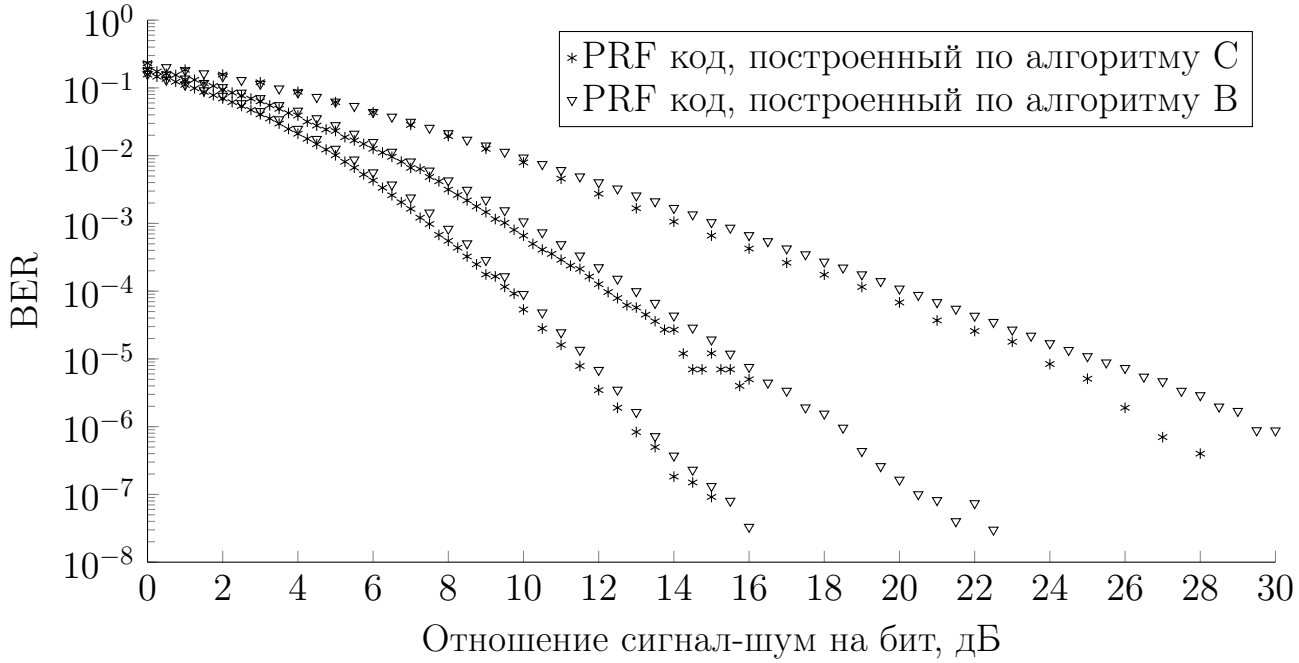

Рис. 1.6. Сравнение результатов моделирования PRF-кодов, полученных по алгоритмам B и C

вине от оптимального. Но при $M = 4$ PRF-код становится оптимальным. Таким образом можно сделать вывод, что корректирующая способность PRF-кодов существенно зависит от количества приёмных антенн и при некоторых параметрах становится оптимальной. При этом скорость PRF-кода ниже единицы. Положительным свойством PRF-кода является наличие алгоритма построения для любого заданного T и N.

На рис. 1.3 представлено сравнение PRF-кода, приведённого в разделе 1.5.2, и PF-кода, построенного по алгоритму C. Сверху вниз $M = 1, 2, 4$. Из графика видно, что корректирующая способность PRF-кода соответствует корректирующей способности PF-кода при вдвое большем числе приёмных антенн. Таким образом порядок разнесения для PRF-кода в два раза больше.

На рис. 1.4 представлено сравнение PF-кодов, полученных по алгоритмам A и C. Первый PF-код получен как подкод кода Рида-Соломона. Данный метод хорош своей простотой, однако мощность полученного кода составляет лишь 50. Кроме того, возможна адаптация алгоритма декодирования PC кода для данного случая. Код, построенный по алгоритму C, имеет большую мощность

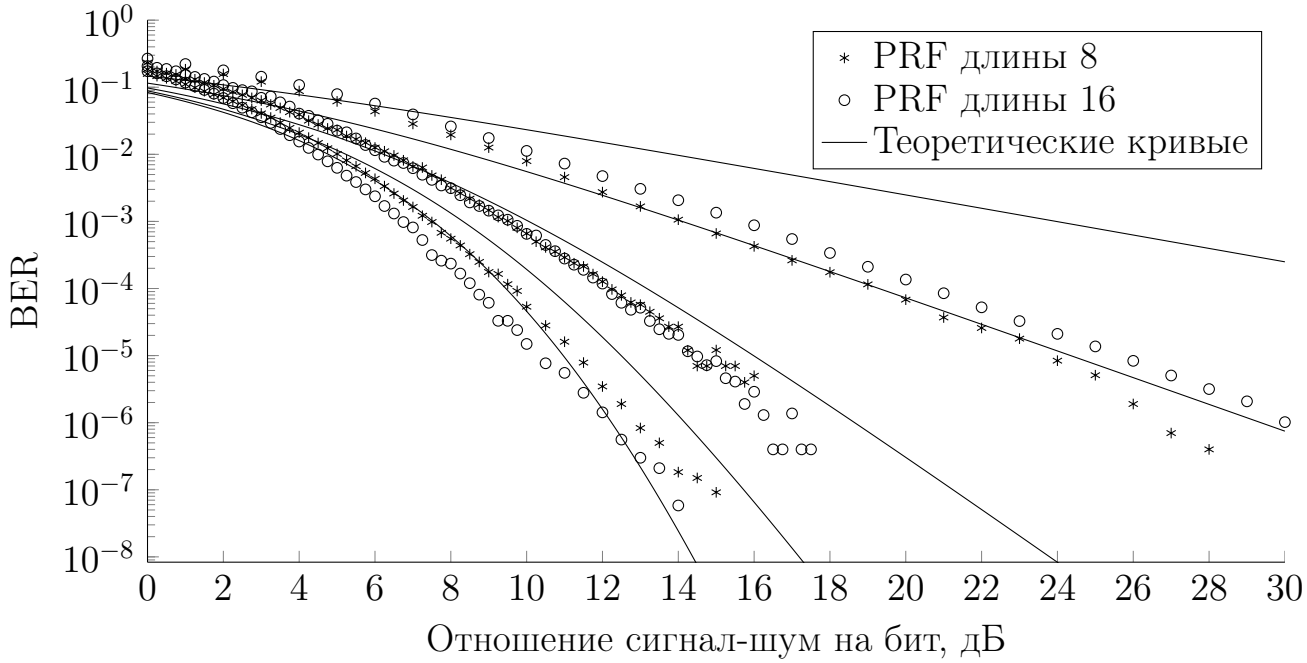

Рис. 1.7. Сравнение результатов моделирования PRF-кодов, полученных для $T = 8$ и 16

– 120. Этот код имеет более высокую скорость, чем максимальный PRF-код, но меньшую корректирующую способность. К недостаткам PF-кода относится невозможность независимой “демодуляции” отдельных столбцов кода, а также изменения фазы отдельных столбцов для увеличения скорости кода.

Обозначения на рис. 1.5 такие же, как на предыдущих рисунках. Эффективный порядок разнесения PF-кода соответствует четверти от оптимального. Таким образом PF-код обладает невысокой корректирующей способностью, однако он имеет простые алгоритмы построения и может иметь достаточно высокую скорость.

На рис. 1.6 сравниваются корректирующие способности PRF-кодов, полученных по алгоритмам B и C. Различие в корректирующей способности объясняется разницей в спектре расстояний кодов. Несмотря на то, что оба кода имеют одинаковое минимальное Хэммингово расстояние, равное 2, у кода, построенного по алгоритму C меньше пар слов, находящихся на расстоянии 2 (95 против 206). По этой причине его корректирующая способность стабильно выше, хотя и ненамного.

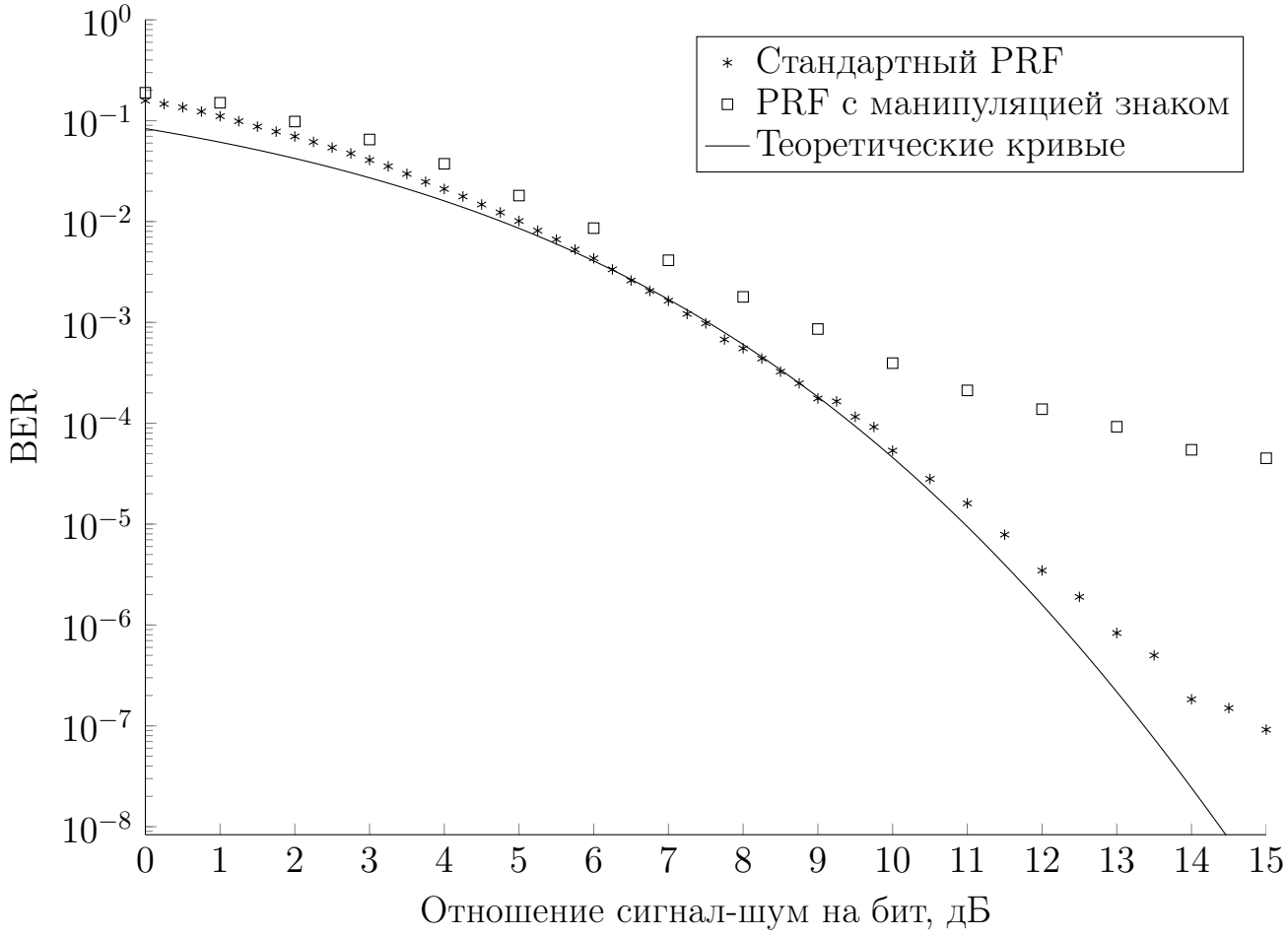

Рис. 1.8. Корректирующая способность кода, изменяющего знаки сигналов, передающихся с каждой антенны

Зависимость корректирующей способности PRF-кодов от параметра T (размер матрицы Адамара) представлена на рис. 1.7. Этот параметр также называется длиной PRF-кода. При увеличении длины корректирующая способность улучшается лишь асимптотически и при большом количестве приёмных антенн M. При малых отношениях сигнал-шум более короткий PRF-код показывает лучшую корректирующую способность. Но для $M = 4$ код с $T = 16$ становится лучше для отношения сигнал-шум выше 5 дБ.

На рис. 1.8 представлено изменение корректирующей способности PRF-кода при использовании манипуляции знака в случае $T = 8, M = 4$. Теоретическая кривая соответствует порядку разнесения 16. Исходный PRF-код был построен по алгоритму C и имел скорость 3/4. Добавление возможности изменять фазу отдельных столбцов кода позволило увеличить скорость до 5/4. Су-

ществование кодов со скоростью больше 1 возможно вследствие использования нескольких передающих антенн и условия (1.5). Корректирующая способность при увеличении скорости ухудшается, но в показанном случае различие составляет 1 дБ. При других параметрах канала различие получалось выше, от 2 до 4 дБ.

1.9. Линейные пространственно-временные коды

Раннее описанные PF и PRF-коды не позволяют построить хорошие линейные коды. Поэтому в этом разделе мы опишем известные линейные пространственно-временные коды.

1.9.1. Решётки и их свойства

В данном разделе используются обозначения, пересекающиеся с обозначениями из предыдущего раздела. Однако эти обозначения относятся к разным объектам, хотя и изоморфным между собой. Для того, чтобы показать удобство описания и исследования пространственно-временных кодов в виде решёток, запишем (1.2) в матричной форме, отличной от (1.3). Для этого представим $c_{t,n}$ в виде столбца $c_{2tN+2n} = \operatorname{Re} c_{t,n}$, $c_{2tN+2n+1} = \operatorname{Im} c_{t,n}$, а $r_{t,m}$ в виде $r_{2tM+2m} = \operatorname{Re} r_{t,m}$, $r_{2tM+2m+1} = \operatorname{Im} r_{t,m}$. Тогда соотношение между этими двумя столбцами, определяемое (1.2) записывается в виде:

$$\mathbf{r} = \mathbf{H}\mathbf{C} + \mathcal{N}, \tag{1.27}$$

так соотношение между $\mathbf{r}$ и $\mathbf{C}$ должно быть аффинным. $\mathbf{H}$ — некая матрица размера $2NT \times 2MT$, а $\mathcal{N}$ — вектор шума, полученный из $\eta_{t,m}$ также, как вектор $\mathbf{r}$ — из $r_{t,m}$.

Отображение $\alpha_{m,n} \to \mathbf{H}$ описывается следующими двумя предложениями. Доказываются они простой подстановкой.

Предложение 1. *Пусть* $\underline{x}_1, \ldots, \underline{x}_n$ *и* $\underline{b}_1, \ldots, \underline{b}_n$ *— некоторые строки одинаковой длины, а* $\mathbf{H}$ *— некоторая матрица. Тогда выражения*

$$\left\| \begin{array}{c} \underline{x}_1 \\ \underline{x}_2 \\ \vdots \\ \underline{x}_n \end{array} \right\| \mathbf{H} = \left\| \begin{array}{c} \underline{b}_1 \\ \underline{b}_2 \\ \vdots \\ \underline{b}_n \end{array} \right\|$$

и

$$\left\| \begin{array}{cccc} \mathbf{H}^T & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}^T & \cdots & \mathbf{0} \\ & & \ddots & \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{H}^T \end{array} \right\| \left\| \begin{array}{c} \underline{x}_1^T \\ \underline{x}_2^T \\ \vdots \\ \underline{x}_n^T \end{array} \right\| = \left\| \begin{array}{c} \underline{b}_1^T \\ \underline{b}_2^T \\ \vdots \\ \underline{b}_n^T \end{array} \right\|$$

равносильны.

