На правах рукописи

Фролов Алексей Андреевич

Построение и исследование кодов со свойством локальности

05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации на соискание ученой степени

доктора физико-математических наук

Москва – 2021

Работа выполнена в *Автономной некоммерческой образовательной организации высшего образования «Сколковский институт науки и технологий».*

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики».

Защита состоится «25» октября 2021 г. в 11:00 на заседании диссертационного совета ФПМИ.05.13.17.006 по адресу: *141701, Московская область, г. Долгопрудный, Институтский переулок, д.9.*

С диссертацией можно ознакомиться в библиотеке Московского физико-технического института (национального исследовательского университета) на сайте института `https://mipt.ru/education/post-graduate/soiskateli.php`.

Работа представлена «20» июня 2021 г. в Аттестационную комиссию федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (национальный исследовательский университет)» для рассмотрения советом по защите диссертаций на соискание ученой степени кандидата наук, доктора наук в соответствии с п. 3.1 ст. 4 Федерального закона «О науке и государственной научно-технической политике».

Общая характеристика работы

Актуальность темы исследования.

В настоящее время активное развитие вычислительной техники и информационных технологий привело к резкому увеличению объемов производимой и обрабатываемой информации. Для доступа к этим данным необходимо создать системы их передачи и хранения, удовлетворяющие все более жестким требованиям к скорости передачи, задержке, надежности, спектральной и энергетической эффективности. Требования зависят от сценария использования. Если мы говорим о широкополосной мобильной связи, то здесь, в первую очередь, важны скорость передачи и спектральная эффективность, например, для поддержки технологий виртуальной и дополненной реальности и просмотра видео с высоким разрешением. В то же самое время для все более популярных систем интернета вещей важна поддержка межмашинного взаимодействия – передачи коротких сообщений датчиками и другими устройствами, подключенными к сети. Выделим два ключевых сценария межмашинного взаимодействия. Первым из них является сверхнадежная связь с низкой задержкой, которая важна для таких приложений, как удаленная хирургия и интеллектуальная транспортная система. Классический пример – беспилотный автомобиль, где важна именно ультранадежная передача (без нее велика вероятность аварийной ситуации). Другой сценарий, связан с массовым подключением устройств к сети. В данном сценарии требования к задержке и надежности не так важны, главной задачей является обеспечение работы очень плотной сети (200 тысяч датчиков и более на квадратный километр) и высокой энергетической эффективности, ведь датчики – это автономные устройства, питающиеся от батарейки. В системах хранения требования предъявляются в первую очередь к объему служебной информации и эффективности процедуры восстановления вышедших из строя узлов. Таким образом, сценарии могут быть различными, но общим во всех случаях будет то, что выполнение требований невозможно без использования методов помехоустойчивого кодирования.

Идея помехоустойчивого кодирования[1] была предложена К. Шенноном – основателем теории информации. Он доказал теоретическую возможность создания достаточно длинных помехоустойчивых кодов, обеспечивающих надежную связь, но не объяснил, как именно такие коды могут быть построены. С тех пор было создано уже несколько поколений кодов (например, коды Рида–Соломона, коды Рида–Маллера, турбо-коды, сверточные коды).

Важнейшим обстоятельством при выборе той или иной кодовой конструкции на практике является наличие быстрых алгоритмов кодирования и декодирования. При этом необходимо, чтобы код обладал хорошими корректирующими свойствами, что верно для большинства линейных кодов. Тем не менее задача декодирования линейного кода по максимуму правдоподобия в общем

[1] *Shannon C. E.* A mathematical theory of communication // The Bell System Technical Journal. 1948. July. Vol. 27, no. 3. P. 379–423.

случае является NP-трудной, что означает, что сложность декодирования, вероятно, растет экспоненциально с длиной кода. Поэтому нужно использовать классы кодов, имеющих минимальный рост сложности в зависимости от длины кода и возможность распараллеливания данных процедур. Одним из свойств, позволяющих строить хорошие коды с простым алгоритмом декодирования, является *свойство локальности*. В литературе можно найти несколько разных определений свойства локальности. Наиболее известным вариантом является *свойство локального декодирования*, когда любой бит кодового слова можно восстановить, просмотрев лишь небольшое число принятых бит[2],[3]. Есть также *свойство локального тестирования*, когда нужно определить с некоторой заранее заданной вероятностью ошибки, является ли слово кодовым, просмотрев небольшое число принятых бит[4]. Далее нас будет интересовать другое свойство локальности, а именно *локальность задания*. Это свойство заключается в том, что любой символ кодового слова является функцией небольшого числа других символов кодового слова. В случае линейных кодов, являющихся основным предметом исследований в данной работе, это означает наличие слов малого веса в дуальном коде. Вспомнив, что слова дуального кода являются проверочными соотношениями, мы приходим к необходимости наличия разреженных проверочных соотношений. Отметим, что мы не требуем, чтобы все проверочные соотношения были малого веса, а требуем лишь, чтобы объединение проверочных соотношений малого веса покрывало все координаты кодового слова. Важнейшими классами кодов со свойством локальности являются коды с малой плотностью проверок (МПП-коды, low-density parity-check codes, LDPC codes)[5] и коды с локальным восстановлением (ЛВ-коды, locally recoverable codes, LRC)[6],[7]. Данная диссертация посвящена теоретическому исследованию данных классов кодов, а также рассмотрению возможности применения этих кодов в современных системах передачи и хранения данных.

МПП-коды – это линейные коды с разреженной проверочной матрицей. Иными словами, проверочная матрица состоит преимущественно из нулей и содержит лишь малое число элементов, отличных от нуля. Ясно, что данные коды обладают свойством локальности, которое позволяет использовать простые алгоритмы передачи сообщений (англ. message passing) для декодирования таких

---

[2] *Yekhanin S.* Locally Decodable Codes: A Brief Survey // Coding and Cryptology / ed. by Y. M. Chee [et al.]. Berlin, Heidelberg : Springer Berlin Heidelberg, 2011. P. 273–282.

[3] *Yekhanin S.* Locally Decodable Codes // Foundations and Trends® in Theoretical Computer Science. 2012. Vol. 6, no. 3. P. 139–255.

[4] *Kaufman T.*, *Viderman M.* Locally Testable vs. Locally Decodable Codes // Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques / ed. by M. Serna [et al.]. Berlin, Heidelberg : Springer Berlin Heidelberg, 2010. P. 670–682.

[5] *Gallager R. G.* Low-Density Parity-Check Codes. MIT Press, 1963.

[6] On the Locality of Codeword Symbols / P. Goplan [et al.] // IEEE Trans. Inf. Theory. 2011. Nov. Vol. 58, no. 11. P. 6925–6934.

[7] *Papailiopoulos D. S.*, *Dimakis A. G.* Locally Repairable Codes // IEEE Trans. Inf. Theory. 2014. Oct. Vol. 60, no. 10. P. 5843–5855.

кодов. МПП-коды были предложены Р. Дж. Галлагером[8] в 1960 году. В этой работе были получены нижняя оценка минимального кодового расстояния и предложены алгоритмы декодирования, подходящие для практического применения: алгоритм распространения доверия (англ. belief propagation) и алгоритм инвертирования бита (англ. bit flipping). В 1974 г. В. В. Зяблов и М. С. Пинскер[9] доказали существование МПП-кодов, способных исправить линейную долю стираний при декодировании с помощью алгоритма, имеющего сложность $O(N \log N)$, где N – это длина кода. В 1975 г. ими был получен аналогичный результат для ошибок[10]. В 1981 г. Р. Таннер[11] предложил метод построения длинных кодов из коротких кодов компонентов. Конструкция МПП-кодов Галлагера является частным случаем конструкции Таннера и получается из нее, если использовать код с двоичной проверкой на четность в качестве компонентного кода. Таким образом, коды построенные Таннером можно назвать обобщенными МПП-кодами. После этого ввиду слабого развития вычислительной техники МПП-коды были на долгое время забыты. Активное исследование МПП-кодов началось в середине 90-х годов в связи с появлением работ М. Сипсера, Д. Спилмана[12] и Д. Маккея[13]. Исследованию двоичных МПП-кодов посвящено множество работ, среди которых следует особо отметить работы таких русских и зарубежных ученых, как Р. Дж. Галлагер, М. С. Пинскер, В. В. Зяблов, К. Ш. Зигангиров, А. М. Барг, Р. Таннер, Д. Спилман, Д. Маккей, Т. Ричардсон, Р. Урбанке, Д. Бурштейн, С. Л. Лицын, Ж. Земор, М. Фоссорье, Д. Деклерк, С.И. Ковалев. Как результат, в настоящее время эти коды приняты для использования в канале данных систем мобильной связи пятого поколения (5G). Несмотря на это, двоичные МПП-коды не подходят для передачи коротких сообщений, а также режима высоких кодовых скоростей, так как имеют при малых вероятностях ошибки, так называемую, “полку” (англ. error floor).

МПП-коды над полем $\mathrm{GF}(q)$ впервые рассмотрены в работе М. Дэви и Д. Маккея[14], где был предложен алгоритм декодирования, являющийся обобщением алгоритма распространения доверия для двоичного случая, и проведено исследование методом имитационного моделирования. Было показано, что недвоичные МПП-коды значительно превосходят двоичные. Кроме того, недвоичные МПП-коды значительно лучше для каналов с пачками ошибок и каналов

---

[8] *Gallager R. G.* Low-Density Parity-Check Codes. MIT Press, 1963.

[9] *Зяблов В. В.*, *Пинскер М. С.* Сложность декодирования низкоплотностных кодов при передаче по каналу со стираниями // Пробл. передачи информ. 1974. т. 10, № 1. с. 5—28.

[10] *Зяблов В. В.*, *Пинскер М. С.* Оценка сложности исправления ошибок низкоплотностными кодами Галлагера // Пробл. передачи информ. 1975. т. 11, № 1. с. 23—36.

[11] *Tanner R.* A recursive approach to low complexity codes // IEEE Transactions on Information Theory. 1981. Sept. Vol. 27, no. 5. P. 533–547.

[12] *Sipser M.*, *Spielman D. A.* Expander codes // IEEE Transactions on Information Theory. 1996. Nov. Vol. 42, no. 6. P. 1710–1722.

[13] *MacKay D. J. C.* Good error correcting codes based on very sparse matrices // IEEE Trans. Inform. Theory. 1999. Vol. 45, no. 2. P. 399–431.

[14] *Davey M. C.*, *MacKay D.* Low-density parity check codes over GF(q) // IEEE Communications Letters. 1998. Vol. 2, no. 6. P. 165–167.

с модуляциями высокой кратности[15]. Число работ, посвященных исследованию недвоичных МПП-кодов, сравнительно невелико. В существующих работах по этой теме приводятся упрощенные варианты алгоритма декодирования и результаты исследований этих модифицированных алгоритмов методом имитационного моделирования. Однако результатов исследований методом имитационного моделирования недостаточно.