Предложение 2. *Для любых* a_{ij}, x_i, b_j*, равенство*

$$\left\| \begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & & \cdots & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{array} \right\| \left\| \begin{array}{c} x_1 \\ x_2 \\ \vdots \\ x_n \end{array} \right\| = \left\| \begin{array}{c} b_1 \\ b_2 \\ \vdots \\ b_m \end{array} \right\|$$

равносильно равенству

$$\left\| \begin{array}{cc|cc|c|cc} a_{11}^{(\mathrm{Re})} & -a_{11}^{(\mathrm{Im})} & a_{12}^{(\mathrm{Re})} & -a_{12}^{(\mathrm{Im})} & \cdots & a_{1n}^{(\mathrm{Re})} & -a_{1n}^{(\mathrm{Im})} \\ a_{11}^{(\mathrm{Im})} & a_{11}^{(\mathrm{Re})} & a_{12}^{(\mathrm{Im})} & a_{12}^{(\mathrm{Re})} & \cdots & -a_{1n}^{(\mathrm{Im})} & a_{1n}^{(\mathrm{Re})} \\ \hline a_{21}^{(\mathrm{Re})} & -a_{21}^{(\mathrm{Im})} & a_{22}^{(\mathrm{Re})} & -a_{22}^{(\mathrm{Im})} & \cdots & a_{2n}^{(\mathrm{Re})} & -a_{2n}^{(\mathrm{Im})} \\ a_{21}^{(\mathrm{Im})} & a_{21}^{(\mathrm{Re})} & a_{22}^{(\mathrm{Im})} & a_{22}^{(\mathrm{Re})} & \cdots & -a_{2n}^{(\mathrm{Im})} & a_{2n}^{(\mathrm{Re})} \\ \hline \cdots & & & & \cdots & & \\ \hline a_{m1}^{(\mathrm{Re})} & -a_{m1}^{(\mathrm{Im})} & a_{m2}^{(\mathrm{Re})} & -a_{m2}^{(\mathrm{Im})} & \cdots & a_{mn}^{(\mathrm{Re})} & -a_{mn}^{(\mathrm{Im})} \\ a_{m1}^{(\mathrm{Im})} & a_{m1}^{(\mathrm{Re})} & a_{m2}^{(\mathrm{Im})} & a_{m2}^{(\mathrm{Re})} & \cdots & -a_{mn}^{(\mathrm{Im})} & a_{mn}^{(\mathrm{Re})} \end{array} \right\| \left\| \begin{array}{c} x_1^{(\mathrm{Re})} \\ x_1^{(\mathrm{Im})} \\ \hline x_2^{(\mathrm{Re})} \\ x_2^{(\mathrm{Im})} \\ \hline \vdots \\ \hline x_n^{(\mathrm{Re})} \\ x_n^{(\mathrm{Im})} \end{array} \right\| = \left\| \begin{array}{c} b_1^{(\mathrm{Re})} \\ b_1^{(\mathrm{Im})} \\ \hline b_2^{(\mathrm{Re})} \\ b_2^{(\mathrm{Im})} \\ \hline \vdots \\ \hline b_m^{(\mathrm{Re})} \\ b_m^{(\mathrm{Im})} \end{array} \right\|$$

где $x^{(\mathrm{Re})}$ *и* $x^{(\mathrm{Im})}$ *— действительная и мнимая части числа* x*.*

Чаще всего пространственно-временные коды проектирует в следующем виде:

$$\mathbf{C} = \mathbf{M}\tilde{\mathbf{s}}, \tag{1.28}$$

где $\mathbf{s}$ — вектор длины $2K$, $\tilde{s}_{2i} + i\tilde{s}_{2i+1} \in \mathcal{M}$, а $\mathcal{M}$ — множество точек некоторой модуляции. В данной работе будет использоваться только M^2 квадратурная амплитудная модуляция (КАМ), поэтому $\tilde{s}_k \in \mathcal{M}_{\mathbb{R}}$ — точки амплитудной модуляции (АМ) порядка M.

Для M^2-КАМ справедливо равенство $\tilde{s}_k = \sqrt{\frac{6}{M^2-1}}\left(s_k - \frac{M-1}{2}\right)$, где $s_k = \overline{0, M-1}$. Подставив это выражение в (1.28) и (1.27) получим

$$\mathbf{r} = \mathbf{HM}\sqrt{\frac{6}{M^2-1}}\left(\mathbf{s} - \frac{M-1}{2}\right) + \mathcal{N} = \mathbf{H}_0(\mathbf{s} - c_0) + \mathcal{N} \tag{1.29}$$

Таким образом не только сам пространственно-временной код является частью многомерной решётки, но и принятое из канала слово также лежит на некоторой решётке, определяемой текущим состоянием канала. Задачей декодера становится поиск ближайшей точки решётки. Кроме того, задача построения пространственно-временного кода сводится к задаче выбора многомерной решётки, обладающей некоторыми свойствами. Прежде, чем обсуждать требуемые свойства, мы опишем основные понятия и свойства решёток.

Определение 4. Пусть $\mathbf{v}_1, \ldots, \mathbf{v}_m$ — линейно-независимые вектора в пространстве $\mathbb{R}^n$ $(m \leq n)$. Тогда набор точек

$$\Lambda = \{x = \sum_{i=1}^{m} \lambda_i \mathbf{v}_i,\ \lambda_i \in \mathbb{Z}\}$$

будем называть *решёткой* размерности m, а $\mathbf{v}_1, \ldots, \mathbf{v}_m$ — *базисом* этой решётки.

Нужно заметить, что разные базисы могут определять одну и ту же решётку.

Определение 5. Матрицу

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \cdots & & \cdots & \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

назовём *порождающей матрицей* решётки. Матрицу $G = MM^T$ назовём матрицей Грамма решётки.

Таким образом, мы можем определить решётку через её порождающую матрицу:

$$\Lambda = \{\mathbf{x} = \lambda M | \lambda \in \mathbb{Z}^m\}$$

Определение 6. *Детерминантом решётки* Λ называется детерминант матрицы Грамма G:

$$\det(\Lambda) = \det(G)$$

Детерминант является инвариантом решётки, он не зависит от выбора базиса. Именно детерминант является главным критерием корректирующей способности кода [18].

1.9.2. Пространственно-временной Golden код

Существует великое множество пространственно временных кодов, имеющих различные характеристики и ограничения. Многие из них описаны в [30]. Здесь мы приведём лишь некоторые известные конструкции.

Кодовые слова «бесконечного» Golden кода задаются в форме (1.3):

$$\mathcal{G}_\infty = \left\{ \mathbf{X} = \frac{1}{\sqrt{5}} \left\| \begin{array}{cc} \alpha(a+b\theta) & \alpha(c+d\theta) \\ \gamma\overline{\alpha}(c+d\overline{\theta}) & \overline{\alpha}(a+b\overline{\theta}) \end{array} \right\| : a,b,c,d \in \mathbb{Z}[i] \right\}, \qquad (1.30)$$

где $\theta = \frac{1+\sqrt{5}}{2}$, $\overline{\theta} = \frac{1-\sqrt{5}}{2}$, $\alpha = 1+i-i\theta$, $\overline{\alpha} = 1+i-i\overline{\theta}$, $\gamma = i$. При использовании на практике, $a, b, c, d \in \mathcal{M}$ выбираются в соответствии с некоторой модуляцией. Но

для исследования свойств Golden кода удобнее использовать его бесконечный вариант.

Важным свойством Golden кода является его неисчезающий детерминант [16]:

$$\delta_{\min}(\mathcal{G}_\infty) = \min_{\mathbf{X}\in\mathcal{G}_\infty} \det(\mathbf{X}) = \frac{1}{5} \tag{1.31}$$

Данное свойство означает, что в первом приближении вероятность неправильного приёма зависит только от минимального Евклидова расстояния модуляции, но не от её порядка. То есть, вероятность неправильного приёма при повышении порядка модуляции растёт медленно.

Важно заметить, что минимальный детерминант конечного Golden кода больше или равен минимальному детерминанту бесконечного. Для 4-КАМ и 16-КАМ он равен $\delta_{\min}(\mathcal{G}_4) = \delta_{\min}(\mathcal{G}_{16}) = 16/5$ [16].

Порождающая матрица комплексной решётки, соответствующей Golden коду, равна

$$\mathbf{M}_{\mathbb{C}} = \frac{1}{\sqrt{5}} \begin{Vmatrix} \alpha & \alpha\theta & 0 & 0 \\ 0 & 0 & \alpha & \alpha\theta \\ 0 & 0 & \gamma\overline{\alpha} & \gamma\overline{\alpha}\overline{\theta} \\ \overline{\alpha} & \overline{\alpha}\overline{\theta} & 0 & 0 \end{Vmatrix}. \tag{1.32}$$

Для получения действительной порождающей матрицы можно воспользоваться предложением 2.

1.9.3. Вложенные коды

Для построения вложенных Golden кодов мы воспользуемся следующим разложением:

$$\mathcal{G}_\infty = [\mathcal{G}_\infty/2\mathcal{G}_\infty] + 2\mathcal{G}_\infty,$$

где $2\mathcal{G}_\infty$ — подкод $\mathcal{G}_\infty$, полученный из него умножением всех его слов на 2, $\mathcal{G}_\infty/2\mathcal{G}_\infty$ — соответствующая ему фактор группа, а $[\mathcal{G}_\infty/2\mathcal{G}_\infty]$ — множество представителей смежных классов подкода. В [17] показано, что данный подкод имеет

большее детерминантное расстояние, а потому должен иметь лучшую корректирующую способность. Так же там показано, что фактор-группа $\mathcal{G}_\infty/2\mathcal{G}_\infty$ изоморфна кольцу квадратных матриц размера 2×2 над полем $\mathbb{F}_2[i]$, $\mathcal{M}_2(\mathbb{F}_2[i])$. Данный изоморфизм очень важен для описания каскадной конструкции, в дальнейшем он будет использован при построении биекции между $\mathcal{G}_4$ и $GF(2^8)$.

Для конечного кода можно записать

$$\mathcal{G}_{16} = [\mathcal{G}_\infty/2\mathcal{G}_\infty] + 2\mathcal{G}_4, \tag{1.33}$$

при этом описанные ранее свойства фактор-группы и подкода сохраняются, а $2\mathcal{G}_4$ очевидно является подкодом кода $\mathcal{G}_{16}$. При этом мы можем рассматривать $\mathcal{G}_4 \leftrightarrow [\mathcal{G}_\infty/2\mathcal{G}_\infty]$.

Алгоритм кодирования кода в таком разложении может быть описан так:

1 На вход кодера поступают 16 информационных бит.

2 Первые 8 бит используются для выбора смежного класса. Обозначим его представителя $s^{(1)}$.

3 Вторые 8 бит кодируются кодом $\mathcal{G}_4$. Полученное кодовое слово обозначим $s^{(2)}$.

4 Результатом кодирования будет слово $s^{(1)} + 2s^{(2)}$.

При декодировании мы будем сначала декодировать слово кодом $\mathcal{G}_{16}$, определяя лишь смежный класс и его представителя и отбрасывая слово кода $\mathcal{G}_4$. Ошибки в выборе смежного класса будут исправлены внешним кодом, после чего мы вычтем его представителя из полученного из канала слова и декодируем результат подкодом $2\mathcal{G}_4$. Подробнее декодирование обобщённой каскадной конструкции будет описан в разделе 3.2. А декодирование отдельных кодов описано в следующем разделе.

1.10. Декодирование

Для декодирования конкретного Golden кода используется сферический декодер [32]. Мы не будем приводить полное описание данного алгоритма здесь, а лишь опишем его структуру. Пусть получен вектор $\mathbf{r} = \mathbf{Hs} + \eta$, где $\mathbf{r} \in \mathbb{R}^N, \mathbf{H} \in \mathbb{R}^{N \times K}$ и $\mathbf{c}$ известны, а $\mathbf{s} \in \mathcal{M} \subset \mathbb{Z}^K$ — искомое. η — шум. Задачей данного алгоритма является поиск $\arg\min_{\mathbf{s} \in \mathcal{M}} (\mathbf{Hs} - \mathbf{r})^T (\mathbf{Hs} - \mathbf{r})$. Данная задача является NP-полной при отсутствии ограничений на структуру матрицы $\mathbf{H}$, но в практических случаях многоантенных систем сложность можно считать полиномиальной [32].

1 Построим проекцию вектора $\mathbf{r}$ на пространство решений:

$$\tilde{\mathbf{s}} = (\mathbf{H}\mathbf{H}^T)^{-1}\mathbf{r} = (\mathbf{H}\mathbf{H}^T)^{-1}\mathbf{H}\mathbf{s} + (\mathbf{H}\mathbf{H}^T)^{-1}\eta,$$

где $\mathbf{s}$ — неизвестное решение.

2 Теперь задачу можно переформулировать как поиск

$$\arg\min_{\mathbf{s} \in \mathcal{M}} \{(\mathbf{s} - \tilde{\mathbf{s}})^T \mathbf{H}^T \mathbf{H} (\mathbf{s} - \tilde{\mathbf{s}})\} = \arg\min_{\mathbf{s} \in \mathcal{M}} \|\mathbf{H}(\mathbf{s} - \tilde{\mathbf{s}})\| = \arg\min_{\mathbf{s} \in \tilde{\mathcal{M}}} \|\mathbf{Hs}\|,$$

где $\tilde{\mathcal{M}} = \mathcal{M} - \tilde{s}$. Это задача поиска точки минимальной нормы, заданной матрицей $\mathbf{H}$.

3 Воспользуемся разложением Холецкого и получим $\mathbf{H}^T\mathbf{H} = \mathbf{U}^T\mathbf{U}$, где $\mathbf{U}$ — верхне-треугольная матрица.

4 Поставим вспомогательную задачу поиска одного из $\mathbf{s} \in \tilde{\mathcal{M}}$, такого что $\|\mathbf{Us}\| < C$, где C — некий радиус, то есть задачу поиска точки внутри сферы.

5 Благодаря верхнетреугольной структуре, мы можем последовательно перебирать значения отдельных координат, пока не найдём все точки, лежащие внутри сферы радиуса C.

6 Выберем из этих точек ближайшую к центру сферы. Она и будет решением задачи.

7 Если таких точек не было найдено, декодирование завершается отказом.

В литературе описано множество вариантов данного алгоритма, требующих меньшего количества операций [19]. Однако общая схема алгоритма сохраняется, а также его итеративная структура. Последнее означает, что сферический декодер получает некоторую последовательность точек, которая сходится к правильному решению. Данное свойство мы используем, чтобы получить некую метрику «надёжности» решения.

При декодировании внешних кодов в обобщённой каскадной конструкции нам понадобятся различные варианты расстановки стираний, а значит нам необходимо определить некоторую метрику «надёжности» решений внутренних кодов. В [38] показано, что хорошим кандидатом для такой метрики является разность расстояний между от ближайшего решения до принятой точки и от второго по удалённости решения до принятой точки. Но для вычисления данной метрики необходимо проводить декодирование внутреннего кода дважды.

В данной работе предлагается более простая метрика. На шаге 5 мы получали сходящуюся последовательность точек, сходящуюся к принятой. Разность удалённости последней и предпоследней точки в данной последовательности мы и будем считать метрикой надёжности. Если эта последовательность содержит менее двух членов, принятый символ считается надёжным. Вычисление такой метрики не увеличивает сложность декодирования.

Этим мы заканчиваем описание внутренних кодов и их декодирования и переходим к внешним кодам.

1.10.1. Моделирование распределения метрики

Хорошая метрика надёжности символов должна быть большой для неправильно декодированных символов и малой — для правильно декодированных.

Чтобы отобразить «качество» выбранной метрики, на рис. 1.9 представлены функции распределения значения метрики, то есть количество символов, метрика надёжности которых меньше указанной. Стирания вводятся для наименее надёжных символов. Можно либо стирать все символы, надёжности которых меньше критической надёжности, либо n самых ненадёжных символов. Поэтому в каждой точке данные функции показывают, сколько символов будет стёрто, если выбрать эту точку в качестве критической.

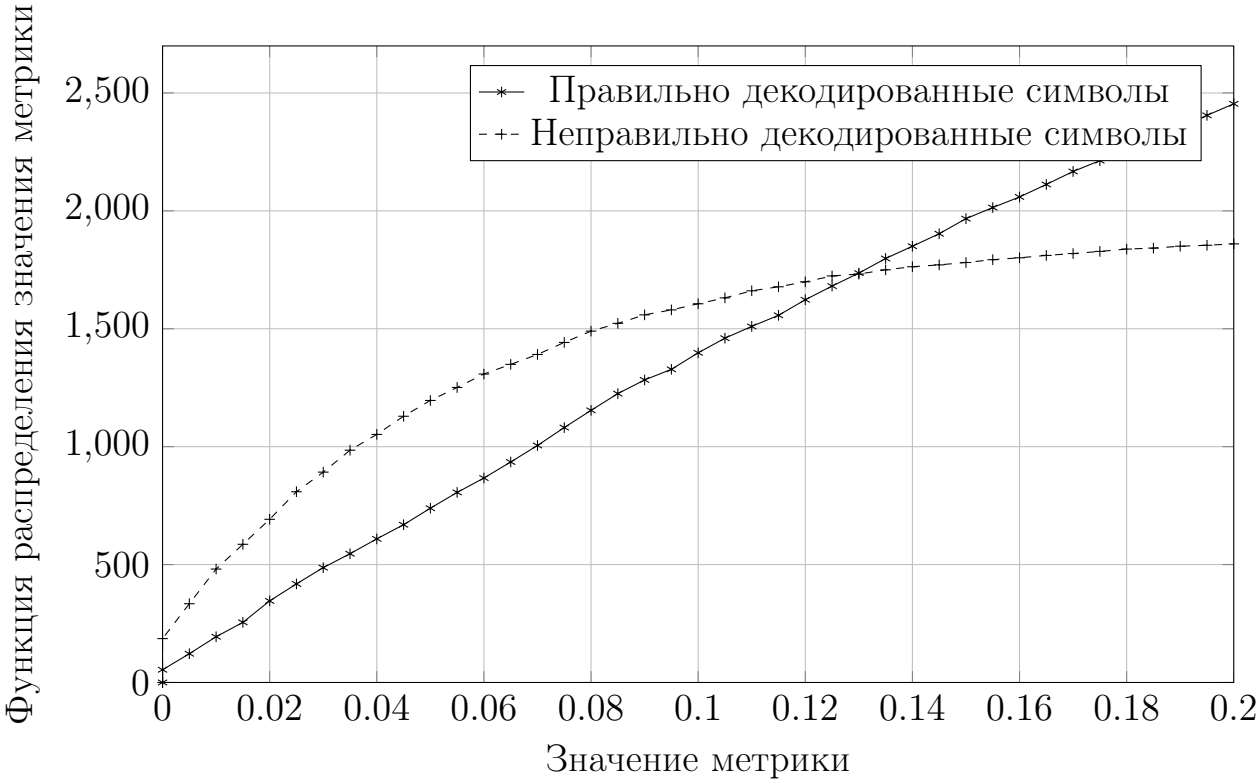

Рис. 1.9. Распределение значения предложенной метрики для отношения сигнал-шум 11 дБ на бит

При моделировании использовался Golden код с модуляцией 16-QAM и двумя приёмными антеннами. Напомним, что Golden используется с двумя передающими антеннами, имеет длину 2 и передаёт 2 символа за 1 временной интервал. Таким образом, скорость кода составляет 8 бит за временной интервал. При моделировании использовался Рэлеевский канал.

Моделирование проводилось при отношении сигнал-шум 11 дБ на бит. Всего было промоделировано 14689 кодовых слов, из которых 12209 было декодиро-

вано правильно, а 2480 — ошибочно. Так как предложенная метрика может быть вычислена не для всех кодовых слов, важно, чтобы она была вычислена для большинства ошибочно декодированных кодовых слов. И действительно, лишь для 522 из 2480 ошибочно декодированных кодовых слов не удалось вычислить значение надёжности. В то же время, из 12209 правильно декодированных кодовых слов метрика была неизвестна для 8309.

Из рис. 1.9 видно, что для диапазона критических значений надёжности 0–0.1 неправильно декодированных символов будет стёрто больше, чем правильно декодированных. Из этого можно заключить, что использование предложенной метрики надёжности может повысить корректирующую способность внешних кодов.

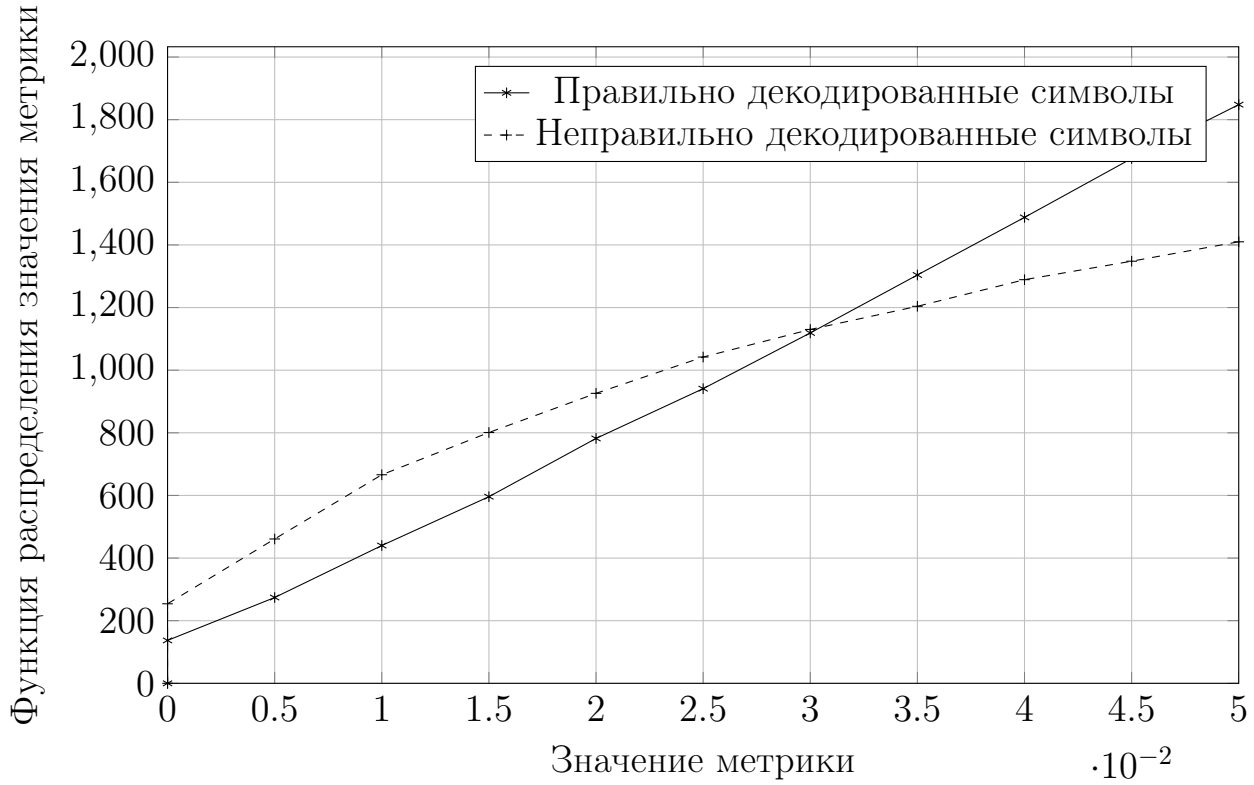

Рис. 1.10. Распределение значения предложенной метрики для отношения сигнал-шум 14 дБ на бит

Для сравнения эффективности использования предложенной метрики при разных отношения сигнал-шум мы повторили предыдущее моделирование для отношения сигнал-шум 14 дБ на бит. Результаты представлены на рис. 1.10. Из

рисунка можно заключить, что метрика остаётся эффективной в таких условиях. Однако, диапазон эффективных критических значений надёжности сузился. Поэтому в следующих главах мы будем не будем выбирать критическое значение надёжности, а вместо этого стирать несколько самых ненадёжных символов. В данных условиях метрика не была вычислена лишь для 366 из 2213 неправильно декодированных слов.

1.11. Пространственно-временные коды для систем с 4 передающими антеннами

Существует обобщение Golden кодов для систем с большим числом антенн под названием Perfect STBC[21] (совершенные пространственно-временные коды). Слово «совершенные» в их названии никак не связано с понятием совершенных алгебраических кодов (коды, лежащие на границе Хэмминга). Данные коды имеют очень большую мощность, что осложняет их использование в обобщённых каскадных конструкциях. Поэтому в данной работе мы используем другие пространственно-временные коды.

Коды DAST (Diagonal Algebraic Space-Time — диагональные алгебраические пространственно-временные коды) [28] при использовании в системах с четырьмя передающими антеннами имеют ту же мощность, что и Golden коды. Поэтому их можно использовать в каскадных системах с теми же внешними кодами. Их кодирование можно описать следующим образом:

$$\mathbf{s} = \mathrm{diag}(x_1, \ldots, x_N)\mathcal{H}, \quad (x_1, \ldots, x_N)^T = \mathbf{M}_N(i_1, \ldots, i_N)^T, \tag{1.34}$$

где $\mathcal{H}$ — $N \times N$ матрица Адамара, $i_1, \ldots, i_N$ — информационные символы, а $\mathbf{M}_N$ — выбранная матрица поворота. В [28] описано несколько способов выбора матрицы $\mathbf{M}_N$, но для просты в данной работе мы будем использовать матрицу поворота совершенных пространственно-временных кодов (в [21] она обозначена $\mathbf{R}$).

1.12. Выводы к главе

- Предложена новая сигнально-кодовая конструкция для МАПП. Сформулировано условие декодируемости кодов для МАПП. Введено определение PF- и PRF-кодов. Предложена конструкция этих кодов, основанная на последовательностях столбцов матрицы Адамара, и её удобное представление в поле $\mathbb{F}_T$. Даны верхняя и нижняя границы мощности PF- и PRF-кодов. Предложены и исследованы алгоритмы построения PF- и PRF-кодов. С их помощью построены коды, достигающие верхнюю границу мощности PF- и PRF-кодов.

- Предложена метрика надёжности для пространственно-временных кодов, декодируемых сферическим декодером. Эффективность использования данной метрики для внесения стираний продемонстрирована для Golden кода при нескольких значений отношения сигнал-шум.

Глава 2

Каскадные коды

2.1. Обобщённые каскадные коды

Обобщённые каскадные коды являются кодовой комбинацией из двух систем кодов компонентов. Одна из этих систем называется системой внутренних кодов, другая — системой внешних кодов. Требуется, чтобы система внутренних кодов была вложенной, и чтобы указанные системы содержали одинаковое число кодов. В данной работе мы предлагаем обобщённую каскадную систему содержащую два внутренних кода и два внешних кода. При этом внешние коды имеют длину $n = 1024$ и построены над полем $GF(2^8)$.

Система внутренних кодов является вложенной, то есть каждый следящий код является подкодом предыдущего. В предложенной конструкции внутренних кодов всего два: некий код и его подкод. Воспользуемся следующим описанием: часть информационных символов первого кода задают смежный класс второго кода, а остальные задают кодовое слово второго кода. Первые мы будем называть информационными символами первого слоя, а вторые — информационными символами второго слоя.

Таким образом при декодировании внутреннего кода сначала декодируется слово первого кода. Затем с помощью полученного кодового слова мы вычисляем представителя смежного класса и вычитаем его из полученного слова. После этого мы можем декодировать слово второго внутреннего кода.

Опишем «способ объединения» внутренних и внешних кодов. В случае, когда внутренние и внешние коды имеют один алфавит, информационный символ i-го слоя j-го внутреннего кода равны j-у кодовому символу i-го внешнего кода. Мы ослабим данное ограничение, потребовав лишь, чтобы алфавит информаци-

онных символов внутреннего кода и алфавит внешнего кода были равномощны. Тогда мы сможем использовать взаимно-однозначное отображение между ними.

Для понимания требований к внутренним и внешним кодам необходимо описать общую структуру алгоритма декодирования. Полностью этот алгоритм будет описан далее, в разделе 3.2. При декодировании мы сначала определим кодовые символы внешнего кода с помощью декодирования внутреннего кода. После этого мы исправим все ошибки в слове внешнего кода и используем полученные символы для вычисления «поправки» к принятому слову внутренних кодов. Затем мы перейдём к декодированию следующего слоя. Если декодирование внешнего кода закончится отказом или ошибкой, дальнейшее декодирование не сможет привести к правильному кодовому слову. Другими словами для правильного декодирования обобщённой каскадной конструкции необходимо правильное декодирование всех внешних кодов.

Как известно, кодовое расстояние кода не превышает кодового расстояния любого его подкода. В предлагаемой конструкции кодовое расстояние второго внутреннего кода (подкода первого внутреннего кода) значительно больше кодового расстояния первого внутреннего кода.

Важным этапом построения хорошей обобщённой каскадной системы является «распределение» избыточности между внешними кодами, то есть выбор скоростей внешних кодов при фиксированной скорости обобщённой каскадной конструкции. Точное решение данной задачи очень трудно построить, поэтому в данной работе мы будем пользоваться простым эмпирическим критерием: вероятность правильного декодирования i-го внешнего кода при условии правильного декодирования всех предыдущих внешних кодов должна быть ограничена константой ϵ не зависящей от i.

2.2. Произведение кодов

В качестве внешних кодов в данной работе предлагается использовать произведения кодов Рида-Соломона.

Коды-произведения, также известные как итеративные коды, являются частным случаем каскадных кодов. Они были впервые предложены в работе [39] в качестве метода построения хороших кодов. Позже они были исследованы в качестве операции над алгеброй кодов в [40]. Длина произведения кодов равна произведению длин кодов, количество информационных символов — произведению количества информационных символов, а кодовое расстояние — произведению кодовых расстояний. Для исправления всех комбинаций ошибок кратности не больше половины расстояния можно использовать алгоритм декодирования каскадных кодов [41]. О некоторых других алгоритмах декодирования можно прочитать в [42, 43]. В данной работе мы рассмотрим более распространённый алгоритм декодирования — итеративный декодер.

Кодовые слова кода произведения обычно представляют в виде матрицы над полей F_q. Столбцы этой матрицы являются кодовыми словами первого кода-компонента, также называемого столбцовым кодом. Строки этой матрицы являются кодовыми словами второго кода-компонента, также называемого строчным кодом. Информационные символы расположены в левом верхнем углу данной матрицы.