В диссертации мы фокусируемся на всестороннем исследовании МПП-кодов. Во-первых, мы проводим теоретическое исследование потенциальных и реализуемых свойств МПП-кодов над полем $\mathrm{GF}(q)$. Далее мы рассматриваем возможность применения таких кодов в современных системах связи. Нас в большей степени интересуют системы интернета вещей и сценарий межмашинного взаимодействия. Мы разрабатываем метод декодирования МПП-кодов на основе глубоких нейронных сетей, способный в значительной степени улучшить корректирующие свойства МПП-кодов при малой длине сообщения. Наконец, мы рассматриваем сценарий массового межмашинного взаимодействия и предлагаем схемы кодирования на основе МПП-кодов, очень близкие к фундаментальным пределам энергетической эффективности.

ЛВ-коды также обладают свойством локальности, которое позволяет оптимизировать процедуру восстановления одного вышедшего из строя диска/сервера. Такие коды крайне важны для систем распределенного хранения данных. Данный класс кодов хорошо исследован в литературе. Предложены оптимальные конструкции ЛВ-кодов как на основе кодов в ранговой метрике[16] (для алфавита, мощность которого растет экспоненциально с длиной кода), так и на основе кодов Рида–Соломона[17] (для алфавита, размер которого растет линейно с длиной кода).

Естественным обобщением ЛВ-кодов являются ЛВ-коды с несколькими восстанавливающими множествами. Данное свойство позволяет обрабатывать несколько одновременных запросов для восстановления одних и тех же данных параллельно, что критически важно для данных, к которым постоянно происходят обращения (так называемых «горячих данных»). Данный класс кодов по своей структуре очень близок к МПП-кодам. В диссертации мы проводим теоретическое исследование таких кодов и устанавливаем границы для их параметров.

Цели и задачи диссертационной работы: разработка математического аппарата, который позволит провести теоретическое исследование классов кодов со свойством локальности, предложить методы построения таких кодов, а также рассмотреть возможности применения этих кодов в современных системах передачи и хранения данных.

---

[15] *Hongxin Song, Cruz J. R.* Reduced-complexity decoding of Q-ary LDPC codes for magnetic recording // IEEE Transactions on Magnetics. 2003. Mar. Vol. 39, no. 2. P. 1081–1087.

[16] Optimal Locally Repairable Codes via Rank Metric Codes / N. Silberstein [et al.] // Proceedings IEEE International Symposium on Information Theory (ISIT). 07/2013. P. 1819–1823.

[17] *Tamo I., Barg A.* A Family of Optimal Locally Recoverable Codes // IEEE Trans. Inf. Theory. 2014. Aug. Vol. 60, no. 8. P. 4661–4676.

Для достижения поставленных целей необходимо решить следующие задачи:

- разработать методы оценки минимального кодового расстояния для МПП-кодов над полем $\mathrm{GF}(q)$.
- разработать методы декодирования и исследования реализуемых корректирующих свойства МПП-кодов над полем $\mathrm{GF}(q)$. Рассмотреть возможность использования методов машинного обучения при декодировании МПП-кодов.
- на основе предложенных подходов разработать методы построения МПП-кодов над полем $\mathrm{GF}(q)$, имеющих хорошие корректирующие свойства.
- оценить возможность применения МПП-кодов в системах множественного доступа, предложить схемы кодирования на основе МПП-кодов, способные разрешать коллизии малой кратности.
- применить разработанный математический аппарат для ЛВ-кодов с несколькими восстанавливающими множествами, найти границы для параметров таких кодов.

Научная новизна. В настоящей работе впервые:

- Теоретически исследованы потенциальные и реализуемые корректирующие свойства МПП-кодов над полем $\mathrm{GF}(q)$, а именно найдены нижняя и верхняя границы на минимальное кодовое расстояние и нижняя оценка радиуса декодирования для алгоритма с малой сложностью реализации.
- Предложен мажоритарный алгоритм декодирования МПП-кодов над полем $\mathrm{GF}(q)$ и его многопороговая модификация.
- Предложен алгоритм декодирования МПП-кодов на основе глубоких нейронных сетей со специальной архитектурой, позволяющей производить обучение только на нулевом кодовом слове.
- Получены асимптотические верхние и нижние оценки относительной (на один подканал) пропускной способности для бесшумного канала с информацией об интенсивности при координированной и некоординированной передаче.
- Установлены неасимптотические верхние и нижние границы на вероятность ошибки для многопользовательского канала Рэлея.
- Предложены схемы кодирования на основе МПП-кодов, способные разрешать коллизии малой кратности и позволяющие обеспечить энергетическую эффективность, очень близкую к фундаментальным пределам в сценарии массового случайного доступа.

- Установлены границы для параметров ЛВ-кодов с несколькими восстанавливающими множествами.

- Предложено обобщение ЛВ-кодов, в котором восстанавливающие множества могут пересекаться по небольшому числу позиций, позволяющее строить коды, имеющие значительно большую скорость и удовлетворяющие требованию сбалансированной нагрузки на диски.

Теоретическая и практическая значимость. Предложенные методы оценки потенциальных и реализуемых корректирующих свойств для кодов со свойством локальности могут использоваться для широкого класса кодов, обладающих этим свойством. Уже в самой диссертации мы продемонстрировали это на примере ЛВ-кодов. Данные методы могут быть использованы для выбора параметров кодов, использующихся на практике, а также построения новых классов кодов.

Практическая значимость полученных результатов определяется тем, что в диссертации рассмотрены перспективные направления развития технологий беспроводной связи, обсуждаемые в настоящее время в комитетах по стандартизации (3GPP, IEEE 802) в рамках работ по созданию сетей пятого поколения. В частности, это задачи межмашинного взаимодействия и использование методов машинного обучения при декодировании. Разработанные технологии легко переносимы на коммерческие приложения и стартапы. Результаты могут быть применены для разработки национального стандарта LP-WAN, чтобы конкурировать с существующими решениями LoRa, SigFox и т.д. Новые конструкции ЛВ-кодов могут быть использованы в распределенных и облачных системах хранения данных.

Положения, выносимые на защиту: На защиту выносятся следующие положения:

1. Верхние и нижняя границы минимального кодового расстояния для МПП-кодов над полем $\mathrm{GF}(q)$.

2. Асимптотическая оценка на радиус декодирования МПП-кодов над полем $\mathrm{GF}(q)$, реализуемый с помощью мажоритарного алгоритма декодирования, имеющего сложность $O(N \log N)$.

3. Алгоритм декодирования МПП-кодов на основе глубоких нейронных сетей со специальной архитектурой, позволяющей производить обучение только на нулевом кодовом слове.

4. Схемы кодирования на основе МПП-кодов, способные разрешать коллизии малой кратности и обеспечивающие очень близкую к фундаментальным пределам энергетическую эффективность в сценарии массового случайного доступа.

5. Границы для параметров ЛВ-кодов с несколькими восстанавливающими множествами.

6. Обобщение ЛВ-кодов, в котором восстанавливающие множества могут пересекаться по небольшому числу позиций, позволяющее строить коды, имеющие значительно большую скорость и удовлетворяющие требованию сбалансированной нагрузки на диски.

Степень достоверности и апробация результатов. Основные результаты диссертации докладывались на следующих конференциях:

- IEEE International Symposium on Information Theory (2011, 2013, 2015, 2017, 2018, 2019, 2020);
- IEEE Information Theory Workshop (2015, 2017);
- International Symposium on Information Theory and its Applications (2018);
- IEEE Wireless Communications and Networking Conference (2019);
- IEEE Vehicular Technology Conference (2019);
- International Symposium "Problems of Redundancy in Information and Control Systems" (2009, 2014, 2016, 2019);
- International Workshop on Algebraic and Combinatorial Coding Theory (2010, 2014, 2018);
- Asilomar Conference on Signals, Systems, and Computers (2019).

Кроме того, они были представлены на следующих семинарах:

- по теории кодирования Института проблем передачи информации РАН, Москва, руководитель – Л.А. Бассалыго;
- лаборатории информационных систем и систем принятия решений Массачусетского технологического института (MIT), г. Кембридж, Массачусетс, руководитель – Ю.Г. Полянский;
- по управлению и обработке сигналов университета Мэриленда, г. Колледж Парк, Мэриленд, руководитель – А.М. Барг;
- по теории кодирования Израильского технологического института (Технион), г. Хайфа, Израиль, руководитель – Р. Рот;
- по криптографии университета г. Рен, Франция, руководитель – П. Лодрё;
- по алгебраической теории кодирования университета г. Ульм, Германия, руководитель – М. Боссерт;

- по теории кодирования Технического университета г. Мюнхен (TUM), Германия, руководитель – Г. Крамер;

- по телекоммуникациям немецкого аэрокосмического цента (DLR), Германия, руководитель – Дж. Лива;

- по алгебраической теории кодирования для сетей и систем хранения данных исследовательского центра Дагштуль, Германия, руководитель – Р. Зедел;

Кроме того были сделаны доклады на профессорских днях московского исследовательского центра компании «Хуавэй» в 2015-2020 гг.

Публикации. Материалы диссертации опубликованы в 33 печатных работах, из них 14 статей [1–14] в рецензируемых журналах и 19 статей [15–33] в сборниках трудов конференций.

Личный вклад автора. Содержание диссертации и основные положения, выносимые на защиту, отражают персональный вклад автора в опубликованные работы. Подготовка к публикации полученных результатов проводилась совместно с соавторами, причем вклад диссертанта был определяющим. Все представленные в диссертации результаты получены лично автором.

Структура и объем диссертации. Диссертация состоит из введения, обзора литературы, пяти глав, заключения и библиографии. Общий объем диссертации 186 страниц, включая 35 рисунков и 5 таблиц. Библиография включает 153 наименования на 17 страницах.

Содержание работы

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

В первой главе исследуются потенциальные корректирующие свойства МПП-кодов над полем $\mathrm{GF}(q)$. Построены нижняя и верхние оценки кодового расстояния для таких кодов. Показано, как меняются корректирующие свойства МПП-кодов при изменении их параметров, что важно для практического применения этих кодов.

МПП-код $\mathcal{C}$ длины N над полем $\mathrm{GF}(q)$ – это линейный код с разреженной проверочной матрицей $\mathbf{H} = [h_{j,i}]$, $1 \le j \le M$, $1 \le i \le N$ размера $M \times N$ над полем $\mathrm{GF}(q)$. Таким образом, проверочная матрица состоит преимущественно из нулей и содержит малое число элементов, отличных от нуля. Далее мы будем рассматривать как регулярные, так и нерегулярные МПП-коды. Начнем с более общего случая – нерегулярных МПП-кодов. Пусть строки матрицы $\mathbf{H}$ имеют веса $n_0^{(j)}$, $j = 1, \ldots, M$, а столбцы – веса $\ell^{(i)}$, $i = 1, \ldots, N$. Под *весом* вектора мы

понимаем вес Хэмминга или число ненулевых элементов в векторе. Обозначим вес вектора $\mathbf{x}$ через $wt\,(\mathbf{x})$. Известно[18], что для скорости кода $\mathcal{C}$ выполнено соотношение

$$R(\mathcal{C}) \geq 1 - \frac{\sum_{i=1}^{N} \ell^{(i)}/N}{\sum_{j=1}^{M} n_0^{(j)}/M},$$

где в числителе и знаменателе дроби стоят средние веса столбцов и строк матрицы соответственно. Равенство достигается в случае полного ранга матрицы $\mathbf{H}$. В случае регулярного МПП-кода все строки матрицы $\mathbf{H}$ имеют вес n_0, а все столбцы – ℓ.