В данной работе мы будем рассматривать только коды-произведения кодов Рида-Соломона $[n_c, k_c, d_c]$ и $[n_r, k_r, d_r]$ над полем F_q. Расстояние такого кода равно $d_r d_c$.

Кодер такого кода размещает информационные символы в левом верхнем углу (размера $k_c \times k_r$) матрицы кодового слова. После этого он кодирует первые k_c строк строчным кодом, размещая проверочные символы в правой части этих строк. Затем он кодирует все столбцы столбцовым кодом, размещая проверочные символы в нижней части этих столбцов.

2.2.1. Итеративный декодер

Опишем итеративный алгоритм декодирования кода-произведения:

1 Декодируем все столбцы принятого слова столбцовым кодом. Если декодирование завершилось отказом, результат декодирования игнорируется. Иначе полученное кодовое слово записывается на место исходного столбца.

2 Аналогично декодируем все строки строковым кодом.

3 Если полученная матрица отличается от входной для шага 1, повторить данную процедуру с шага 1.

Для такого алгоритма декодирования существует очевидная неисправимая комбинация ошибок, образованная подматрицей размера $\lceil \frac{d_c}{2} \rceil \times \lceil \frac{d_r}{2} \rceil$ не содержащей нулевых элементов и нулевыми элементами за её пределами. Вероятность появления такой комбинации ошибок и будет нижней оценкой на вероятность неправильного декодирования кода произведения.

2.2.2. Нижняя граница вероятности неправильного декодирования

Предложение 3. *Вероятность неправильного декодирования для итеративного декодера кода произведения больше или равна*

$$P_f \geq \binom{n_r}{e_r}\binom{n_c}{e_c} p^{e_r e_c}(1-p)^{n_r n_c - e_r e_c}, \tag{2.1}$$

где $e_r = \lceil \frac{d_r}{2} \rceil$, $e_c = \lceil \frac{d_c}{2} \rceil$, *а* n_r *и* n_c *длины строчного и столбцового кодов соответственно.*

Правая часть выражения (2.1) равна вероятности появления неисправимой комбинации ошибок, описанной выше.

Предложение 4. *Вероятность неправильного декодирования для итеративного декодера кода произведения больше или равна*

$$P_f \geq \binom{n_r}{e_r}\binom{n_c}{e_c} p^{e_r e_c}(1-p)^{n_r n_c - e_r e_c}(n_r n_c - e_r e_c)\frac{p}{1-p} \tag{2.2}$$

Доказательство. Данная нижняя граница определяет вероятность появления подматрицы без нулевых элементов и одной ошибки вне её. Никакая одна ошибка не может помочь исправить плотную подматрицу ошибок. Докажем этот факт.

Если ошибка располагается в столбце без других ошибок, она будет декодирована на первом шаге алгоритма соответствующим столбцовым кодом. В этом случае задача свелась к предыдущим.

Рассмотрим случай, когда она располагается в столбце, в котором есть e_c других ошибок. Если столбцовый код не сможет декодировать данной столбец, на следующем шаге алгоритма декодирования эту ошибку исправит строчный код, что сведёт комбинацию ошибок к предыдущей.

Пусть столбцовый код произвёл ошибочное декодирование столбца с e_c+1 ошибками. При этом он изменяет не более e_c-1 символов. Пусть он исправил a ошибок и внёс b. Тогда вес разности полученного и переданного кодового слова одного столбца будет $e_c + 1 - a + b \geq d$ в силу кодового расстояния. Данное неравенство выполняется лишь при $a = 0$, $b \geq d - e_c - 1 = \lfloor \frac{d}{2} \rfloor - 1 \geq e_c - 2$. Таким образом столбцовый декодер не может исправить ни одной ошибки, а все ошибки вне плотной подматрицы будут исправлены строчным кодом. □

Появление двух ошибок в столбце может привести к исправимой комбинации ошибок, поэтому при формулировке следующего утверждения мы вынуждены исключить такой случай.

Теорема 9. *Пусть $e_c < e_r$. Тогда вероятность неправильного декодирования для итеративного декодера кода произведения больше или равна*

$$P_f \geq \binom{n_r}{e_r}\binom{n_c}{e_c} p^{e_r e_c}(1-p)^{n_r n_c - e_r e_c} \times \\ \times \left(\sum_{t=0}^{e_c} \sum_{w=0}^{t} \binom{n_r n_c - e_r n_c}{t-w} \binom{e_r}{w} (n_c - e_c)^w \left(\frac{p}{1-p}\right)^t - (n_r - e_r)\left(\frac{p}{1-p}\right)^{e_c} \right) \tag{2.3}$$

Доказательство. Данная нижняя граница определяет вероятность появления подматрицы без нулевых элементов и t ошибок вне её. При $t < e_c$ такая добавка не может привести к появлению подматрицы большего размера, а потому ни одна комбинация ошибок не будет учтена дважды.

Как было показано в доказательстве предыдущего предложения, добавление двух ошибок в один столбец неисправимой комбинации ошибок может сделать её исправимой. Поэтому мы разделяем ошибки в столбцах подматрицы (их количество обозначено w) и ошибки в других столбцах (их количество равно $t-w$). Количество способов их расстановки первых равно $\binom{e_r}{w}(n_c - e_c)^w$, а вторых — $\binom{n_r n_c - e_r n_c}{t-w}$. Добавив суммирование по t и w и поправку, описанную ниже, получим (2.3).

При $t = e_c$ и $w = 0$ существуют $n_r - e_r$ «плохих» комбинаций дополнительных ошибок, приводящих к образованию подматрицы большего размера. Действительно, если все e_c ошибок расположены в одном столбце, в строках исходной плотной подматрицы ошибок, полученная комбинация ошибок будет представлена плотной подматрицей размера $(e_c+1)\times e_r$. Если мы не «запретим» такие комбинации ошибок, они будут учтены e_r раз. □

2.2.3. Итеративный декодер с внесением стираний

Нижняя граница, описанная в предыдущем разделе, обусловлена не свойствами самого кода, а выбранным алгоритмом декодирования. В этом разделе предлагается новая модификация итеративного алгоритма декодирования, поз-

воляющий «обойти» данную нижнюю границу. Новый декодер использует высокую обнаруживающую способность укороченных кодов Рида-Соломона, чтобы определить положение неисправимой комбинации ошибок. Приведём его подробное описание.

1 Проведём декодирование принятого слова итеративным декодером.

2 Если на предыдущем шаге мы получили кодовое слово, завершим декодирование, выдав это слово.

3 Иначе, назовём все столбцы, декодирование которых на последней итерации закончилось либо отказом, либо исправлением ошибок, *«плохими»*. «Хорошими» будут являться лишь те столбцы, которые были исправлены на более ранних итерациях.

4 Аналогично разделим строки на «хорошие» и «плохие».

5 Внесём стирания на пересечении «плохих» строк и столбов.

6 Повторим декодирование итеративным декодером слова, полученного на шаге 1, со стираниями, определёнными на прошлом шаге.

7 Результат этого декодирования и будет результатом работы данного алгоритма.

К сожалению, данный алгоритм обладает тем же эффективным кодовым расстоянием, что и итеративный. Действительно, существует комбинация ошибок, которая за первую итерацию итеративного декодера перейдёт в неправильное кодовое слово. Однако, предложенный алгоритм может правильно исправить большинство комбинаций ошибок минимального веса.

2.2.4. Моделирование

Для моделирования были выбраны следующие параметры:

- Произведение $[32, 30, 3]_{256}$ и $[32, 28, 5]_{256}$ кодов Рида-Соломона.
- Скорость данного кода составляет 0.82.
- Данный код имеет 840 информационных символов, длина его равна 1024, а расстояние — 15.
- Использовался 256-ричный симметричный канал.

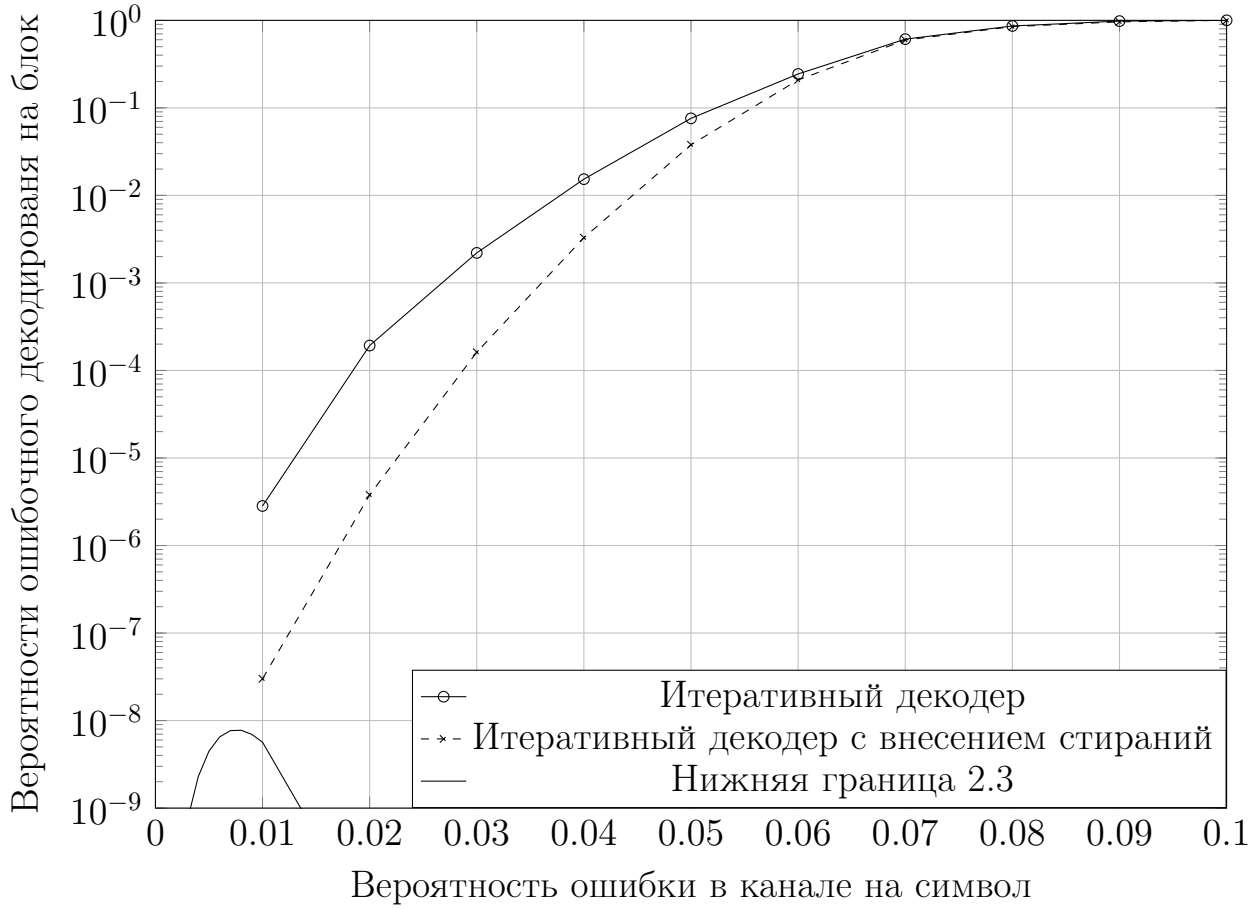

Рис. 2.1. Сравнение итеративного декодера и итеративного декодера с внесением стираний для кода-произведения

На рис. 2.1 представлены результаты моделирования. Как можно заметить, предложенный декодер имеет лучшую корректирующую способность при низких вероятностях ошибки в канале. И, что более важно, вероятность ошибочного декодирования у него спадает быстрее, чем у итеративного декодера. Из этого можно сделать вывод, что поведение каскадной сигнально-кодовой конструкции при больших отношениях сигнал-шум будет значительно улучшено.

2.3. ОЛО коды

В качестве альтернативы произвдению кодов Рида-Соломона для использования в качестве внешних кодов можно использовать коды с обобщённой локализацией ошибок (ОЛО коды). Они имеют более сложную конструкцию и намного большее число параметров. Поэтому выбор правильных параметров ОЛО кода представляет из себя отдельную задачу, приближённое решение которое приводиться в 2.3.2.

Коды с локализацией ошибок были предложены в 1963 году Вульфом и Элспасом [44]. Эти коды являются промежуточным звеном между кодами, обнаруживающими ошибки, и кодами, исправляющими ошибки, так как они позволяют определить подблок, в котором произошли ошибки, но не позволяют их исправить. В 1965 году [45] Вульф обобщил понятие ЛО-кодов на случай произвольных внутренних и внешних кодов. В 1972 году Зяблов показал [46], что ЛО-коды можно использовать и для исправления ошибок, приведя новый алгоритм декодирования. Такие коды называются обобщёнными ЛО-кодами или ОЛО-кодами. В 2000 году [47] была доказана эквивалентность классов ОЛО-кодов и обобщённых каскадных кодов. ОЛО-коды также рассматривались в работах [41, 48–51].

Конструкция ОЛО-кодов основана на конструкции обобщённых каскадных кодов. С целью облегчения восприятия в данной работе будет описан несистематический метод кодирования. В рассматриваемом ОЛО коде внутренние и внешние коды принадлежат вложенным системам кодов Рида-Соломона, имеющих длину $n_A = 8$ и $n_B = 128$ над полем $GL(2^8)$, соответственно. Здесь и далее мы обозначаем величины, соответствующие внешним кодам, индексом B, а величины, соответствующие внутренним кодам, индексом A.

При описании ОЛО-кода будут использоваться две кодовые матрицы: «внутренняя» матрица $\mathbf{C} = (c_{ij})$ и «внешняя» матрица $\mathbf{S} = (s_{ij})$. Столбцы $\mathbf{c}_j$ матри-

цы $\mathbf{C}$ связаны со столбцами $\mathbf{s}_j$ матрицы $\mathbf{S}$ следующим соотношением:

$$s_{ij} = \sum_{k=1}^{n_A} c_{kj}\alpha^{k(n_A-i+1)} = \sum_{k=0}^{n_A-1} c_{kj}H_{ki}, \tag{2.4}$$

где $i, j = \overline{0, n-1}$, $\mathbf{H} = \|H_{ki}\| = \alpha^{k(n_A-i+1)}$. Для эффективного вычисления значений символов «внешней» матрицы мы использовали быстрое преобразование Фурье. К сожалению, так как преобразование Фурье в данной формуле является укороченным, обратное преобразование нужно проводить умножением на обратную матрицу. Однако в силу малой длины $n_A = 8$ сложность данного преобразования остаётся невысокой. Таким образом,

$$c_{ij} = \frac{1}{n_A}\sum_{k=1}^{n_A} s_{kj}(\mathbf{H}^{-1})_{ki} \tag{2.5}$$

Обозначим размерность i-го внешнего кода k_i. Размерность ОЛО-кода при этом равна $K = \sum\limits_{i=1}^{n_A} k_i$. Словами внешнего кода являются строки матрицы $\mathbf{S}$. Информационными символами i-й строки являются первые k_i её элементов. Здесь $(k_1, \ldots, k_{n_A}) = (68, 98, 120, 121, 125, 125, 127, 127)$, а $K = 911$. Алгоритм выбора параметров ОЛО кода будет описан в 2.3.2.