Код $\mathcal{C}$ можно представить в виде двудольного графа[19], называемого *графом Таннера*, см. рис. 1. Граф состоит из N символьных вершин $v_1, v_2, \ldots, v_N$ и M проверочных вершин $c_1, c_2, \ldots, c_M$. Символьная вершина v_i и проверочная вершина c_j соединены ребром тогда и только тогда, когда $h_{j,i} \neq 0$, данное ребро имеет метку $h_{j,i} \in \mathrm{GF}(q)$. Введем обозначения $\Gamma(i) = \{j : h_{j,i} \neq 0, 1 \leq j \leq M\}$ и $\Phi(j) = \{i : h_{j,i} \neq 0, 1 \leq i \leq N\}$. Чтобы проверить, является ли слово $\mathbf{r} = (r_1, r_2, \ldots, r_N) \in \mathrm{GF}(q)^N$ кодовым, поставим символы слова в соответствие символьным вершинам ($v_i \leftarrow r_i, i = 1, \ldots, N$). Каждая проверочная вершина c_j, $1 \leq j \leq M$, накладывает следующее линейное ограничение

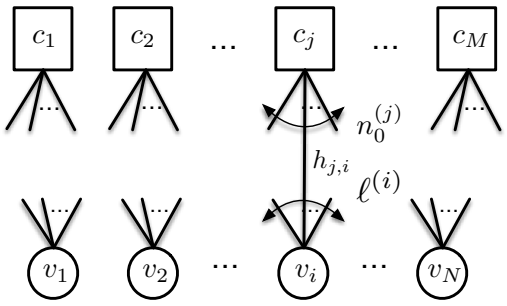

Рис. 1: Граф Таннера

$$c_j : \sum_{t \in \Phi(j)} h_{j,t} r_t = 0,$$

и можно сказать, что проверочные вершины соответствуют кодам с проверкой на четность длины $n_0^{(i)}$, $i = 1, \ldots, M$, над полем $\mathrm{GF}(q)$. Далее мы будем называть эти коды *кодами-компонентами*. Слово $\mathbf{r} \in \mathcal{C}$ тогда и только тогда, когда все наложенные ограничения выполнены (символы, пришедшие в коды-компоненты по ребрам графа Таннера сформировали кодовые слова этих кодов).

Коды с проверкой на четность можно заменить на любые линейные коды, имеющие те же длины. Так мы приходим к *обобщенным МПП-кодам*. Далее (для простоты изложения) мы рассматриваем только случай, когда все коды-компоненты одинаковы (обозначим этот код через $\mathcal{C}_0$). Код $\mathcal{C}_0$ является линейным $[n_0, R_0 n_0, d_0]$ кодом над полем $\mathrm{GF}(q)$. Обозначим проверочную матрицу компонентного кода через $\mathbf{H}_0$. Эта матрица имеет размер $m_0 \times n_0$, где

[18] *Gallager R. G.* Low-Density Parity-Check Codes. MIT Press, 1963.

[19] *Tanner R.* A recursive approach to low complexity codes // IEEE Transactions on Information Theory. 1981. Sept. Vol. 27, no. 5. P. 533–547.

$m_0 = (1 - R_0)n_0$. Пусть $g_0(s)$ – это *нумератор весов* кода $\mathcal{C}_0$, т.е.

$$g_0(s) = 1 + \sum_{W=d_0}^{n_0} A(W)s^W,$$

где $A(W)$ – это число слов веса W в коде $\mathcal{C}_0$. Обозначим через $g_1(s)$ нумератор весов всех остальных слов, т.е.

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

Обозначим через $\mathbf{S}$ синдром принятого вектора $\mathbf{r}$, т.е. $\mathbf{S} = \mathbf{r}\mathbf{H}^T$. Данный синдром состоит из синдромов компонентных кодов и может быть представлен в виде

$$\mathbf{S} = \left(\begin{array}{cccc} \mathbf{s}_1 & \mathbf{s}_2 & \dots & \mathbf{s}_M \end{array} \right),$$

где $\mathbf{s}_i$, $i = 1, \dots, M$ – синдром i-го компонентного кода. Полученное представления называют *обобщенным синдромом.*

Для доказательств мы будем использовать вероятностный метод[20], также известный как метод случайного кодирования[21]. Введем *ансамбль* $\mathcal{E}(b, n_0, \ell)$ МПП-кодов над полем $\mathrm{GF}(q)$ по аналогии с ансамблем двоичных МПП-кодов Галлагера. Рассмотрим блочную диагональную матрицу

$$\mathbf{H}_b = \left(\begin{array}{cccc} \mathbf{H}_0 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_0 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{H}_0 \end{array} \right)_{bm \times bn_0},$$

на главной диагонали которой находятся b проверочных матриц $\mathbf{H}_0$ кода $\mathcal{C}_0$.

Пусть $\varphi(\mathbf{A}) = \mathbf{A} \cdot \mathbf{\Pi} \cdot \mathrm{diag}(\gamma_1, \dots, \gamma_N)$, где $\mathbf{\Pi}$ – это матрица перестановки, а $\gamma_j \in \mathrm{GF}(q) \backslash \{0\}$, $j = 1, \dots, N$. Тогда матрица

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

размера $\ell bm \times bn_0$, составленная из ℓ таких матриц, как слоев, является разреженной проверочной матрицей МПП-кода из ансамбля $\mathcal{E}(b, n_0, \ell)$.

Определение 1. *Элементы ансамбля $\mathcal{E}(b, n_0, \ell)$ получаются путем независимого выбора преобразований $\varphi_i, i = 1, 2, \dots, \ell$.*

---

[20] *Эрдёш П., Спенсер Д.* Вероятностные методы в комбинаторике. М.: Мир, 1976.

[21] *Shannon C. E.* A mathematical theory of communication // The Bell System Technical Journal. 1948. July. Vol. 27, no. 3. P. 379–423.

Отметим, что в отличие от определения ансамбля для двоичных кодов[22] здесь добавляется умножение на константы, не равные нулю.

Нам также понадобится *ансамбль квазициклических МПП-кодов*[23]. Квазициклические МПП-коды (КЦ МПП-коды) являются важным классом МПП-кодов. Такие коды просты в описании, для них есть эффективные алгоритмы кодирования и декодирования, основанные на алгоритме распространения доверия. Все это делает эти коды популярными в практических приложениях. Рассмотрим следующую двоичную матрицу размера $m \times n$

$$\mathbf{H}_{\text{base}} = [h_{i,j}] \in \{0,1\}^{m \times n}.$$

Эту матрицу мы будем называть базовой матрицей.

Построим проверочную матрицу $\mathbf{H}$ КЦ МПП-кода $\mathcal{C}$. Для этого расширим матрицу $\mathbf{H}_{\text{base}}$ циклическими матрицами (циркулянтами), умноженными на ненулевые элементы поля $\mathrm{GF}(q)$, т.е.

$$\mathbf{H} = \begin{bmatrix} \alpha_{1,1}\mathbf{P}_{1,1} & \alpha_{1,2}\mathbf{P}_{1,2} & \cdots & \alpha_{1,n}\mathbf{P}_{1,n} \\ \alpha_{2,1}\mathbf{P}_{2,1} & \alpha_{2,2}\mathbf{P}_{2,2} & \cdots & \alpha_{2,n}\mathbf{P}_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{m,1}\mathbf{P}_{m,1} & \alpha_{m,2}\mathbf{P}_{m,2} & \cdots & \alpha_{m,n}\mathbf{P}_{m,n} \end{bmatrix} \in \mathrm{GF}(q)^{ms \times ns},$$

где $\mathbf{P}_{i,j}$ – двоичный циркулянт размера $s \times s$ и веса[24] $h_{i,j}$, $i = 1, \ldots, m$; $j = 1, \ldots, n$. $\alpha_{i,j} \in \mathrm{GF}(q) \backslash \{0\}$, $i = 1, \ldots, m$; $j = 1, \ldots, n$.

Пусть $h_q(x) = -x \log_q x - (1-x)\log_q(1-x) + x \log_q(q-1)$, где $0 \leq x \leq 1$. В случае $q = 2$ это функция двоичной энтропии, и мы будем использовать обозначение $h(x)$.

В *разделе 1.4* получена нижняя оценка минимального кодового расстояния для ансамбля $\mathcal{E}(b, n_0, \ell)$ МПП-кодов над полем $GF(q)$. Основной результат этого раздела сформулирован в виде теоремы 1.1. Определим функцию

$$F_1(\omega, n_0) = h_q(\omega) + \max_{s>0} \left(\omega \log_q(s) - \frac{1}{n_0} \log_q(g_0(s)) \right).$$

Теорема 1.1. ([3]) *Для любых $d_0 \geqslant 2$ и $\frac{d_0}{d_0 - 1} < \ell < n_0$, существует число $\delta^* = \delta^*(n_0, \ell, g_0) > 0$, такое что*

- *в ансамбле $\mathcal{E}(b, n_0, \ell)$ существуют коды, для которых выполнено следующее неравенство*

$$d(\mathcal{C}) > \delta N,$$

для любого $0 < \delta < \delta^*$.

---

[22] *Gallager R. G.* Low-Density Parity-Check Codes. MIT Press, 1963.

[23] *Fossorier M. P. C.* Quasi-cyclic low-density parity-check codes from circulant permutation matrices // IEEE Transactions on Information Theory. 2004. Aug. Vol. 50, no. 8. P. 1788–1793.

[24] весом циркулянта называется вес его первой строки.

- *число таких кодов* $(G(b))$ *удовлетворяет соотношению*

$$\lim_{b\to\infty}\frac{G(b)}{|\mathcal{E}(b,n_0,\ell)|}=1.$$

Число δ^* *– это наименьший положительный корень* (*относительно переменной* ω) *уравнения*

$$\ell F_1(\omega,n_0)-h_q(\omega)=0.$$

В *разделе 1.5* получена верхняя оценка минимального кодового расстояния для МПП-кодов над полем $GF(q)$ с помощью метода укорочения. Основной результат этого раздела сформулирован в виде теоремы 1.2.

Теорема 1.2. ([3]) *Пусть* $\mathcal{C}$ *– это обобщенный МПП-код длины* N *скорости* R *с минимальным кодовым расстоянием* δN *и компонентным* $[n_0,R_0n_0,d_0]$ *кодом* $\mathcal{C}_0$ *над полем* $GF(q)$. *Тогда для достаточно больших* N *выполнено неравенство*

$$R(\mathcal{C})\le\min_{\frac{q}{q-1}\delta\leqslant\tau\leqslant1}\left\{R_0(1-\tau)+R^*\left(\frac{\delta}{\tau}\right)\tau\right\}+o(1),$$

где $R^*(\delta)$ *– любая верхняя граница скорости кода.*

Рассмотрим ансамбль $\mathcal{E}(b,n_0,\ell)$. Воспользовавшись соотношением[25] $R\geqslant 1-\ell\,(1-R_0)$, получим следующую верхнюю границу

$$R(\mathcal{C})\le\min_{\frac{q}{q-1}\delta\leqslant\tau\leqslant1}\left[1-\frac{\ell\tau}{\ell+\tau-1}\left(1-R^*\left(\frac{\delta}{\tau}\right)\tau\right)\right]$$

В *разделе 1.6* получена верхняя оценка минимального кодового расстояния для МПП-кодов над полем $GF(q)$ на основе подсчета числа синдромов. Основной результат этого раздела сформулирован в виде теорем 1.3 и 1.4.