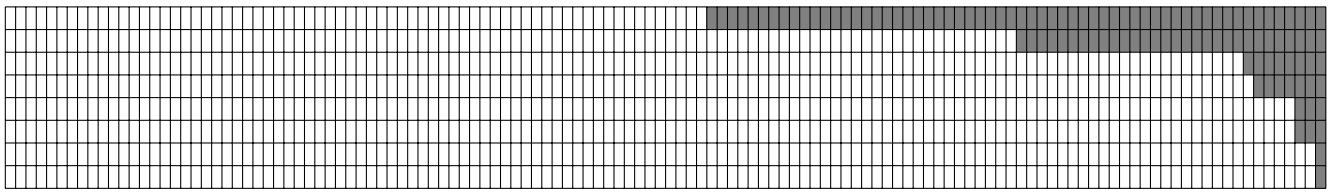

Рис. 2.2. Распределение избыточности ОЛО кода

При кодировании мы записываем информационные символы в K элементов матрицы $\mathbf{S}$, как показано на рис. 2.2. Каждый внешний код кодирует соответствующую ему часть информации и записывает полученное кодовое слово в строку матрицы. Затем по формуле (2.5) мы находим матрицу $\mathbf{C}$. Матрица $\mathbf{C}$ является кодовым словом ОЛО кода. В предложенной конструкции её символы кодируются PRF кодом.

Так как ОЛО-код является по построению обобщённым каскадным кодом, мы можем воспользоваться формулой для расстояния обобщённого каскадного

кода [41] (учтя расстояние внутреннего кода Рида-Соломона):

$$d = \min_i d_i^A d_i^B = \min_i i \cdot d_i^B \tag{2.6}$$

i-й внешний код соответствует i-ой строке матрицы $\mathbf{S}$. В предложенной конструкции $d = 14$, оно достигается при $i = 7$. Таким образов внешние коды «упорядочены» по возрастанию скорости, а соответствующие им наборы внутренних кодов — по её убыванию. Декодирование внешних кодов будет проходить «сверху вниз».

2.3.1. Классический декодер

Для декодирования внутреннего кода используется модификация алгоритма Берлекэмпа-Месси [52], далее называемая «условным» декодированием. При этом декодирование одного вектора происходит многократно с разными уровнями избыточности. На вход данного декодера поступают принятое слово $\mathbf{v}$, поправка к синдрому ΔS^A и количество проверочных символов r. Опишем этот алгоритм подробно:

1 Вычисляем r компонент синдрома S_i^A принятого слова $\mathbf{v}$.

2 $\tilde{S}_i^A = S_i^A + \Delta S_i^A$

3 Вычисляем многочлен локаторов искажений $\Lambda(x)$.

4 Вычислить рекуррентное продолжение $\tilde{S}_i^A$.

5 Определим вектор ошибки e_i и вычислим $\tilde{v}_i = v_i + e_i$.

Для описания алгоритма введём некоторые обозначения:

$\overline{\mathbf{S}}_i$ подматрица матрицы $\mathbf{S}$, составленная из i верхних её строк.

S_i i-ая строка матрицы матрицы $\mathbf{S}$.

Данные декодер является итеративным. Опишем m-ю его итерацию ($m = \overline{1,n}$).

1 В начале итерации известны: принятая «внутренняя» матрица $\mathbf{C}$, переданные («правильные») $\overline{\mathbf{S}}_{m-1}$ и строка S_m, возможно содержащая ошибки.

2 Декодируем m-ую строку матрицы m-ым внешним кодом.

3 Для $j = \overline{1,n_B}$ декодируем j-й столбцы «условным» декодером с избыточностью $r = m$ символов и поправкой к синдрому $\Delta S_i^A = s_{ij}, i = \overline{1,m}$. Результат декодирования обозначим $\tilde{v}_{ij}$.

4 Вычислим $s_{m+1,j}$ по формуле (2.4) для $j = \overline{1,n_B}$, положив $c_{ij} = \tilde{v}_{ij}$.

Если хотя бы один внешний код не смог исправить все ошибки, декодирование закончится с ошибкой.

2.3.2. Выбор параметров ОЛО кода

Известны два основных критерия выбора параметров ОЛО кода: максимизация кодового расстояния и минимизация вероятности ошибки для выбранного канала. В первом случае мы выбираем избыточности внешних кодов так, чтобы $d_i^B i \geq \hat{d}$ для заданного $\hat{d}$. При этом расстояние ОЛО кода $d \geq \hat{d}$ в соответствии с (2.6). Например, для $\hat{d} = 43, n_A = 8, n_B = 128$ будет выбран код с $(k_1, \ldots, k_{n_A}) = (86, 107, 114, 118, 120, 121, 122, 123), K = 911$. Однако такой код будет обладать низкой корректирующей способностью для «реальных» вероятностей ошибки в канале (при которых вероятность неправильного декодирования превышает 10^{-8}).

В данной работе мы будем пользоваться другим критерием выбора параметров ОЛО кода: минимизация вероятности ошибки для выбранного канала. Ограничимся рассмотрением недвоичного симметричного канала и зафиксируем вероятность ошибки в нём $p = 0.01$. Тогда сформулируем задачу следующим

образом: *определить параметры* $k_1, \ldots, k_{n_A}$, *такие чтобы вероятность неправильного декодирования ОЛО кода не превышала* $\hat{P}_G$, *а* $K = \sum_{i=1}^{n_A} k_i \to \min$.

К сожалению, поиск решения данной задачи возможен лишь с помощью моделирования, так как формул для вычисления вероятности неправильного декодирования ОЛО кода неизвестно. Поэтому сформулируем более простую задачу, решение которой мы представим далее. *определить параметры* $k_1, \ldots, k_{n_A}$, *такие чтобы вероятность неправильного декодирования каждого внешнего кода при условии, что кодовые слова предыдущих внешних кодов известны, не превышала* $\hat{P}_B = 10^{-8}$, *а* $k_i \to \min$, *для всех* $i = \overline{1, n_A}$.

Обозначим вероятность ошибочного декодирования кода Рида-Соломона $P_e(q, n, d, p_e, p_t)$, а вероятность отказа от декодирования $P_t(q, n, d, p_e, p_t)$, где q — мощность поля, n — длина кода, d — его расстояние и p_e, p_t — вероятности ошибки и стирания на входе декодера. Обозначим $P_{e+t}(q, n, d, p_e, p_t) = P_e(q, n, d, p_e, p_t) + P_t(q, n, d, p_e, p_t)$ вероятность неправильного декодирования. Тогда вероятность неправильного декодирования i-го внешнего кода равна:

$$P_i^B = P_{e+t}(q, n_B, d_i^B, P_e(q, n_A, i, p, 0), P_t(q, n_A, i, p, 0)) \tag{2.7}$$

В [52, Глава 14] приведены выражения для вероятностей неправильного и ошибочного декодирования кода Рида-Соломона:

$$P_{e+t}(q, n, d, p_e, p_t) = \sum_{e=0}^{n} \sum_{t=d-2e}^{n-e} \binom{n}{e} \binom{n-e}{t} p_e^e p_t^t (1 - p_e - p_t)^{n-e-t}$$

$$P_e(q, n, d, p_e, 0) = \sum_{h=0}^{n} \left(\frac{p_e}{1-q}\right)^h (1-p_e)^{n-h} \sum_{s=0}^{\lfloor \frac{d-1}{2} \rfloor} \sum_{l=1}^{n} A_l(q, n, d) N(q, n, l, h, s)$$

$$A_l(q, n, d) = \binom{n}{l} \sum_{j=0}^{l-d} (-1)^j \binom{l}{j} (q^{l-d+1-j} - 1)$$

$$N(q, n, l, h, s) = \sum_{\substack{0 \le i,j \le n \\ i+2j+h=s+l}} \binom{n-l}{j+h-l} \binom{l}{i} \binom{l-i}{j} (q-1)^{j+h-l} (q-2)^i$$

Теперь мы можем найти наименьшие d_i^B, такие что $P_i^B \leq \hat{P}_B$. Коды Рида-Соломона с такими расстояниями будут внешними в выбранном нами ОЛО коде. Например, при $n_A = 8, n_B = 128, q = 2^8, p = 0.01, \hat{P}_B = 10^{-8}$ мы получим расстояния внешних кодов $(d_1^B, \ldots, d_8^B) = (61, 31, 9, 8, 4, 4, 2, 2)$, а $(k_1^B, \ldots, k_8^B) = (68, 98, 120, 121, 125, 125, 127, 127)$, $K = \sum k_i^B = 911$. Кодовое расстояние ОЛО кода при этом равно 14.

Теорема 10. *Вероятность неправильного декодирования ОЛО кода ограничена сверху величиной*

$$P_G \leq \sum_{i=1}^{n_A} P_i^B \tag{2.8}$$

Доказательство. ОЛО код декодируется правильно тогда и только тогда, когда все его внешнии коды декодуются правильно. Поэтому событие неправильного декодирования ОЛО кода можно представить в виде суммы несовместных событий следующего вида: первые $i-1$ внешних кодов декодированы правильно, а i-ый декодирован неправильно ($i = \overline{1, n_A}$). Обозначим вероятности этих событий $P_{G,i}$. Но $P_{G,i} \leq P_i^B$. А значит

$$P_G = \sum_{i=1}^{n_A} P_{G,i} \leq \sum_{i=1}^{n_A} P_i^B$$

□

Для ОЛО кода, параметры которого описаны в предыдущем абзаце, $P_1 = 3 \cdot 10^{-8}$, а для кода, описанного в первом абзаце этого раздела (кода, максимизирующего своё кодовое расстояние), $P_1 = 7 \cdot 10^{-4}$.

2.3.3. Моделирование

Для моделирования был выбран код

$$(k_1^B, \ldots, k_8^B) = (68, 98, 120, 121, 125, 125, 127, 127)$$

скорости 0.89, описанный в предыдущем параграфе. Его параметры выбраны так, чтобы вероятность неправильного декодирования не превышала $8 \cdot 10^{-8}$ при

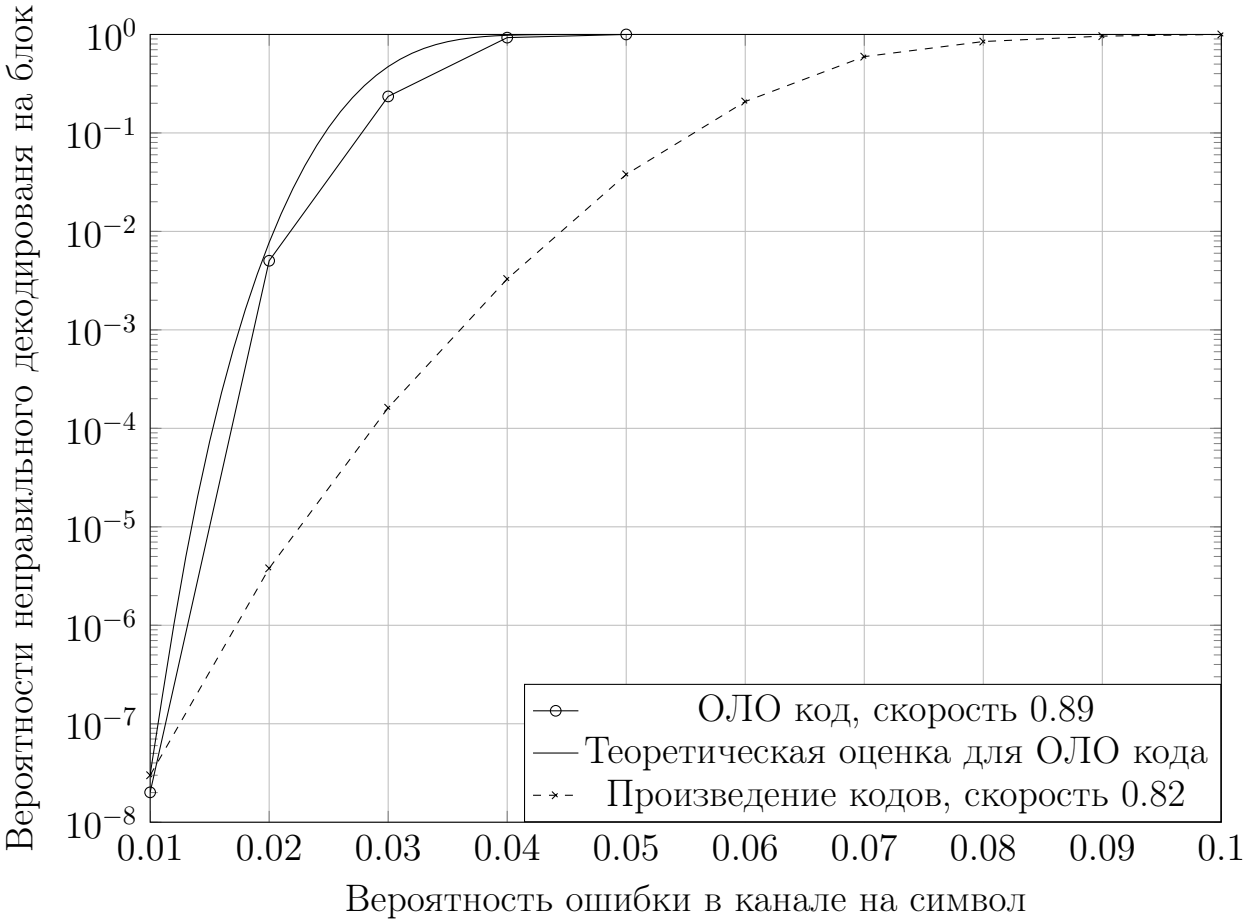

Рис. 2.3. Сравнение корректирующих способностей ОЛО кода и произведения кодов

вероятности ошибки в канале 0.01. Для сравнения взято код-произведение скорости 0.82, описанный в параграфе 2.2.4 и имеющий близкую корректирующую способность при вероятности ошибки в канале 0.01.

Результаты моделирования представлены на рис. 2.3. Несмотря на более высокую скорость и меньшее кодовое расстояние, ОЛО код имеет более крутой спад кривой вероятности неправильного декодирования. Из этого можно предположить, что при меньших вероятностях ошибки в канале ОЛО код будет иметь лучшую корректирующую способность, чем произведение кодов.

Теоретическая кривая на рис. 2.3 построена по формуле 2.8 для вышеуказанного ОЛО кода. Из рисунка видно, что данная достаточно точна, чтобы использовать её для выбора параметров ОЛО кода.

2.4. Выводы к главе

- Предложена нижняя оценка для неправильного декодирования произведения кодов.
- Предложен новый алгоритм декодирования произведения кодов, особенно эффективный для высокоскоростных кодов.
- Предложена методика выбора параметров кода с обобщённой локализацией ошибок, обладающего заданной корректирующей способностью при указанной вероятности ошибки в канале. Моделирование показало, что полученные данным методом коды имеют корректирующую способность, близкую к заданной при построении.

Глава 3

Каскадные коды с внутренним пространственно-временным кодом

3.1. Описание и кодирование

В данной работе предлагается новая двухслойная каскадная сигнально-кодовая конструкция. Системой внутренних кодов является вложенная система Golden кодов, а в качестве внешних кодов выступают произведения кодов Рида-Соломона. Выпишем параметры данной системы.

- Внутренние коды представлены кодами $\mathcal{G}_{16}$ и $2\mathcal{G}_4$, то есть Golden кодом с модуляцией КАМ-16 и его подкодом. Длина данных кодов составляет два временных отсчёта. Они используют две передающие антенны.

- Внешний код первого слоя — произведение $[32, 24, 9]_{2^8}$ укороченных кодов Рида-Соломона. Данный код имеет 576 информационных символов и скорость 0,56.