Теорема 1.3. ([9]) *Пусть* $\mathcal{C}$ *– это обобщенный МПП-код длины* N *скорости* R *с минимальным кодовым расстоянием* δN *и компонентным* $[n_0,R_0n_0,d_0]$*-кодом* $\mathcal{C}_0$ *над полем GF(q). Пусть* $g_0(s,n_0,d_0)$ *– это нумератор весов кода* $\mathcal{C}_0$. *Тогда для достаточно больших* N *выполнено неравенство*

$$R(\mathcal{C})\le1-\max_{\delta/2\le\omega\le1}\left[\frac{h_q(\omega)-R_{CW}(q,\omega,\delta)}{h_{q^{m_0}}(1-p_0(\omega))}\right]+o(1),$$

где

$$p_0(\omega)=(1-\omega)^{n_0}g_0\left(\frac{\omega}{(1-\omega)(q-1)}\right).$$

[25] *Tanner R.* A recursive approach to low complexity codes // IEEE Transactions on Information Theory. 1981. Sept. Vol. 27, no. 5. P. 533–547.

Для того, чтобы сформулировать теорему 1.4 нам потребуется понятие многочлена весов строк

$$\rho(x) = \sum_{i=r_{\min}}^{r_{\max}} \rho_i x^i,$$

где ρ_i – это доля строк проверочной матрицы, имеющих вес i, а $r_{\min}$ и $r_{\max}$ – это соответственно минимальный и максимальный веса строк.

Теорема 1.4. ([9]) *Пусть $\mathcal{C}$ – это МПП-код длины N скорости R с минимальным кодовым расстоянием δN и многочленом весов строк $\rho(x)$. Тогда для достаточно большого N выполняется неравенство*

$$R(\mathcal{C}) \le 1 - \max_{\delta/2 \le \omega \le 1} \frac{h_q(\omega) - R_{CW}(q, \omega, \delta)}{h_q\left[\frac{q-1}{q}\left(1 - \rho\left(1 - \frac{q}{q-1}\omega\right)\right)\right]} + o(1).$$

В *разделе 1.7* получена верхняя оценка минимального кодового расстояния для квазициклических МПП-кодов над полем $GF(q)$. Основной результат этого раздела сформулирован в виде теоремы 1.5.

Упорядочим столбцы матрицы $\mathbf{H}_{\text{base}}$ в порядке возрастания весов. Пусть l_j – вес j-го столбца $\mathbf{H}_{\text{base}}$, $t_2 > t_1$ и $\ell = \bar{l}(2, m+1-k)$, тогда

$$\bar{l}(t_1, t_2) = \frac{1}{t_2 - t_1 + 1} \sum_{i=t_1}^{t_2} l_i.$$

Теорема 1.5. ([24]) *Пусть $\mathcal{C}$ – это КЦ МПП-код над полем GF(q) с базовой матрицей $\mathbf{H}_{base}$ размера $m \times n$,и пусть k такое целое число, что $0 \le k \le m$, тогда*

$$d(\mathcal{C}) \le (m+1)k!\ell^{m-k}.$$

Полученная оценка не зависит от s. Если m и n фиксированы и $s \to \infty$, тогда $d(\mathcal{C})$ ограничено сверху константой.

В *разделе 1.8* приводится анализ результатов, полученных для ансамбля $\mathcal{E}(b, n_0, \ell)$ при $q = 64, q = 256, q = 1024$. Использованы следующие обозначения:

- δ_{GV} – граница Варшамова–Гилберта;
- $\delta_{\text{sc}}^{(U)}$ – верхняя граница минимального кодового расстояния на основе подсчета числа синдромов;
- $\delta_{\text{short}}^{(U)}$ – верхняя граница для МПП-кодов с помощью укорочения;
- $\delta^{(L)}$ – нижняя граница для МПП-кодов;
- δ_{BHL} – лучшая верхняя граница минимального кодового расстояния недвоичных кодов[26].

[26] *Ben-Haim Y., Litsyn S.* A New Upper Bound on the Rate of Non-Binary Codes // 2006 IEEE International Symposium on Information Theory. 2006. P. 297–301.

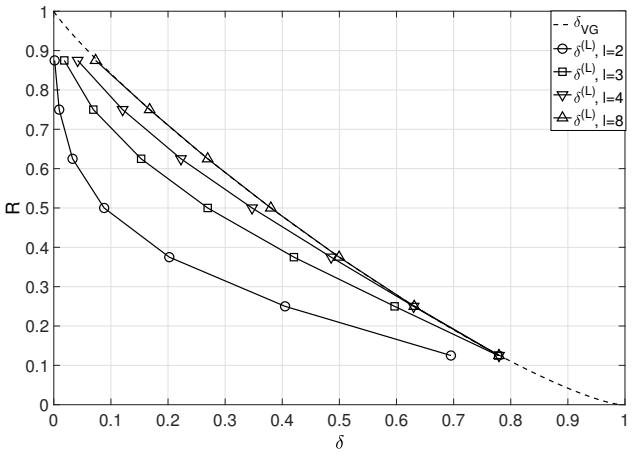

Рис. 2: Нижние границы при $q = 256$

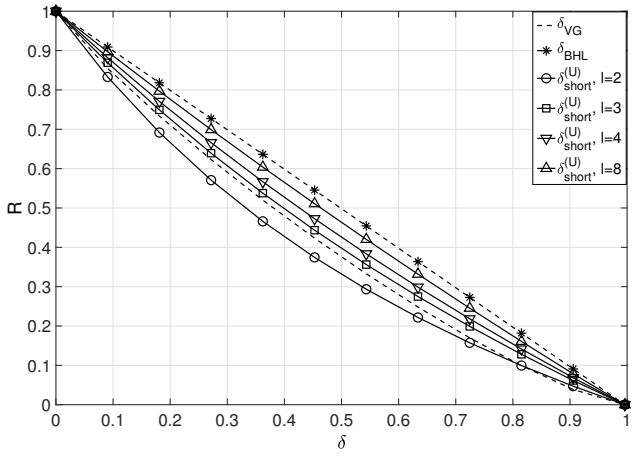

Рис. 3: Верхние границы при $q = 256$

Таблица 1: Результаты для высокоскоростных кодов, $q = 8$

$(\ell, n_0); R$	δ_{GV}	$\delta_{\text{sc}}^{(U)}$	$\delta_{\text{short}}^{(U)}$	δ_{BHL}
(3,10); 0,7	0,1260	0,2102	**0,1831**	0,2242
(3,50); 0,94	0,0179	**0,0263**	0,0313	0,0356
(3,100); 0,97	0,0080	**0,0106**	0,0141	0,0161
(3,200); 0,985	0,0036	**0,0043**	0,0064	0,0073
(3,500); 0,994	0,0013	**0,0013**	0,0022	0,0026
(3,600); 0,995	0,0011	**0,0010**	0,0018	0,0021

На рис. 2 приведено сравнение нижних границ, построенных для МПП-кодов с разным числом слоев ($\ell = 2, 3, 4, 8$). В качестве компонентного кода выбран код Рида–Соломона. На рис. 3 приведено сравнение верхних границ, построенных для МПП-кодов с разным числом слоев ($\ell = 2, 3, 4, 8$).

Сравним границы δ_{GV}, $\delta_{\text{sc}}^{(U)}$, $\delta_{\text{short}}^{(U)}$ и δ_{BHL} для случая высокоскоростных кодов над полем $GF(8)$. Результаты приведены в таблице 1. Результирующая верхняя граница (полученная из приведенных) выделена жирным. Насколько известно автору, это лучшая верхняя граница для МПП-кодов над полем $GF(q)$. Результаты первой главы опубликованы в работах [3; 9; 15; 19; 24].

Во второй главе исследуются реализуемые корректирующие свойства МПП-кодов над полем $\mathrm{GF}(q)$. Предложены новые просто реализуемые алгоритмы декодирования. Проведено теоретическое исследование предложенных алгоритмов и выведены нижние асимптотические оценки на радиусы декодирования, реализуемые данными алгоритмами. Данные оценки на сегодняшний являются наилучшими оценками на радиусы декодирования МПП-кодов над полем $\mathrm{GF}(q)$ при малой сложности реализации. Кроме того предложен метод построения проверочных матриц квазициклических МПП-кодов полем $\mathrm{GF}(q)$, которые лучше всего подходят для практического применения. Эффективность данного метода продемонстрирована с помощью имитационного моделирования. В данной главе в качестве кода-компонента используется только *код с проверкой на*

четность над полем $\mathrm{GF}(q)$.

Раздел 2.2 посвящен теоретическим оценкам радиуса декодирования, реализуемого однопороговым и многопороговым мажоритарными алгоритмом декодирования. В *разделе 2.2.1* приводятся оценки на вес обобщенного синдрома при условии W ошибок в принятой последовательности. Сначала заметим, что для любого МПП-кода из ансамбля $\mathcal{E}(b, n_0, \ell)$ выполняется следующая тривиальная верхняя оценка на вес синдрома

$$wt\,(\mathbf{S}) \le U(W) \triangleq W\ell.$$

Определим следующую функцию

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

где максимум берется по всем положительным s, таким что выполнено неравенство

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

Следующая теорема дает нижнюю границу на вес синдрома.

Теорема 2.1 ([1]) *Для любых* $0 < \alpha < 1$ *и* $\frac{2}{1-\alpha} < \ell < n_0$ *существует число* $\omega^* = \omega^*(\alpha, n_0, \ell) > 0$, *такое что*

- *в ансамбле* $\mathcal{E}(b, n_0, \ell)$ *существуют коды, для которых выполнено следующее неравенство*

$$wt\,(\mathbf{S}) > L(W) = \alpha W \ell \tag{2}$$

для любых векторов ошибок веса W, $0 < W \le W^* = \omega^* N$.

- *число таких кодов* $(G(b))$ *удовлетворяет соотношению*

$$\lim_{N\to\infty} \frac{G(b)}{|\mathcal{E}(b, n_0, \ell)|} = 1.$$

Число ω^* *– это наименьший положительный корень уравнения*

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

Заметим, что условие (3) означает, что соответствующий коду граф Таннера является несбалансированным $(\ell, n_0, \omega^*, \ell/2)$ графом-расширителем[27].

[27] *Sipser M., Spielman D. A.* Expander codes // IEEE Transactions on Information Theory. 1996. Nov. Vol. 42, no. 6. P. 1710–1722.

Выберем $\alpha = 1/2$. В соответствии с теоремой 2.1 в ансамбле $\mathcal{E}(b, n_0, \ell)$ существуют коды, для которых выполнено следующее неравенство

$$wt\,(\mathbf{S}) > L(W) = \frac{W\ell}{2} \tag{3}$$

для любых векторов ошибок веса W, $0 < W \leq W^* = \omega^*(1/2, n_0, \ell)N$. Выберем МПП-код над полем $\mathrm{GF}(q)$, который удовлетворяет свойству (3). Обозначим этот код через $\mathcal{C}^*$. Далее мы будем работать только с этим кодом.