- Внешний код второго слоя — произведение $[32, 30, 3]_{2^8}$ и $[32, 28, 5]_{2^8}$ укороченных кодов Рида-Соломона. Данный код имеет 840 информационных символов и скорость 0,82.

- Таким образом внешние коды имеют длину 1024, а внутренние коды имеют 2^8 смежных классов мощности 2^8.

- Общая скорость предложенной кодовой конструкции составляет 5,5 бита (0.68 символа) за один временной интервал. Общая длина равна 2048 временных интервала.

Выбор параметров внешних кодов можно рассматривать последовательно, так как общая вероятность ошибочного приёма представлена формулой

$P\{B_1\} + P\{B_2|\overline{B_1}\}P\{\overline{B_1}\}$, где B_1 и B_2 — события ошибочного декодирования первого и второго слоя, соответственно, а $\overline{B_1}$ — событие успешного декодирования первого слоя. Моделирование показало, что параметры внешнего кода первого слоя определяет положение и крутизну спада кривой вероятности ошибочного декодирования, а параметры внешнего кода второго слоя определяют наличие и положение «полки» той же кривой, то есть резкого уменьшения скорости спада. Таким образом мы сначала подбирали параметры внешнего кода первого слоя при фиксированном «хорошем» втором коде так, чтобы спад был достаточно крутым. После этого данный код фиксировался, а у внешнего кода второго слоя избыточность понижалась до тех пор, пока не появлялась «полка». Приведённые параметры внешних кодов позволяют достигнуть вероятности ошибки на блок порядка 10^{-8} с минимальной избыточностью при использовании итеративного декодера с введением стираний.

Алгоритм кодирования уже был кратко описан в разделе 2.1, но мы приведём его ещё раз, с учётом выбранных кодов-компонент. Для описания «взаимодействия» внутренних и внешних кодов нам потребуется ввести взаимно-однозначное отображение (биекция) из $GF(2^8)$ в $[\mathcal{G}/2\mathcal{G}]$. Очевидно, данное отображение существует не одно, но выбор какого-либо из них имеет значения в предложенной конструкции. Обозначим данное отображение $\mathcal{L}$.

Информационные символы представляются в виде двух векторов $\mathbf{i}^{(1)}, \mathbf{i}^{(2)}$ длины 576 и 840 полем $GF(2^8)$. Эти вектора кодируются внешними кода первого и второго слоя, соответственно. Полученные векторы обозначим $\mathbf{v}^{(1)}, \mathbf{v}^{(2)}$.

Для кодирования внутренних кодов мы воспользуемся формулой

$$\mathbf{C}[k] = \mathbf{M}\sqrt{\frac{6}{M^2-1}}\left(\mathcal{L}(\mathbf{v}_k^{(1)}) + 2\mathcal{L}(\mathbf{v}_k^{(2)}) - \frac{M-1}{2}\right).$$

Здесь мы сначала переводим кодовые символы внешних кодов в бесконечное поле, затем модулируем их и кодируем их Golden кодом.

Предыдущий шаг можно интерпретировать и по-другому. Сначала закодируем $\mathcal{L}(\mathbf{v}_k^{(1)})$ кодом $\mathcal{G}/2\mathcal{G}$, то есть выберем смежный класс. После этого с по-

мощью кода $\mathcal{G}_4$ и информационного символа $\mathcal{L}(\mathbf{v}_k^{(2)})$ выберем элемент данного смежного класса. В таком описании проще рассуждать о кодовых расстояниях внутренних кодов.

Кодовое слово обобщённой каскадной конструкции задаётся формулой

$$\mathbf{C} = \left\| \begin{array}{c} \mathbf{C}[1] \\ \mathbf{C}[2] \\ \vdots \\ \mathbf{C}[1024] \end{array} \right\|$$

3.2. Декодер

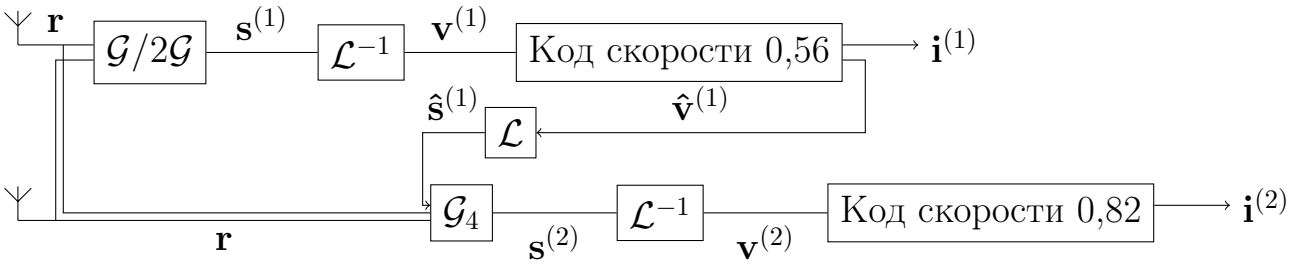

Рис. 3.1. Блок схема декодера обобщённого каскадного кода.

Блок-схема декодера представлена на рис. 3.1. Дополним её текстовым описанием:

1 Полученное с антенн слово разбивается на 1024 части, и каждая из них отправляется на декодер первого внутреннего кода.

2 Сферический декодер декодирует отдельное слово внутреннего кода (содержащее 8 символов над полем $\mathbb{R}$) и получает смежный класс, соответствующий полученному слову ($\mathbf{s}^{(1)}$).

3 Данный смежный класс отображается в символ поля $GF(2^8)$,

$$v_k^{(1)} = \mathcal{L}^{-1}(\mathbf{s}^{(1)}[k]).$$

4 Полученные символы $v_1^{(1)} \dots v_{1024}^{(1)}$ декодируются внешним кодом первого слоя. Полученный вектор обозначим $\hat{\mathbf{v}}^{(1)}$.

5 Каждый символ вектора $\hat{\mathbf{v}}^{(1)}$ отображается в вектор $\hat{\mathbf{s}}^{(1)}[k] = \mathcal{L}(\hat{v}_k^{(1)}) \in \mathbb{R}^8$.

6 Сферический декодер декодирует исходное полученное слово в смежном классе, определяемом $\hat{\mathbf{s}}$. Полученный вектор обозначим $\mathbf{s}^{(2)}$.

7 Эти вектора отображаются в поле $GF(2^8)$ и декодируются внешним кодом второго слоя.

8 Информационный вектор получается объединением информационных векторов, полученных на шагах 4 и 7.

Основной идей данного алгоритма является декодирование внутреннего кода второго слоя в известном смежном классе. В этом заключается основное отличие обобщённой каскадной конструкции от кодов с неравномерной защитой. Данная особенность позволяет внутреннему коду второго слоя иметь большее расстояние, а значит и лучшую корректирующую способность. Именно поэтому внешний код второго слоя может иметь большую скорость, чем внешний код первого слоя.

Кроме того, в разделе 1.10 описана метрика надёжности решений декодера внутреннего кода. Однако декодер внешних кодов исправляет ошибки и стирания, но не может учитывать надёжности отдельных символов. Поэтому мы предлагаем декодер предложенной конструкции по обобщённому минимальному расстоянию. Опишем его как расширение предыдущего алгоритма.

1 На шаге 2 выходом декодера будут не только символы $\mathbf{s}^{(1)}[k]$, но и их надёжности.

2 На шаге 4 мы будем проводить несколько попыток декодирования, первая из которых совпадает с описанной в предыдущем алгоритме.

3 Если данная попытка завершается отказом от декодирования, мы повторим попытку, внеся дополнительные стирания. Для этого в матричном представлении кодового слова внешнего кода (произведения кодов Рида-Соломона) в каждом столбце мы внесём стирания в два самых ненадёжных символа. Если надёжности нестёртых символов одного их столбцов неизвестны, в данный столбец стирания вноситься не будут. В силу особенностей декодера кодов Рида-Соломона, внесение нечётного числа стираний не имеет смысла.

4 Если декодирование опять завершается отказом, мы увеличим число стираний до 4 на столбец и снова повторим попытку. Мы будем продолжать вносить дополнительные стирания до тех пор, пока их число не превысит расстояние столбцового кода.

5 Таким образом декодирование внешнего кода завершится отказом только в том случае, если отказом завершатся попытки со всеми указанными комбинациями стираний.

6 Декодирование второго слоя происходит аналогично.

В данном алгоритме декодирование повторяется до первого успешного декодирования. Теоретически, декодирование при всех комбинациях стираний и создание списка результатов должно давать лучшую корректирующую способность. Однако при моделировании ни разу не наблюдалось ошибочное декодирование внешних кодов, то есть оно заканчивалось отказом, либо давало на выходе правильное кодовое слово. Это свойство произведения кодов Рида-Соломона хорошо известно и являлось одной из причин их выбора в качестве внешних кодов. В то же среднее время декодирования до первого успеха в несколько раз меньше времени декодирования в список. Поэтому для предложенной кодовой конструкции указан именно такой алгоритм декодирования.

3.3. Моделирование

Параметры предложенной конструкции уже были приведены в разделе 3.1, но мы повторим их здесь.

- Внутренние коды представлены кодами $\mathcal{G}_{16}$ и $2\mathcal{G}_4$, то есть Golden кодом с модуляцией КАМ-16 и его подкодом. Длина данных кодов составляет два временных интервала. Они используют две передающие антенны.

- Внешний код первого слоя — произведение $[32, 24, 9]_{2^8}$ укороченных кодов Рида-Соломона. Данный код имеет 576 информационных символов и скорость 0,56.

- Внешний код второго слоя — произведение $[32, 30, 3]_{2^8}$ и $[32, 28, 5]_{2^8}$ укороченных кодов Рида-Соломона. Данный код имеет 840 информационных символов и скорость 0,82.

- Таким образом внешние коды имеют длину 1024, а внутренние коды имеют 2^8 смежных классов мощности 2^8.

- Общая скорость предложенной кодовой конструкции составляет 5,5 бита (0.68 символа) за один временной интервал. Общая длина равна 2048 временных интервала.

Всё моделирование проводилось с двумя приёмными антеннами. Исследовались различные комбинации алгоритмов декодирования. Для начала приведём общий результат моделирования предложенной конструкции. На рис. 3.2 изображены кривые вероятностей ошибок на блок и на бит для предложенной конструкции. При декодировании внешних кодов использовался итеративный декодер с внесением стираний, при декодировании обобщённой каскадной конструкции — декодер по обобщённому минимальному расстоянию. Для сравнения на рисунке также изображены кривые вероятностей ошибки внутренних

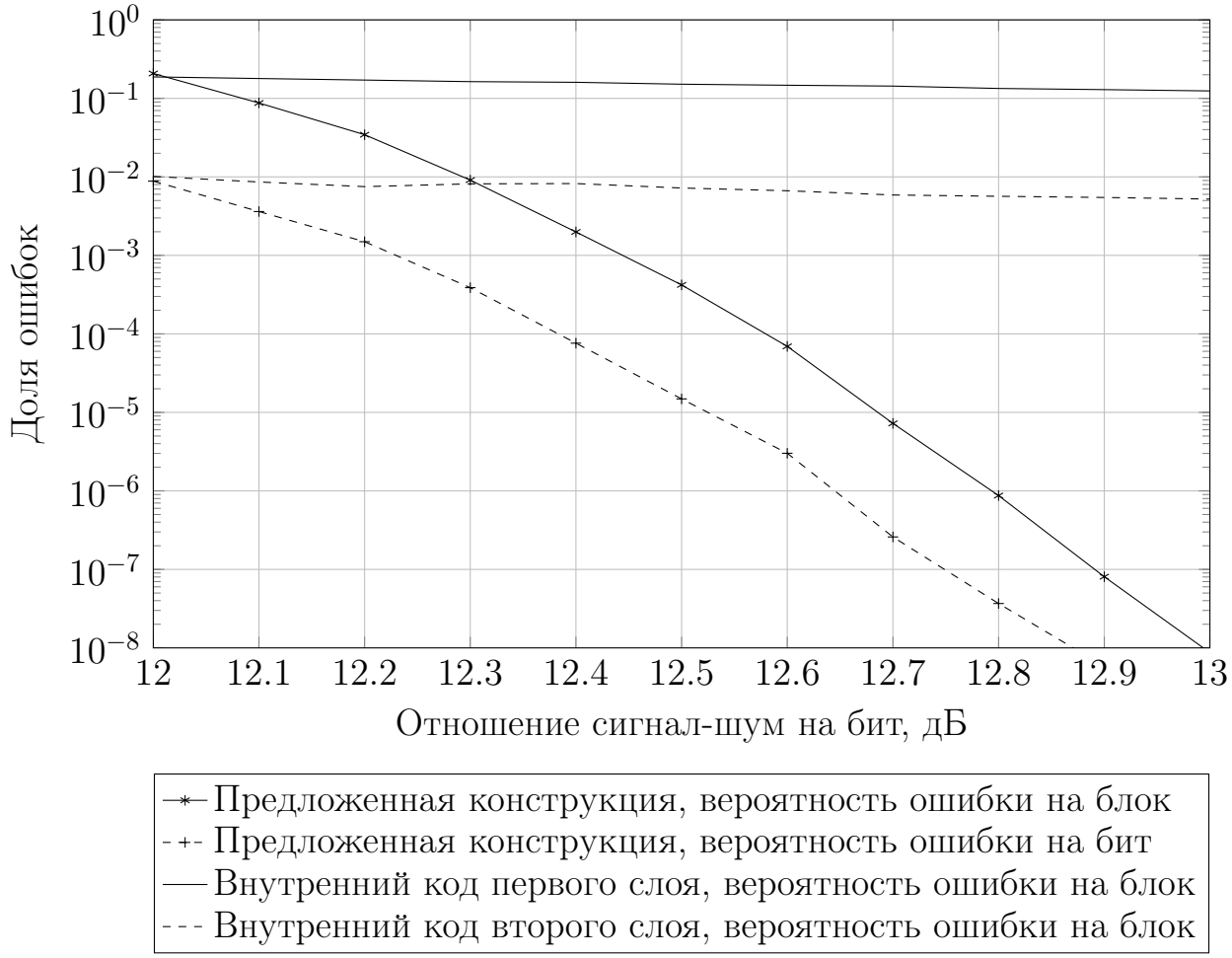

Рис. 3.2. Корректирующая способность предложенной конструкции

кодов. Из рисунка видно, что спад вероятности ошибки начинается примерно с 12–12.2 дБ, и за каждый 0.1 дБ вероятность ошибки убывает примерно в 10 раз. Заданная вероятность ошибки 10^{-8} на блок достигается на отношении сигнал шум 13 дБ на бит. Golden код без внешнего кода достигает такой вероятности ошибки на блок (при более коротком блоке) лишь при отношении сигнал-шум 35 дБ. Сравнение этих параметров с параметрами некоторых других сигнально-кодовых конструкций будет приведено на следующих графиках.

В качестве сигнально-кодовой конструкции для сравнения результатов предлагается каскадная система, с внутренним Golden кодом и внешним кодом Рида-Соломона $[1024, 708, 317]_{2^{16}}$. Данная конструкция имеет тот же внутренний код и ту же скорость. Кроме того, код Рида-Соломона имеет лучшее расстояние. Однако данная конструкция не использует разбиение Golden кода на смежные

классы, а потому, как видно из рис. 3.3, имеет более поздний спад. Большее кодовое расстояние должно привести более резкому спаду, однако при вероятностях неправильного декодирования более 10^{-8} данный эффект не заметен. Таким образом, обобщённые каскадные конструкции имеют серьёзный энергетический выигрыш по сравнению с обычными каскадными конструкциями с жёстким декодированием. Сравнение с кодами, имеющими декодеры с мягким входом, в данной работе не проводилось.