В *разделе 2.2.2* предложен однопороговый мажоритарный алгоритм декодирования $\mathcal{A}_S$. Алгоритм является итеративным алгоритмом декодирования с жестким решением. Под *итерацией* мы понимаем последовательную обработку всех N символов декодируемой последовательности ($\mathbf{r} = (r_1, r_2, \ldots, r_N)$). Важно отметить, что алгоритм работает с символами последовательно. Это означает, что в случае замены символа сначала все изменения вносятся в декодируемую последовательность, пересчитывается синдром, и только после этого алгоритм переходит к следующему символу. Данный алгоритм является обобщением алгоритма инвертирования бита (англ. bit flipping) для двоичных МПП-кодов. Ключевое различие заключается в следующем. В двоичном случае проверочная вершина посылает двоичное сообщение символьной вершине: произвести инвертирование или нет. В недвоичном случае проверочные вершины посылают значения ошибок, и алгоритм должен это учитывать.

Опишем основные шаги алгоритма.

Вычисление сообщений от проверочных узлов. Соответствующая символьная вершина v_i подключена к ℓ проверочным вершинам c_j, $j \in \Gamma(i)$. Каждая из этих проверочных вершин посылает v_i сообщение $m_{j\to i}$, $j \in \Gamma(i)$. Сообщения вычисляются следующим образом

$$m_{j\to i} = -h_{j,i}^{-1} s_j,$$

где s_j – синдром j-го кода-компонента

Критерий замены символа. Пусть сообщения $m_{j\to i}$, $j \in \Gamma(i)$ вычислены в соответствии с правилом, приведенным выше. Пусть $A_{\max}$ – это самое большое подмножество одинаковых ненулевых сообщений, пусть $a = |A_{\max}|$ и пусть m – это значение сообщений из $A_{\max}$. Обозначим через θ величину порога – целое число, такое что $0 \leq \theta < \ell$. Наконец, обозначим через z число ненулевых сообщений. Сформулируем критерий замены. Если $a - z > \theta$ мы заменяем символ r_i символом $r_i + m$, и пересчитываем синдром. После алгоритм переходит к следующему символу. В пределах этого раздела $\theta = 0$. Мы ввели этот параметр для нашего удобства и будем использовать его в многопороговой версии алгоритма.

Критерий останова. Алгоритм останавливается, если во время итерации не было сделано изменений в декодируемой последовательности $\mathbf{r}$.

Основной результат *раздела 2.2.2* сформулирован в виде теоремы 2.2.

Теорема 2.2 ([11]) *Пусть $\mathcal{C}^*$ – это МПП-код над полем $GF(q)$, удовлетворяющий (3). Если число ошибок в принятой последовательности*

$$W \le W^{(S)} = \frac{W^*}{2}\frac{\ell+2}{\ell+1},$$

то алгоритм $\mathcal{A}_S$ (с порогом $\theta = 0$) исправит все ошибки со сложностью $O(N \log N)$.

Следствие 2.1*Введем следующее обозначение*

$$\alpha^{(S)} = \frac{\ell+2}{2(\ell+1)}$$

и рассмотрим асимптотическую оценку ($N \to \infty$) относительного радиуса декодирования $\rho^{(S)}$, реализуемого Алгоритмом 1*. Имеем*

$$\rho^{(S)} \ge \frac{W^{(S)}}{N} = \alpha^{(S)}\omega^*.$$

В *разделе 2.2.3* оценка радиуса декодирования улучшена путем перехода к многопороговому декодеру. Пусть $t \ge 1$, введем последовательность целочисленных порогов

$$0 = \theta_1 < \theta_2 < \ldots < \theta_t < \ell.$$

Опишем многопороговый алгоритм декодирования $\mathcal{A}_M$. Идея состоит в последовательном применении алгоритма $\mathcal{A}_S$ с разными порогами замены символа к декодируемой последовательности. Мы начинаем с наибольшего порога θ_t и заканчиваем наименьшим – $\theta_1 = 0$. Основной результат *раздела 2.2.3* сформулирован в виде теоремы 2.3.

Теорема 2.3. ([11]) *Пусть $\mathcal{C}^*$ – это МПП-код над полем $GF(q)$, удовлетворяющий свойству* (3)*. Пусть $0 = \theta_1 < \theta_2 < \ldots < \theta_t < \ell$ – последовательность порогов. Если число ошибок в принятой последовательности*

$$W \le W_{t+1},$$

где

$$W_i = W_{i-1}\frac{\ell+3\theta_{i-1}+2}{\ell+2\theta_{i-1}+\theta_i+2},\ W_1 = W^*, \theta_{t+1} = \ell,$$

то алгоритм $\mathcal{A}_M$ исправит все ошибки со сложностью $O(N \log N)$.

Рассмотрим случай, когда присутствуют все пороги от 0 до $\ell - 1$. Тогда

$$W^{(M)} = \left(\prod_{i=1}^{\ell}\frac{\ell+3i-1}{\ell+3i}\right)W^*.$$

Введем обозначение

$$\alpha^{(M)} = \prod_{i=1}^{\ell}\frac{\ell+3i-1}{\ell+3i}$$

Таблица 2: Результаты для $q = 64$

$(\ell,\, n_0);\, R$	δ	ω^*	$\rho^{(S)}$	$\rho^{(M)}$	$\rho^{(M)}/\rho^{(S)}$
(21, 24); 0.125	0.7355	0.0156	0.0082	0.0099	1.207
(24, 32); 0.25	0.5863	0.0131	0.0068	0.0083	1.221
(20, 32); 0.375	0.4585	0.0104	0.0054	0.0066	1.222
(22, 44); 0.5	0.3445	0.0081	0.0042	0.0052	1.238
(27, 72); 0.625	0.2415	0.0059	0.0031	0.0038	1.226
(24, 96); 0.75	0.1485	0.0037	0.0019	0.0024	1.263
(26, 208); 0.875	0.0661	0.0017	0.0009	0.0011	1.222

и рассмотрим асимптотическую оценку ($N \to \infty$) относительного радиуса декодирования ($\rho^{(M)}$), реализуемого алгоритмом $\mathcal{A}_M$ (в случае, когда присутствуют все пороги). Получим следующее

$$\rho^{(M)} \geq \frac{W^{(M)}}{N} = \alpha^{(M)}\omega^*.$$

Лемма 2.4. *Выполняется следующее неравенство*

$$0.630... = \sqrt[3]{\frac{1}{4}} \leq \alpha^{(M)} \leq \sqrt[3]{\frac{\ell+2}{4\ell+2}}.$$

В *разделе 2.2.4* приводится анализ результатов. В таблице 2 приведены зависимости δ (относительного минимального расстояния), ω^*, $\rho^{(S)}$ и $\rho^{(M)}$ от скорости кода R. Отметим, что ℓ подбиралось в каждом случае, чтобы максимизировать соответствующую величину. Для нашего случае максимумы величин ω^*, $\rho^{(S)}$ и $\rho^{(M)}$ были достигнуты на одном и том же ℓ, параметр ℓ также приведен в таблицах. Отметим, что отношение $\rho^{(M)}/\rho^{(S)} \geq 1.2$ для всех рассмотренных нами случаев. Таким, образом переход к многим порогам приводит к увеличению радиуса декодирования, не влияя на порядок сложности. Насколько известно автору, полученные здесь оценки являются лучшими на сегодняшний день оценками радиуса декодирования, реализуемого МПП-кодами над полем $\mathrm{GF}(q)$ при использовании алгоритма декодирования с малой сложностью.

Для доказательства теоретических результатов был использован последовательный мажоритарный алгоритм декодирования, так как для других алгоритмов доказательства становятся проблематичными. На практике же можно использовать более эффективные алгоритмы, такие как алгоритм распространения доверия. В *разделе 2.3.2* предложен алгоритм построения проверочных матриц КЦ МПП-кодов над полем $\mathrm{GF}(q)$ для алгоритма распространения доверия. Известно, что псевдокодовые слова являются причиной плохой работы алгоритма распространения доверия. Псевдокодовые слова в свою очередь появляются из-за наличия коротких циклов в проверочной матрице. Таким образом, главная задача алгоритма заключается в устранении циклов при расширении

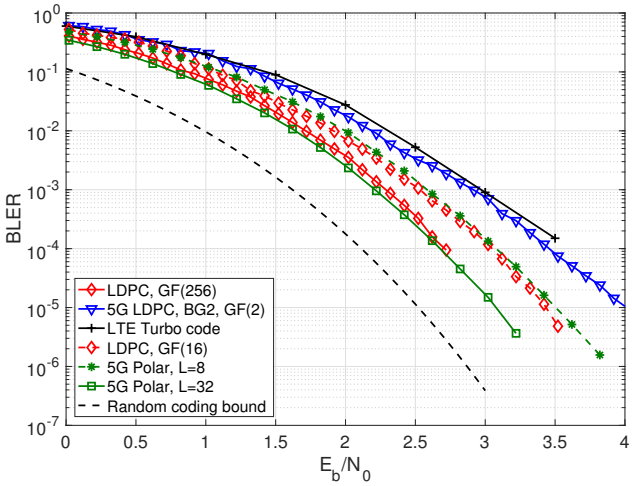

Рис. 4: Результаты моделирования для канала с АБГШ и модуляцией BPSK, $K = 64$ бит и $N = 256$ бит.

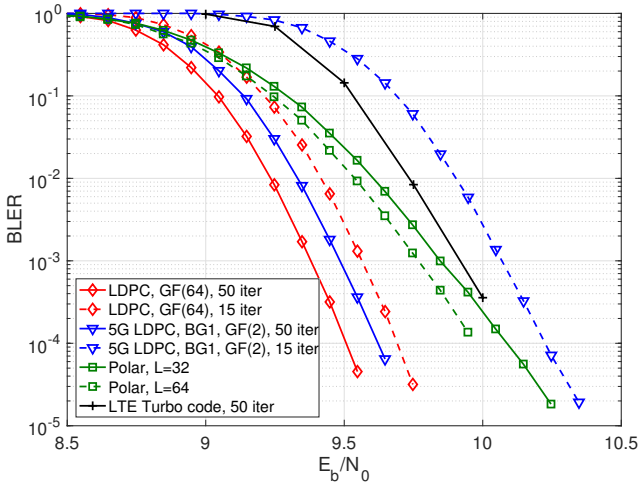

Рис. 5: Результаты моделирования для канала с АБГШ и модуляцией КАМ-64, $K = 4926$ бит и $N = 6270$ бит.

базовой матрицы. Алгоритм состоит из двух шагов. На первом шаге на основе анализа порога итеративного декодирования выбирается базовая матрица (протограф). На втором шаге алгоритм находит короткие циклы в базовой матрице и пытается их разрушить путем выбора циркулянтов и элементов поля GF(q). В первую очередь алгоритм старается разрушить циклы с наименьшим числом ребер, выходящих наружу цикла.

В *разделе 2.3.3* представлены результаты имитационного моделирования. Продемонстрируем эффективность предложенного алгоритма на двух примерах. В первом случае рассмотрен канал с АБГШ и модуляцией КАМ-64, $K = 4926$ бит и $N = 6270$ бит. Такие параметры соответствуют одному из случаев стандарта 3GPP New Radio (NR), который должен стать основополагающим стандартом для систем беспроводной связи пятого поколения (5G). Во втором случае рассмотрен канал с АБГШ и модуляцией BPSK, $K = 64$ бит и $N = 256$ бит. Эти параметры характерны для стандарта LPWAN (Low-power Wide-area Network, энергоэффективная сеть дальнего радиуса действия) и систем интернета вещей. Результаты приведены на рис. 4 и рис. 5 соответственно. Для сравнения также приведены результаты для двоичных МПП-кодов из стандарта 3GPP NR, турбо-кодов из стандарта LTE (4G) и полярных кодов. Мы видим, что КЦ МПП-коды над полем GF(q), в отличие от остальных классов кодов, одинаково хорошо работают как при большой, так и при малой длине блока. Результаты второй главы опубликованы в работах [1; 2; 11; 18; 24; 25].

В соответствии с результатами предыдущей главы двоичные МПП-коды достаточно плохо работают при малой длине блока. Это связано с наличием в проверочной матрице таких кодов большого числа множеств останова (англ. trapping set), каждое из которых формируется на основе одного или нескольких циклов малой длины. Главная задача, решаемая **в третьей главе**, – это улуч-

шение помехоустойчивости алгоритмов декодирования двоичных МПП-кодов с использованием методов машинного обучения и, в частности, глубоких нейронных сетей. Отметим, что в литературе уже были попытки построить декодеры на основе нейронных сетей. Легко видеть, что эта задача классификации: выход канала необходимо отнести к одному из классов (кодовых слов). Очевидное и существенное отличие данной задачи от традиционных задач классификации заключается в экспоненциально большом числе классов. Действительно, ведь уже линейный код длины $N = 100$ бит и скорости $R = 0.5$ содержит 2^{50} кодовых слов. Даже это количество слов слишком велико, чтобы полностью обучить нейронную сеть (иными словами, показать ей все слова). Таким образом, единственный способ победить проклятие размерности – это комбинация существующих методов декодирования и алгоритмов машинного обучения. За основу был взят подход с использованием алгоритма распространения доверия. Нейронная сеть строится с использованием правил алгоритма распространения доверия: связи в слоях определяются графом Таннера, а также использованы специальные функции активации. В результате получим разреженную нейронную сеть со специальной архитектурой. Преимуществами данного подхода являются малое число обучаемых параметров и возможность обучения только на нулевом слове.

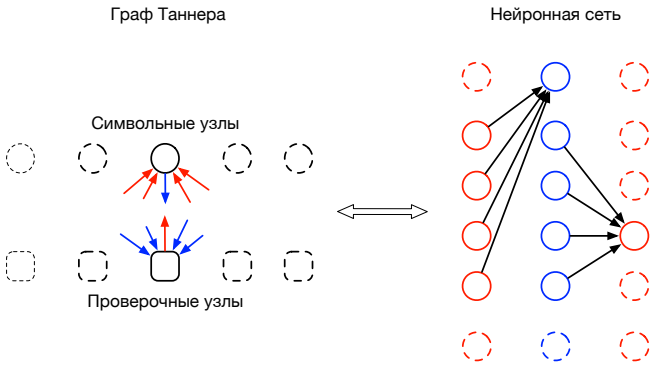

Рис. 6: Граф Таннера и нейронная сеть

В *разделе 3.3* описана архитектура нейронной сети. Связи между слоями устанавливаются на основе связей (ребер) в графе Таннера, соответствующем коду. Можно сказать, что граф нейронной сети получается “разворачиванием” графа Таннера. Поясним сказанное на рис. 6. Вершины нейронной сети соответствуют сообщениям, передаваемым по ребрам графа Таннера, а ребра нейронной сети показывают, от каких сообщения зависит текущее сообщение. На рис. 6 синим цветом выделены сообщения, идущие от вершин-символов к вершинам-проверкам, а красным – сообщения, идущие в другую сторону. Такими же цветами выделены узлы результирующей нейронной сети. На рис. 6 показана только одна итерация, соответствующая двум слоям (символьному и проверочному) в нейронной сети. Разреженная нейронная сеть, построенная на основе графа Таннера, состоит из входного слоя, внутренних слоев (по два на каждую итерацию) и выходного слоя. Построенная нейронная сеть производит все те же самые операции, что и алгоритм распространения доверия. Для улучшения помехоустойчивости мы добавляем в нашу нейронную сеть обучаемые параметры (веса). Отметим, что веса должны быть неотрицательными – это условие гарантирует возможность обучения лишь на нулевом слове. Обучаемые веса позволяют нам улучшить помехоустойчивость,

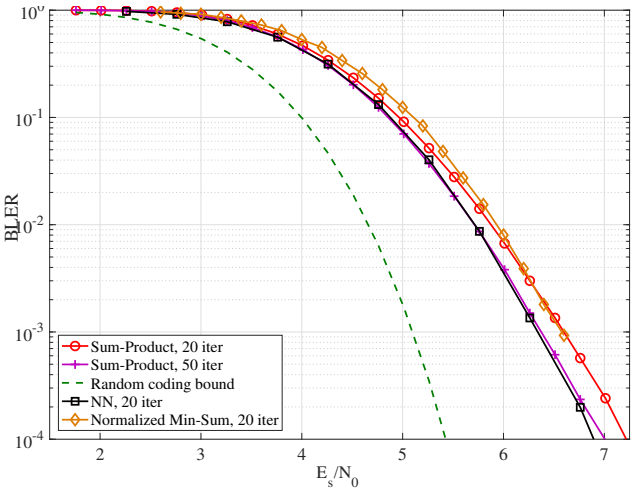

Рис. 7: Канал с АБГШ и модуляцией QPSK, $R = 0.75$, $K = 120$

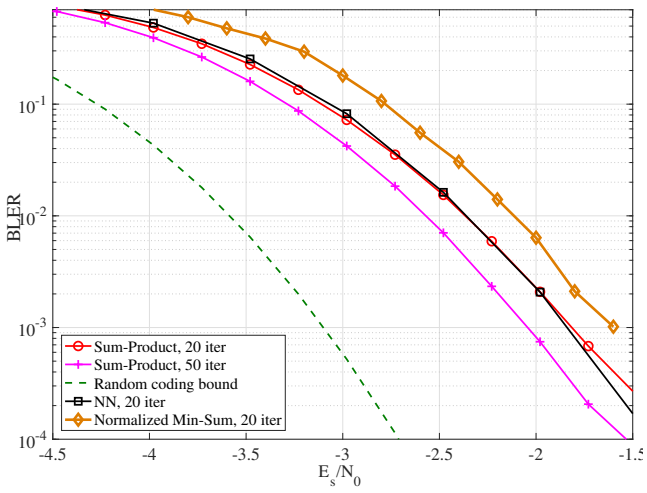

Рис. 8: Канал с АБГШ и модуляцией QPSK, $R = 0.2$, $K = 120$

не меняя код. В качестве функций активации мы выберем функцию суммы на символьном слое и функцию минимум на проверочном слое, т.е. нейронная сеть работает в соответствии с правилами алгоритма Минимум-Сумма. Отметим, что идея добавления весов к алгоритму Минимум-Сумма не нова, но наш подход позволяет регулярным образом (с использованием алгоритма обратного распространения ошибки) выбирать оптимальные значения весов. Практически все использующиеся на практике МПП-коды являются квазициклическими. Мы используем это свойство и уменьшим количество обучаемых параметров, а именно используем одни и те же величины для циркулянта. Для улучшения помехоустойчивости и ускорения процесса обучения мы добавим остаточные соединения (англ. residual connection). В качестве функции потерь была выбрана функция перекрестной энтропии.

В *разделе 3.4* приведены результаты имитационного моделирования. Продемонстрируем эффективность предложенного алгоритма на двух примерах $R = \{0.75, 0.5\}$, число информационных бит K во всех случаях одинаково и равно 120. В обоих случаях рассматривается канал с АБГШ и модуляцией QPSK. Можно видеть, что новый алгоритм значительно лучше (0.2–0.3 дБ по уровню BLER $= 10^{-2}$) стандартного алгоритма Минимум-Сумма с нормализацией. Разрыв становится больше с уменьшением скорости кода. Также отметим, что данный метод позволяет сократить требуемое число итераций декодера (с 50 до 20). Данный результат можно объяснить так: обучаемые веса помогают уничтожать множества останова декодера.

Четвертая глава посвящена применению МПП-кодов в сценарии множественного доступа. Получившая в последние годы большую популярность концепция Интернета вещей подразумевает взаимодействие большого числа автономных устройств, редко передающих небольшие объемы данных и обладающих ограниченным запасом энергии. Данная задача активно исследуется в рамках комитета по стандартизации 3GPP и получила название массовое межма-

шинное взаимодействие (massive machine type communications, mMTC). Данный сценарий является одним из ключевых сценариев для беспроводных сетей пятого поколения (5G). С целью уменьшения сложности аппаратного обеспечения, задержки и энергопотребления целесообразно перейти к доступу без предварительного подключения (англ., grant-free). Иными словами, устройство передает пакет сразу, как он появился без установления соединения и запроса на передачу. В литературе данная проблема также известна как *некоординированный множественный доступ* или *случайный доступ*. Основным отличием нашей постановки является огромное число устройств, что приводит к значительно большей вероятности коллизии. Для решения этой проблемы требуются новые классы кодов, которые могут разрешать коллизии, возникающие при несогласованных передачах. В этой главе мы разрабатываем схемы передачи на основе МПП-кодов.

Далее мы рассматриваем несколько моделей каналов, начиная с идеализированных бесшумных каналов[28] и заканчивая более близкими к реальности каналами. Приведем формальные описания. Обозначим число активных пользователей через S, $S \geqslant 2$.

Бесшумный канал без информации об интенсивности (А-канал). Пусть $\mathcal{Q} = \{1, 2, \ldots, Q\}$. Если входе канала слова $X_i = (X_{i,1}, \ldots, X_{i,n}) \in \mathcal{Q}^n$, $i = 1, \ldots, S$, то на выходе

$$Y = \left(\bigcup\nolimits_{i=1}^{S} X_{i,1}, \ldots, \bigcup\nolimits_{i=1}^{S} X_{i,n} \right).$$

В литературе данный канал также называют гиперканалом множественного доступа[29].

Заметим, что такая модель канала допускает и более широкую трактовку. Так входы канала в моменты времени $j = 1, \ldots, n$ можно рассматривать как двоичные векторы $\mathbf{x}_{i,j}$ длины Q с одной единицей в позиции, соответствующей элементу $X_{i,j}$ множества $\mathcal{Q}$. В этом случае выход канала можно рассматривать как поэлементную дизъюнкцию векторов на входе, т.е.

$$Y = \left(\mathbf{y}_1 = \bigvee\nolimits_{i=1}^{S} \mathbf{x}_{i,1}, \ldots, \mathbf{y}_n = \bigvee\nolimits_{i=1}^{S} \mathbf{x}_{i,n} \right).$$

Таким образом, этот канал является, по сути, векторным дизъюнктивным каналом [5].