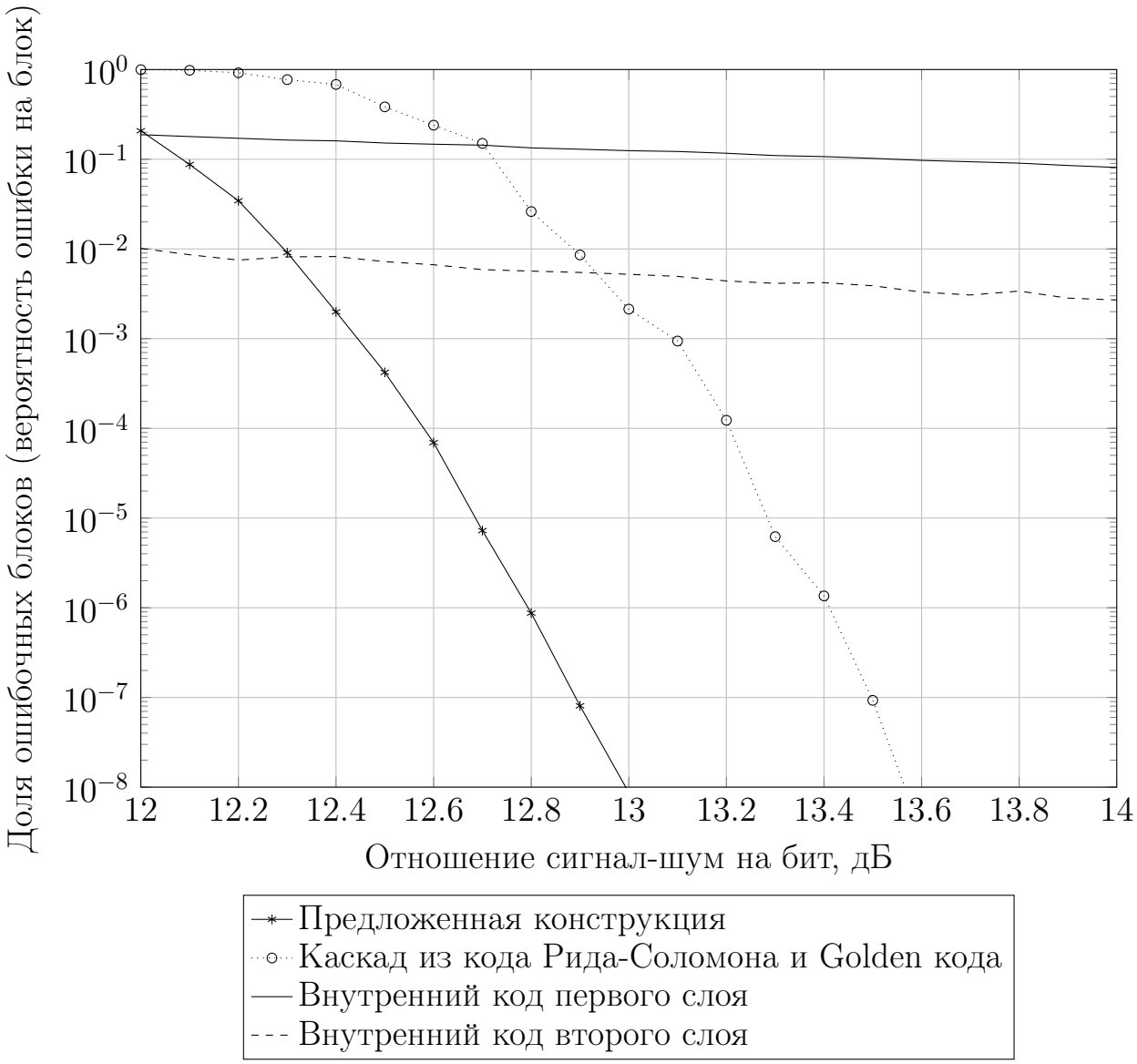

Рис. 3.3. Корректирующая способность предложенной конструкции

Для описания эффективности предложенных алгоритмов декодирования, было проведено сравнительное моделирование с ранее известными декодерами.

Были исследованы различия в корректирующей способности, во-первых, итеративного декодера и итеративного декодера с внесением стираний, и, во-вторых, классического декодера обобщённых каскадных кодов и декодера по обобщённому минимальному расстоянию (GMD-декодер). Результаты этого моделирования можно увидеть на рис. 3.4.

Сравнивая сплошную и штриховую кривые, соответствующие итеративному декодеру с внесением стираний (см. раздел 2.2.3) и классическому итеративному декодеру (см. раздел 2.2.1), можно увидеть главное преимущество предложенного алгоритма: кривая вероятности ошибки не становится пологой на всём диапазоне моделирования. В обоих случаях использовался декодер обобщённого каскадного кода по минимальному обобщённому расстоянию. Так как расстояние внешнего кода второго слоя составляет лишь $3 * 5 = 15$ при длине 1024, разумно предположить, что кривая вероятности ошибки должна стать пологой при больших отношениях сигнал-шум. Проверить этот факт моделированием достаточно сложно в силу низких вероятностей ошибки.

Штриховая и штрих-пунктирная кривые на рис. 3.4 (они также обозначены символами «o» и «+» соответственно) изображают вероятности ошибки при декодировании классическим алгоритмом для обобщённых каскадных кодов и алгоритмом декодирования по обобщённому минимальному расстоянию. Использование последнего даёт выигрыш в 0.2 дБ, однако не помогает бороться с пологостью кривой вероятности ошибки при больших отношениях сигнал-шум. В обоих моделирования для декодирования внешних кодов применялся итеративный декодер. Основной вывод, который можно сделать из этого сравнения: алгоритм декодирования обобщённого каскадного кода по обобщённому минимальному расстоянию имеет небольшой энергетический выигрыш по сравнению с классическим декодером.

Кроме того, на рис. 3.4 изображена нижняя граница (2.3), описанная в предложении 9, вычисленная для внешнего кода второго слоя. Можно заметить, что она с точностью до двух порядков описывает положение пологой части кри-

вой вероятности ошибки. Это означает, что данную оценку можно использовать для предсказания появления пологой части для кодов-произведений. Кроме того, может заметить, что на итеративный алгоритм с внесением стираний данная нижняя граница не распространяется.

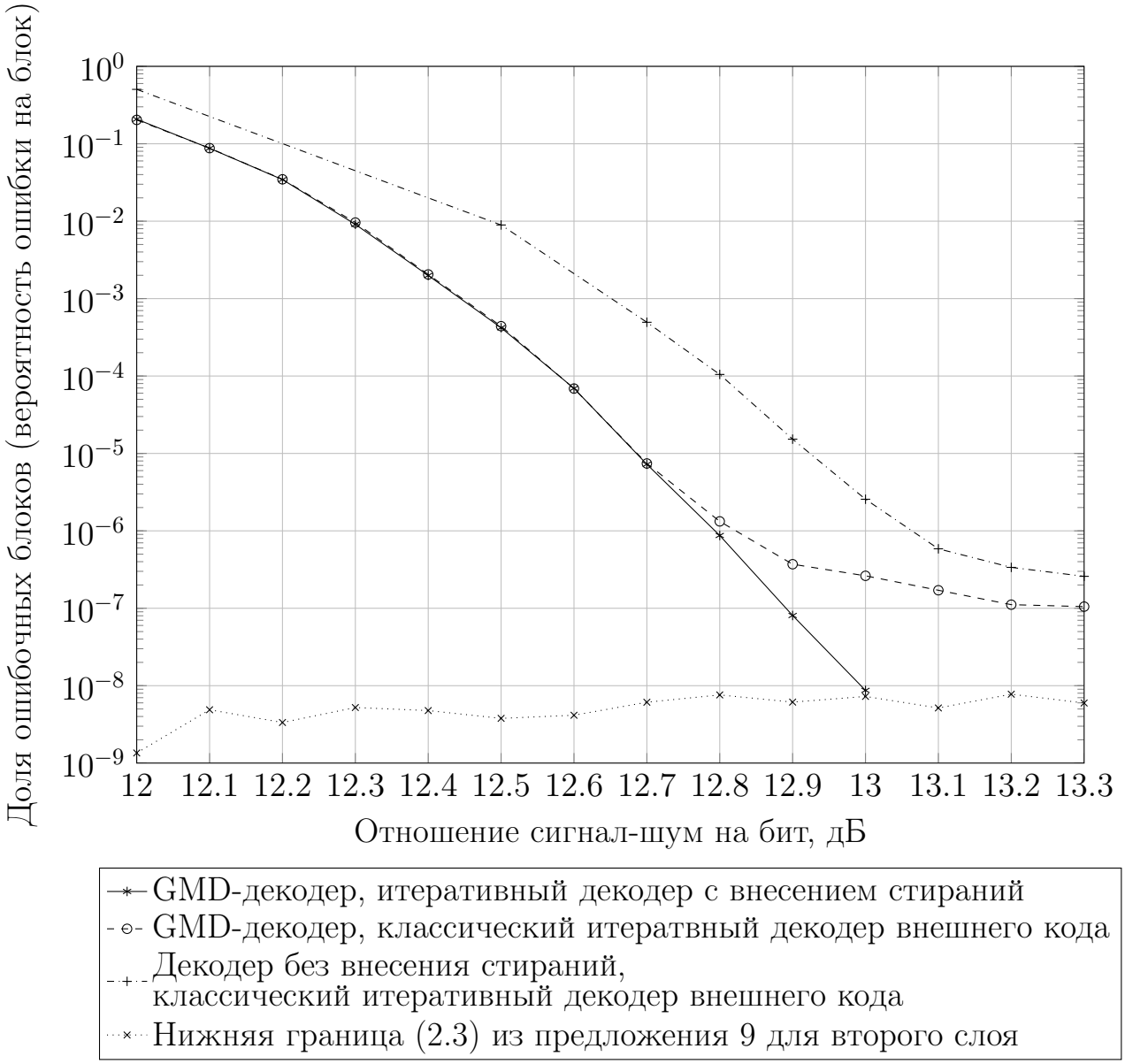

Рис. 3.4. Сравнение алгоритмов декодирования

3.4. Выводы к главе

- Описан алгоритм декодирования обобщённого каскадного кода.

- Предложен алгоритм декодирования обобщённого каскадного кода по обобщённому минимальному расстоянию (GMD-декодер).

- Методом имитационного моделирования показано, что предложенная обобщённая каскадная конструкция имеет лучшую корректирующую способность, чем простая каскадная конструкция.

Заключение

Основные результаты:

1 Исследована конструкция PF- и PRF-кодов, основанная на столбцах матрицы Адамара.

2 Построены верхняя и нижняя границы мощности PF- и PRF-кодов.

3 Разработана метрика надёжности для пространственно-временных кодов, декодируемых сферическим декодером.

4 Построена нетривиальная нижняя граница для вероятности неправильного декодирования произведения кодов.

5 Разработан новый алгоритм декодирования произведения кодов.

6 Предложена обобщённая каскадная конструкция для систем многоантенных передачи и приёма.

Список литературы

1. Крещук А.А., Давыдов А.А., Зяблов В.В. Коды для многоантенной передачи и приема на основе ортогональных последовательностей // Проблемы передачи информации. — 2011. — Т. 47, № 4. — С. 3–26.
2. Kreshchuk A.A., Zyablov V.V. Generalized concatenated system with embedded space-time codes for MIMO systems // Journal of Communications Technology and Electronics. — 2014. — Vol. 59, no. 12. — P. 1489–1500.
3. Kreshchuk Alexey, Potapov Vladimir. On some MIMO coded modulations based on Hadamard matrices // The XIII International Symposium “Problems of Redundancy in Information and Control Systems” / IEEE. — 2012. — P. 35–36.
4. Kreshchuk A., Zyablov V. Embedded space-time block codes for concatenated systems // Problems of Redundancy in Information and Control Systems (REDUNDANCY), 2014 XIV International Symposium on. — 2014. — June. — P. 62–65.
5. Kreshchuk A., Zyablov V. Generalized concatenated MIMO system with GMD decoding // 8th International Symposium on Turbo Codes and Iterative Information Processing. — 2014. — August. — P. 259–263.
6. Крещук А.А. Кодовая конструкция для систем MIMO, основанная на подмножестве строк матрицы Адамара // Информационные технологии и системы - 2010. — 2010. — 9. — С. 104–107.
7. Крещук А.А. Сравнение алгоритмов декодирования кода Рида-Соломона, исправляющих стирания и несколько ошибок // Информационные технологии и системы - 2011. — 2011. — 10. — С. 130–134.
8. Крещук А.А. Применение кодов с обобщённой локализацией ошибок в системах с многоантенной передачей и приёмом // Информационные технологии и системы - 2013. — 2013. — 9. — С. 491–494.

9. Крещук А.А., Зяблов В.В. Нижняя граница на вероятность ошибочного итеративного декодирования кодов-произведения // Информационные технологии и системы - 2014. — 2014. — Сентябрь. — С. 451–453.
10. Kreshchuk A., Zyablov V., Ryabinkin E. A new iterative decoder for product codes // Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory ACCT2014. — 2014. — September. — P. 211–214.
11. Прокис Д. Цифровая связь. — М. : Радио и связь, 2000. — 800 с. — ISBN: 525601434X.
12. Tarokh V., Seshadri N., Calderbank A.R. Space-time codes for high data rate wireless communication: performance criterion and code construction // Information Theory, IEEE Transactions on. — 1998. — Mar. — Vol. 44, no. 2. — P. 744–765.
13. Alamouti S. A simple transmit diversity technique for wireless communications // Selected Areas in Communications, IEEE Journal on. — 1998. — Oct. — Vol. 16, no. 8. — P. 1451–1458.
14. Tarokh V., Jafarkhani H., Calderbank A. R. Space-Time Block Codes from Orthogonal Designs // IEEE Transactions on Information Theory. — 1999. — Jul. — Vol. 45, no. 5. — P. 1456–1467.
15. Belfiore J.-C, Rekaya G. Quaternionic lattices for space-time coding // Information Theory Workshop, 2003. Proceedings. 2003 IEEE. — 2003. — March. — P. 267–270.
16. Belfiore J.-C., Rekaya G., Viterbo E. The Golden code: A 2 x 2 full-rate space-time code with nonvanishing determinants // IEEE Transactions on information theory. — 2005. — Vol. 51, no. 4. — P. 1432–1436.
17. Golden Space-Time Block-Coded Modulation / L. Luzzi, G.R.-B. Othman, J.-C Belfiore, E. Viterbo // Information Theory, IEEE Transactions on. — 2009. — Feb. — Vol. 55, no. 2. — P. 584–597.
18. Lusina Paul James. Algebraic Designs of Space Time Codes : Ph. D. thesis / Paul James Lusina ; University of Ulm. — 2003. — 128 p.