Бесшумный канал с информацией об интенсивности (Б-канал). Данный канал отличается от А-канала лишь тем, что помимо списка переданных элементов выход канала содержит информацию о кратности каждого элемента. Входы

---

[28] *Shih-Chun Chang, Wolf J.* On the T-user M-frequency noiseless multiple-access channel with and without intensity information // IEEE Transactions on Information Theory. 1981. Vol. 27, no. 1. P. 41–48.

[29] *Бассалыго Л. А., Рыков В. В.* Гиперканал множественного доступа // Пробл. передачи информ. 2013. т. 49, № 4. с. 3—12.

канала точно такие же, как в случае A-канала, а выход можно представить как поэлементную сумму векторов на входе, т.е.

$$Y = \left(\mathbf{y}_1 = \sum\nolimits_{i=1}^{S} \mathbf{x}_{i,1}, \ldots, \mathbf{y}_n = \sum\nolimits_{i=1}^{S} \mathbf{x}_{i,n} \right).$$

Таким образом, этот канал является, по сути, векторным суммирующим каналом [7].

Суммирующий канал с АБГШ. Если входе канала слова $X_i = (X_{i,1}, \ldots, X_{i,n}) \in \mathbb{R}^n$, $i = 1, \ldots, S$, то на выходе

$$Y = \sum_{i=1}^{S} X_i + Z, \quad Z \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_n). \tag{4}$$

Также потребуем $\|X_i\|_2^2 \leq Pn$, $i = 1, \ldots, S$, для некоторого заданного ограничения на входную мощность P, $P > 0$.

Канал Рэлея. Если входе канала слова $X_i = (X_{i,1}, \ldots, X_{i,n}) \in \mathbb{C}^n$, $i = 1, \ldots, S$, то на выходе

$$Y = \sum_{i=1}^{S} H_i X_i + Z, \quad Z \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_n), H_i \sim \mathcal{CN}(0, 1), i = 1, \ldots, S. \tag{5}$$

Также потребуем $\|X_i\|_2^2 \leq Pn$, $i = 1, \ldots, S$, для некоторого заданного ограничения на входную мощность P, $P > 0$.

Осталось пояснить, как мы будем измерять вероятность ошибки. Пусть в канал передаются сообщения $W_1, W_2, \ldots, W_S$, Y – это выход канала, а $L(Y)$ – список восстановленных сообщений. Тогда

$$p_e = \frac{1}{S} \sum_{i=1}^{S} \Pr[W_i \notin L(Y)].$$

В *разделе 4.2* рассматриваются бесшумные каналы без/с информацией об интенсивности (A- и Б-каналы). В литературе была исследована пропускная способность A-канала при координированной[30],[31] и некоординированной[32],[33] передаче. Отметим, что некоординированная передача соответствует использованию однопользовательского приема (другие пользователи рассматриваются

[30] *Shih-Chun Chang, Wolf J.* On the T-user M-frequency noiseless multiple-access channel with and without intensity information // IEEE Transactions on Information Theory. 1981. Vol. 27, no. 1. P. 41–48.

[31] *Бассалыго Л. А., Пинскер М. С.* Вычисление асимптотики суммарной пропускной способности M-частотного бесшумного канала с множественным доступом для T пользователей // Пробл. передачи информ. 2000. т. 36, № 2. с. 3—9.

[32] *Вильхельмссон Л., Зигангиров К.* Об асимптотической пропускной способности одного многопользовательского канала // Пробл. передачи информ. 1997. т. 33, № 1. с. 12—20.

[33] *Гобер П., Винк А. Х.* Замечание к статье Л. Вильхельмссона и К.Ш. Зигангирова «Об асимптотической пропускной способности одного многопользовательского канала» // Пробл. передачи информ. 2000. т. 36, № 1. с. 21—25.

как шум), в то время как координированная передача – многопользовательского приема. В этом разделе нами была исследована пропускная способность Б-канала. Нас интересует асимптотика следующего вида: $Q \to \infty$, $S = \gamma Q$ $(0 < \gamma < \infty)$.

В *разделе 4.2.1* рассмотрен случай координированной передачи. Общая пропускная способность канала C_{c} при координированной передаче определяется следующим образом

$$\begin{aligned} C_{\mathrm{c}}(Q,S) &= \max\{I(X_1,X_2,\ldots,X_S;Y)\} = \\ &= \max\{H(Y) - H(Y|X_1,X_2,\ldots,X_S)\} = \\ &= \max\{H(Y)\}, \end{aligned}$$

где $H(X)$ – энтропия случайной величины X, а максимум берется по всем возможным независимым распределениям величин $X_1, X_2, \ldots, X_S$.

Так как на выходе канала могут появляться только векторы длины Q с суммой элементов S, то

$$C_{\mathrm{c}}(Q,S) \leqslant C_{\mathrm{c}}^{(\mathrm{U})}(Q,S) = \log_2 \binom{S+Q-1}{S}, \tag{6}$$

ведь всего таких векторов в точности $\binom{S+Q-1}{S}$.

Введем следующую величину

$$c_{\mathrm{c}}(\gamma) = \lim_{Q\to\infty} \{C_{\mathrm{c}}(Q,\gamma Q)/Q\}.$$

Доказательство существования функции $c_{\mathrm{c}}(\gamma)$ приведено в [7].

Из (6) легко получить, что

$$c_{\mathrm{c}}(\gamma) \leqslant c_{\mathrm{c}}^{(\mathrm{U})}(\gamma) = (\gamma+1)\log_2(\gamma+1) - \gamma\log_2(\gamma).$$

Нижняя граница представлена в следующей теореме.

Теорема 4.1. ([7])*Пусть* $0 < \gamma < \infty$, *тогда*

$$c_c(\gamma) \geqslant c_c^{(L)}(\gamma) = \sum_{i=0}^{\infty} \left[\frac{\gamma^i}{i!} e^{-\gamma} \log_2(i!)\right] - \gamma \log_2\left(\frac{\gamma}{e}\right).$$

На рис. 9 показаны полученные границы $c_{\mathrm{c}}^{(\mathrm{L})}(\gamma)$ и $c_{\mathrm{c}}^{(\mathrm{U})}(\gamma)$, также для сравнения приведена нижняя граница[34] $c_{\mathrm{c}}^{(\mathrm{disj})}(\gamma)$ пропускной способности А-канала при координированной передаче.

[34] *Бассалыго Л. А., Пинскер М. С.* Вычисление асимптотики суммарной пропускной способности М-частотного бесшумного канала с множественным доступом для Т пользователей // Пробл. передачи информ. 2000. т. 36, № 2. с. 3—9.

В *разделе 4.2.2* рассмотрен случай некоординированной передачи. Далее мы рассматриваем только случай, когда все пользователи используют одинаковые распределения входных символов, т.е.

$$P(X_i = j) = p_j, \quad i = 1, \ldots, S,\ j = 1, \ldots, Q.$$

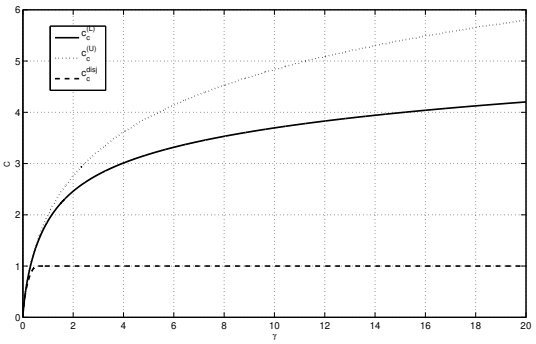

Рис. 9: Границы для $c_{\text{c}}(\gamma)$

Пропускная способность C_i для i-го пользователя может быть вычислена так

$$C_i(Q, S) = \max\{I(X_i; Y)\},$$

где максимум берется по всем распределениям X_i.

Так как пользователи являются равноправными, то общая пропускная способность C_{uc} при некоординированной передаче равна сумме пропускных способностей отдельных пользователей

$$C_{\text{uc}}(Q, S) = \sum_{i=1}^{S} C_i(Q, S) = S \max_{p_1, p_2, \ldots, p_Q} \{I(X; Y)\}.$$

Здесь, в отличие от случая координированной передачи, введем две величины ($Q \to \infty$, $S = \gamma Q$)

$$\overline{c_{\text{uc}}(\gamma)} = \limsup_{Q \to \infty} \{C_{\text{uc}}(Q, \gamma Q)/Q\}$$

и

$$\underline{c_{\text{uc}}(\gamma)} = \liminf_{Q \to \infty} \{C_{\text{uc}}(Q, \gamma Q)/Q\}.$$

Конечность верхнего и нижнего пределов следует из полученных ниже границ.

Теорема 4.2. ([7]) *Справедливо неравенство*

$$C_{uc}(Q, S) \leqslant S \log_2 \left(1 + \frac{Q-1}{S}\right).$$

Теперь, использовав несколько входных распределений, мы получим нижнюю границу для $\underline{c_{\text{uc}}}$.

Теорема 4.3. ([7]) *Справедливо неравенство*

$$\underline{c_{uc}(\gamma)} \geqslant c_{uc}^{(L)}(\gamma) = \begin{cases} \gamma \sum\limits_{i=0}^{\infty} \frac{\gamma^i}{i!} e^{-\gamma} \log_2 \left(\frac{i+1}{\gamma}\right), & \gamma < \gamma^*, \\ 0,8371..., & \gamma \geqslant \gamma^*. \end{cases}$$

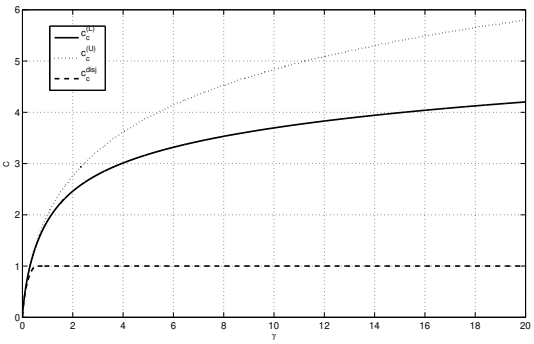

Рис. 10: Границы для $c_{\text{uc}}(\gamma)$

На рис. 10 показаны полученные границы $c_{\text{uc}}^{(\text{L})}(\gamma)$ и $c_{\text{uc}}^{(\text{U})}(\gamma)$, также для сравнения приведена нижняя граница[35],[36] $c_{\text{uc}}^{(\text{disj})}(\gamma)$ пропускной способности А-канала при некоординированной передаче. Мы видим, что относительная пропускная способность Б-канала при некоординированной передаче ограничена сверху константой. Также можно заметить, что выигрыш по сравнению с А-каналом невелик.

В *разделе 4.2.3* предложена схема передачи для А-канала. Каждый пользователь кодирует передаваемую информацию Q-ичным (n, k, d) кодом C (все пользователи используют один и тот же код).