19. Damen M.-O., El-Gamal H., Caire G. On maximum-likelihood detection and the search for the closest lattice point // Information Theory, IEEE Transactions on. — 2003. — Oct. — Vol. 49, no. 10. — P. 2389–2402.
20. El-Gamal H., Damen M.-O. Universal space-time coding // Information Theory, IEEE Transactions on. — 2003. — May. — Vol. 49, no. 5. — P. 1097–1119.
21. Perfect Space-Time Block Codes / F. Oggier, G. Rekaya, J.-C Belfiore, E. Viterbo // Information Theory, IEEE Transactions on. — 2006. — Sept. — Vol. 52, no. 9. — P. 3885–3902.
22. Mroueh L., Rouquette-Leveil S., Belfiore J.-C. Application of Perfect Space Time Codes: PEP Bounds and Some Practical Insights // Communications, IEEE Transactions on. — 2012. — March. — Vol. 60, no. 3. — P. 747–755.
23. Viterbo E., Hong Yi. Applications of the Golden Code // Information Theory and Applications Workshop, 2007. — 2007. — Jan. — P. 393–400.
24. Closest point search in lattices / E. Agrell, T. Eriksson, A Vardy, K. Zeger // Information Theory, IEEE Transactions on. — 2002. — Aug. — Vol. 48, no. 8. — P. 2201–2214.
25. Hong Yi, Viterbo E., Belfiore J.-C. Golden Space-Time Trellis Coded Modulation // Information Theory, IEEE Transactions on. — 2007. — May. — Vol. 53, no. 5. — P. 1689–1705.
26. Damen O., Chkeif A, Belfiore J.-C. Lattice code decoder for space-time codes // Communications Letters, IEEE. — 2000. — May. — Vol. 4, no. 5. — P. 161–163.
27. Xin Yan, Wang Zhengdao, Giannakis G.B. Space-time diversity systems based on linear constellation precoding // Wireless Communications, IEEE Transactions on. — 2003. — Mar. — Vol. 2, no. 2. — P. 294–309.
28. Damen M.-O., Abed-Meraim K., Belfiore J.-C. Diagonal algebraic space-time block codes // Information Theory, IEEE Transactions on. — 2002. — Mar. — Vol. 48, no. 3. — P. 628–636.

29. ten Brink S., Kramer G., Ashikhmin A. Design of low-density parity-check codes for modulation and detection // Communications, IEEE Transactions on. — 2004. — April. — Vol. 52, no. 4. — P. 670–678.
30. Jafarkhani H. Space-time coding: theory and practice. — Cambridge Univ Pr, 2005. — 320 p.
31. From theory to practice: an overview of MIMO space-time coded wireless systems / D. Gesbert, M. Shafi, Da shan Shiu et al. // Selected Areas in Communications, IEEE Journal on. — 2003. — apr. — Vol. 21, no. 3. — P. 281–302.
32. Oggier F., Viterbo E. Algebraic Number Theory and Code Design for Rayleigh Fading Channels // Foundations and Trends in Communications and Information Theory. — 2004. — Vol. 1, no. 3. — P. 333–415.
33. Davydov A.A., Zyablov V.V., Kalimullin R.E. Subcodes of Reed–Solomon Code with Special Properties // Proc. 12th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2010), Novosibirsk, Russia. — 2010. — P. 116–122.
34. Давыдов А.А., Зяблов В.В., Калимуллин Р.Э. Специальные последовательности как подкоды кода Рида-Соломона // Проблемы передачи информации. — 2010. — Т. 46, № 4. — С. 56–82.
35. Мак-Вильямс Ф.Д., Слоэн Н.Д.А. Теория кодов, исправляющих ошибки. — М. : Связь, 1979. — 744 с.
36. Peterson W.W., Weldon E.J. Error-correcting codes. — The MIT Press, 1972. — 572 p.
37. Stanley R.P. Enumerative combinatorics. — Cambridge Univ Pr, 2001. — Vol. 2. — 642 p.
38. Forney Jr G David. Exponential error bounds for erasure, list, and decision feedback schemes // Information Theory, IEEE Transactions on. — 1968. — Vol. 14, no. 2. — P. 206–220.

39. Elias P. Error-free Coding // Information Theory, Transactions of the IRE Professional Group on. — 1954. — September. — Vol. 4, no. 4. — P. 29–37.
40. Slepian David. Some further theory of group codes // Bell System Technical Journal. — 1960. — Vol. 39, no. 5. — P. 1219–1252.
41. Блох Э.Л., Зяблов В.В. Линейные каскадные коды. — М. : Наука, 1982. — 229 с.
42. Зяблов В.В. Алгоритмы поэтапного декодирования итерированных и каскадных кодов // Передача цифровой информации по каналам с памятью: Сборник статей / Под ред. Э.Л. Блох. — М. : Наука, 1970.
43. Зяблов В.В. Оптимизация алгоритмов каскадного декодирования // Проблемы передачи информации. — 1973. — Т. 9, № 1. — С. 19–24.
44. Wolf J, Elspas B. Error-locating codes–A new concept in error control // Information Theory, IEEE Transactions on. — 1963. — Vol. 9, no. 2. — P. 113–117.
45. Wolf Jack K. On an extended class of error-locating codes // Information and Control. — 1965. — Vol. 8, no. 2. — P. 163–169.
46. Зяблов В.В. Новая трактовка кодов для локализации ошибок, их корректирующие свойства и алгоритмы декодирования // Сб. Передача дискретных сообщений по каналам с группирующимися ошибками. — 1972. — С. 8–18.
47. Maucher Johannes, Zyablov Victor V, Bossert Martin. On the equivalence of generalized concatenated codes and generalized error location codes // Information Theory, IEEE Transactions on. — 2000. — Vol. 46, no. 2. — P. 642–649.
48. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды: Алгебраическая теория и сложность реализации. — М. : Связь, 1976. — 240 с.
49. Кобозева И.Г., Зяблов В.В. Исследование сигнально-кодовых конструкций на основе трёхмерных кодов с локализацией ошибок // Информационные процессы. — 2013. — Т. 13, № 1. — С. 1–18.
50. Kobozeva I.G., Zyablov V.V. Using GEL Codes for Optical Channel // The XII Symposium “Problems of Redundancy in Information and Control Sys-

tems". — 2009. — P. 126–127.

51. Форни Д. Каскадные коды. — М. : Мир, 1970. — 208 с.
52. Блейхут Р. Теория и практика кодов, контролирующих ошибки. — М. : Мир, 1986. — 576 с.

Приложение

Подмножества поля F_{2^m} с фиксированной суммой элементов

Используются обозначения из 1.4.1 и 1.4.2. Поле F_{2^m} представляется в виде (1.13).

Лемма 9. *Рассматривается* $[2^m-1, 2^m-1-m, 3]_2$*-код Хэмминга.*

1 *Каждому кодовому слову веса* w *соответствуют два RF-подмножества поля* F_{2^m}*:* $(w,0)_{2^m}^{RF}$*-подмножество из ненулевых элементов и* $(w+1,0)_{2^m}^{RF}$*-подмножество, включающее нулевой элемент. Между совокупностями всех кодовых слов веса* w *и* $w-1$ *и всех* $(w,0)_{2^m}^{RF}$*-подмножеств существует взаимно-однозначное соответствие.*

2 *Рассмотрим смежный класс кода с синдромом* $s \neq 0$*. Каждому слову веса* w *смежного класса соответствуют два RF-подмножества поля* F_{2^m}*:* $(w,s)_{2^m}^{RF}$*-подмножество из ненулевых элементов и* $(w+1,s)_{2^m}^{RF}$*- подмножество, включающее нулевой элемент. Между совокупностями всех слов смежного класса веса* w *и* $w-1$ *и всех* $(w,s)_{2^m}^{RF}$*- подмножеств существует взаимно-однозначное соответствие.*

Доказательство. Проверочная матрица кода состоит из всех различных *ненулевых* двоичных m-разрядных *столбцов*, которые можно трактовать как *элементы поля* F_{2^m} в соответствии с (1.13). Нулевой столбец (не входящий в матрицу) соответствует нулевому элементу поля F_{2^m}.

1 Каждому кодовому слову веса w соответствует набор из w различных ненулевых столбцов, сумма которых равна нулевому столбцу. Можно добавить к такому w-набору нулевой столбец и получить набор из $w+1$ различных столбцов с нулевой суммой.

2 Рассмотрим смежный класс кода с ненулевым m-разрядным синдромом-столбцом, который можно трактовать как ненулевой элемент s поля F_{2^m}.

Каждому слову смежного класса веса w соответствует набор из w различных ненулевых столбцов, сумма которых равна s. Можно добавить к такому w-набору нулевой столбец и получить набор из $w+1$ различных столбцов с суммой s.

По построению, указанное в пунктах 1 и 2 соответствие между словами и наборами столбцов является взаимно-однозначным. □

Следствие 3. *Пусть* $3 \le w \le 2^m - 1$. *Тогда*

$$N^{(0)}_{w,2^m} = A_{w-1,2^m} + A_{w,2^m} \tag{1}$$

и для $s \neq 0$ *величина* $N^{(s)}_{w,2^m}$ *не зависит от* s. *Справедливо следующее:*

$$N^{(s)}_{w,2^m} = \overline{A}_{w-1,2^m} + \overline{A}_{w,2^m},\ s \neq 0. \tag{2}$$

Доказательство. Соотношения (1) и (2) следуют из леммы 9. Заметим также, что все смежные классы двоичного кода Хэмминга имеют одинаковый спектр весов [35, раздел 6.6]. □

Для вычисления величин $N^{(s)}_{w,2^m}$ по формулам (1), (2) полезны следующие известные соотношения для спектра весов двоичного $[2^m-1, 2^m-1-m, 3]_2$-кода Хэмминга и его смежного класса [35].

$$A_{0,2^m} = A_{2^m-1,2^m} = 1, \quad A_{1,2^m} = A_{2,2^m} = A_{2^m-3,2^m} = A_{2^m-2,2^m} = 0, \tag{3}$$

$$A_{3,2^m} = \frac{1}{3}\binom{2^m-1}{2}, \quad A_{4,2^m} = \frac{2^m-4}{3\cdot 4}\binom{2^m-1}{2} = \frac{1}{2^m-3}\binom{2^m-1}{4}, \tag{4}$$

$$wA_{w,2^m} + A_{w-1,2^m} + (2^m - w + 1)A_{w-2,2^m} = \binom{2^m-1}{w-1}. \tag{5}$$

$$\overline{A}_{w,2^m} = \frac{1}{2^m-1}\left(\binom{2^m-1}{w} - A_{w,2^m}\right). \tag{6}$$

Из (3) – (6) следует, что

$$\overline{A}_{0,2^m} = \overline{A}_{2^m-1,2^m} = 0, \quad \overline{A}_{1,2^m} = \overline{A}_{2^m-2,2^m} = 1, \quad \overline{A}_{2,2^m} = \overline{A}_{2^m-3,2^m} = 2^{m-1} - 1, \tag{7}$$

$$\overline{A}_{3,2^m} = \frac{(2^m-4)(2^{m-1}-1)}{3}, \quad \overline{A}_{4,2^m} = \frac{(2^{m-1}-1)(2^m-4)^2}{3\cdot 4}. \tag{8}$$

Лемма 10. *Справедливо следующее:*

$$\begin{aligned} N^{(0)}_{1,2^m} &= N^{(0)}_{2^m,2^m} = N^{(0)}_{2^m-1,2^m} = N^{(s)}_{1,2^m} = N^{(s)}_{2^m-1,2^m} = 1,\ s \neq 0, \\ N^{(0)}_{2,2^m} &= N^{(0)}_{2^m-2,2^m} = N^{(s)}_{2^m,2^m} = 0,\ s \neq 0, \\ N^{(s)}_{2,2^m} &= N^{(s)}_{2^m-2,2^m} = 2^{m-1},\ s \neq 0. \end{aligned} \tag{9}$$

Доказательство. Используются соотношения (3),(7) и следующие факты: сумма всех элементов поля равна нулю; сумма двух различных элементов поля F_{2^m} не равна нулю. □

Лемма 11. *Пусть $n \leq 2^m$ и для всех $s = 0, 1, \ldots, 2^m - 1$ методами леммы 9 построены все возможные $(n, s)^{RF}_{2^m}$-подмножества поля F_{2^m}. Упорядочим каждое $(n, s)^{RF}_{2^m}$-подмножество произвольным образом, превратив его в $(n, s)^{RF}_{2^m}$-вектор из $F^n_{2^m}$. Тогда для фиксированного s все полученные векторы $(n, s)^{RF}_{2^m}$-векторы образуют $(n, N^{(s)}_{n,2^m}, 2)^{PRF}_{2^m}$-код, вложенный либо в $[n, n-1, 2]_{2^m}$-РС-код (если $s = 0$), либо в смежный класс этого кода с синдромом $s \neq 0$.*

Доказательство. Используется лемма 4. Заметим также, что минимальное расстояние любого смежного класса $[n, n-1, 2]_{2^m}$-РС-кода равно 2. □

Лемма 12. *Рассматривается поле F_{2^m} и четверки $\{a, b, c, d\}$ различных элементов поля с нулевой суммой $a + b + c + d = 0$. Справедливо следующее.*

1 *Всего существует $N^{(0)}_{4,2^m}$ четверок, где*

$$N^{(0)}_{4,2^m} = \frac{1}{4}\binom{2^m}{3}.$$

2 *Каждый элемент поля входит в $\frac{1}{3}\binom{2^m-1}{2}$ четверок и не входит в $\frac{1}{2^m-3}\binom{2^m-1}{4}$ четверок.*

3 *Каждая пара a, b элементов поля полностью входит в $2^{m-1}-1$ четверок и не имеет пересечений с $\frac{1}{3}\binom{2^m-1}{2}(2^{m-2}-2) + 2^{m-1} - 1$ четверками. При*

этом существует $\frac{1}{6}(2^m-2)(2^m-4)$ *четверок, включающих элемент* a *и не содержащих элемент* b.

Доказательство. 1 Утверждение вытекает из (1) и (4).

2 Зафиксируем элемент a. Чтобы получить четверку с нулевой суммой, только два из трех элементов b, c, d можно выбрать произвольно. Число способов выбора равно $\binom{2^m-1}{2}$. При этом одна и та же четверка задается тремя выборами. Таким образом, точно $\frac{1}{3}\binom{2^m-1}{2}$ четверок с нулевой суммой включают элемент a. Остальные $N^{(0)}_{4,2^m} - \frac{1}{3}\binom{2^m-1}{2}$ четверок не содержат этот элемент.

3 Зафиксируем элементы a и b.

Чтобы получить четверку с нулевой суммой, только один из двух элементов c, d можно выбрать произвольно. Число способов выбора равно 2^m-2. При этом одна и та же четверка задается двумя выборами. Таким образом, точно $2^{m-1}-1$ четверок с нулевой суммой включают пару элементов a, b.

Из сказанного следует, что элемент a входит в $\frac{1}{3}\binom{2^m-1}{2}$ четверок, $2^{m-1}-1$ из которых содержат также элемент b. Следовательно, имеется $\frac{1}{3}\binom{2^m-1}{2} - (2^{m-1}-1)$ четверок,включающих элемент a и не содержащих элемент b.

Оставшаяся ситуация – отсутствие пересечений – выполняется для $N^{(0)}_{4,2^m} - 2\left(\frac{1}{3}\binom{2^m-1}{2} - (2^{m-1}-1)\right) - (2^{m-1}-1)$ четверок.

□

Лемма 13. *Рассматривается поле* F_{2^m} *и четверки* $\{a, b, c, d\}$ *различных элементов поля с ненулевой суммой* $a+b+c+d=s$. *Всего существует* $N^{(s)}_{4,2^m}$ *таких четверок, где*

$$N^{(s)}_{4,2^m} = \frac{2^m(2^{m-2}-1)(2^{m-1}-1)}{3},\ s \neq 0.$$

Доказательство. Утверждение вытекает из (2) и (8). □