Пусть $S = \gamma Q$. Введем асимптотическую величину

$$\rho(\gamma, k, c) = \lim_{Q\to\infty} \frac{R_\Sigma\left(Q, \gamma Q, k, 2^{-cn}\right)}{Q}, \tag{7}$$

характеризующую количество информации, передаваемой всеми активными пользователями в расчете на один подканал с вероятностью отказа от декодирования $p_e \leq 2^{-cn}$.

Теорема 4.5. ([5])*При* $\gamma < -\ln\left(1 - 2^{-c}\right)$ *справедливо соотношение*

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

Л. Вильхельмссон и К. Ш. Зигангиров показали[37], что при некоординированной передаче в случае равномерного распределения вероятностей символов на входе (как и в рассматриваемом случае) $\rho(\gamma, k, c) \leqslant -\gamma\log_2\left(1 - e^{-\gamma}\right)$. Предложенная конструкция позволяет обеспечить асимптотическую относительную суммарную скорость передачи сколь угодно близкую к этой верхней границе при $c = \varepsilon$.

В *разделе 4.3* рассмотрен суммирующий канал с АБГШ, а также предложена схемы кодирования на основе МПП-кодов и алгоритма совместного итеративного декодирования. Мы предполагаем, что пользователи используют разные кодовые книги $\mathcal{C}_1, \ldots, \mathcal{C}_S$, полученные из общей кодовой книги $\mathcal{C}$ случайными перестановками. Для того, чтобы построить кодовую книгу $\mathcal{C}$ рассмотрим слова двоичного $[n, k]$ МПП-кода и заменим каждый 0 на $+\sqrt{P}$, а каждую 1 на $-\sqrt{P}$.

[35] *Вильхельмссон Л., Зигангиров К.* Об асимптотической пропускной способности одного многопользовательского канала // Пробл. передачи информ. 1997. т. 33, № 1. с. 12—20.

[36] *Гобер П., Винк А. Х.* Замечание к статье Л. Вильхельмссона и К.Ш. Зигангирова «Об асимптотической пропускной способности одного многопользовательского канала» // Пробл. передачи информ. 2000. т. 36, № 1. с. 21—25.

[37] *Вильхельмссон Л., Зигангиров К.* Об асимптотической пропускной способности одного многопользовательского канала // Пробл. передачи информ. 1997. т. 33, № 1. с. 12—20.

Мы можем представить правило максимального правдоподобия для бита в виде фактор-графа[38], приведенного на рис. 11.

При декодировании мы используем итеративный алгоритм распространения доверия, являющийся частным случаем широкого класса алгоритмов передачи сообщений (англ. message passing). Далее итерации нашего алгоритма мы будем называть внешними итерациями, а под внутренними итерациями понимать итерации при декодировании пользовательских МПП-кодов.

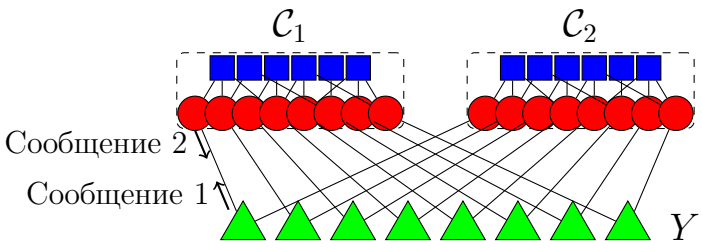

Рис. 11: Алгоритм совместного итеративного декодирования, фактор-граф для случая $S = 2$.

Для построения МПП-кодов нами был модифицирован метод PEXIT[39]. Отметим лишь существенные отличия от случая одного пользователя. Многопользовательский канал с АБГШ не является симметричным, следовательно, метод PEXIT нельзя применить для нулевого кодового слова. В связи с этим была произведена модификация метода передачи, заключающаяся в добавлении и вычитании случайного вектора, распределенного равномерно на $\{0,1\}^n$ и делающая канал симметричным. Имитационное моделирование показало, что предложенная схема выигрывает более 1.5 дБ у схем кодирования, представленных в литературе. Выигрыш растет с ростом S. Также отметим, что с увеличением S нужно использовать все более разреженные МПП-коды. Так для случая $S = 2$ наш алгоритм построил код со средним весом столбцов 3.5, в то же самое время для $S = 4$ средний вес столбцов – 1.9.

В *разделе 4.4* рассмотрен канал Рэлея. В *разделе 4.4.1* выводится граница несуществования

Теорема 4.7. ([13]) *Пусть*

$$L_n = n\log(1+PG) + \sum_{i=1}^{n}\left(1 - |\sqrt{PG}Z_i - \sqrt{1+PG}|^2\right) \tag{8}$$

$$S_n = n\log(1+PG) + \sum_{i=1}^{n}\left(1 - \frac{|\sqrt{PG}Z_i - 1|^2}{1+PG}\right) \tag{9}$$

где $G = |H|^2$ *and* $Z_i \overset{iid}{\sim} \mathcal{CN}(0,1)$. *Тогда для любого* n *и* $0 < \epsilon < 1$ *выполняется неравенство*

$$\log(M) \le \log(S) + \log\frac{1}{\Pr\left[L_n \ge n\gamma_n\right]}, \tag{10}$$

[38] *Richardson T., Urbanke R.* Modern coding theory. Cambridge university press, 2008.

[39] *Liva G., Chiani M.* Protograph LDPC Codes Design Based on EXIT Analysis // IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference. 11.2007. с. 3250—3254.

где γ_n – это решение уравнения

$$\Pr\left[S_n \le n\gamma_n\right] = \epsilon. \tag{11}$$

В *разделе 4.4.2* выводятся границы существования на основе метода проекций [13] и метода последовательного погашения интерференции (ППИ). Во всех случаях ниже применяется метод случайного кодирования с гауссовской кодовой книгой: каждое кодовое слово X_j порождается независимо от других в соответствии с распределением $\mathcal{CN}(0, P'I_{n_1})$, где $P' \le P$. Если $\|X_j\|^2 > n_1 P$, то передачи не происходит (можно сказать, что в канал посылается вектор 0). Пусть $p^*(M, n, P, H)$ – это граница на вероятность ошибки при фиксированной скорости и длине для однопользовательского случая (отметим, что коэффициент H в данном случае неизвестен декодеру).

Теорема 4.9. ([33]) *Зафиксируем $P' < P$. Пусть $T \le S$. При условии идеального погашения интерференции для канала (5) с S пользователями и ограничением на мощность передачи P существует код $\mathcal{C} \in \mathcal{E}(M, n)$, такой что выполнена следующая граница*

$$p_e(\mathcal{C}, T, S) \le p_0 + \frac{S-T}{S} + \frac{1}{S}\sum_{i=1}^{T}(T-i+1)\mathbb{E}\left[p^*\left(M, n, \frac{P'V}{1+\sum_{j=i+1}^{S}|H_j|^2}, H_i\right)\right],$$

где

$$p_0 = \frac{\binom{S}{2}}{M} + S\Pr\left[\frac{P'}{2}\sum_{i=1}^{2n_1}\xi_i^2 > nP\right], \quad \xi_i \overset{iid}{\sim} \mathcal{N}(0,1)$$

и математическое ожидание берется по переменным $H_1, H_2, \ldots, H_S$: $|H_1| \ge |H_2| \ge \ldots \ge |H_S|$.

В *разделе 4.4.3* описаны схемы кодирования на основе МПП-кодов. Начнем со схемы совместного итеративного декодирования. Данная схема строится на основе схемы из раздела 4.3. Необходимо добавить в фактор-граф четвертый тип узлов, соответствующих коэффициентам замирания. Отметим, что алгоритм декодирования также осуществляет оценку коэффициентов замирания, являющихся скрытыми параметрами модели. В пределах одной внешней итерации пользовательские сообщения декодируются последовательно. Это необходимо, чтобы разрушить симметрию, ведь в соответствии с моделью пользователи используют одну и ту же кодовую книгу, и если декодировать их одновременно, то все МПП-коды выдадут одно и то же решение. Для практической реализации этого алгоритма мы используем модель смеси гауссовских распределений (СГР).

Перейдем к практической схеме на основе алгоритма ППИ. Основная идея алгоритма может быть описана следующим образом. Мы декодируем сильнейшего из оставшихся пользователей и вычитаем его из принятого сигнала. Для

первого шага применяется обычный однопользовательский алгоритм декодирования МПП-кода. Наиболее интересным представляется второй шаг. Сложность состоит в том, что мы знаем кодовое слово, но не знаем коэффициента замирания, что делает вычитание проблематичным. Рассмотрим этот шаг более подробно. Пусть $\mathcal{C}_0$ – это множество найденных кодовых слов. Мы предлагаем следующее правило вычитания (через Y' обозначим выход канала после удаления интерференции) $Y' = Y - P_{<\mathcal{C}_0>}Y$, где $P_{<\mathcal{C}_0>}Y$ – это оператор ортогональной проекции Y на подпространство, порожденное векторами из множества $\mathcal{C}_0$.

Раздел 4.4.5 посвящен применению разработанных схем на базе МПП-кодов в сценарии массового случайного доступа. Начнем с модели системы[40]. В системе работают $K_{\text{tot}} \gg 1$ пользователей, но в каждый момент времени лишь K_a пользователей являются активными. Передача ведется кадрами длины n комплексных отсчетов. В системе есть синхронизация по кадрам, для этого базовая станция рассылает сигнальные сообщения (англ., beacons), обозначающие начало кадра. В кадре каждый из активных пользователей передает k-битное сообщение. Мы полагаем, что пользователи используют одно и то же множество сообщений $[M] \triangleq \{1, \ldots, M\}$ и общую кодовую книгу $\mathcal{C} = \{X(W)\}_{W=1}^{M}$ размера M. Через $W_i \in [M]$ обозначим сообщение пользователя i. Для того, чтобы передать сообщение W_i, пользователь использует кодовое слово $X_i = X(W_i) \in \mathbb{C}^n$. В дополнение требуется выполнение условия $||X(W)||_2^2 \leq nP$, $\forall W \in [M]$, имеющего смысл естественного ограничения на передаваемую мощность.

В связи с тем, что используется общая кодовая книга, идентификация пользователей невозможна и от декодера требуется лишь вернуть множество $\mathcal{L}(Y) = \{W_1, W_2, \ldots, W_{K_a}\}$ переданных сообщений с точностью до перестановки. Таким образом, мы разделяем задачи идентификации и передачи данных. Вероятность ошибки на пользователя (PUPE) определяется следующим образом

$$P_e = \frac{1}{K_a} \sum_{i=1}^{K_a} \Pr[W_i \notin \mathcal{L}(Y)].$$

В данном разделе мы рассматриваем канал (5). Средняя энергия, затрачиваемая на передачу одного информационного бита, вычисляется следующим образом $E_b/N_0 = nP/k$. Наша главная задача состоит в минимизации E_b/N_0 при условии $P_e \leq \varepsilon$.

Мы используем протокол T-кратная слотированная АЛОХА. Идея протокола заключается в разрешении коллизий кратности до T, где T – это некоторый заранее выбранный параметр. Пусть $T, n_1 \in \mathbb{N}$, причем $T < K_a$ и $n_1 < n$. Кадр длины n делится на $L = n/n_1 \in \mathbb{N}$ слотов длины n_1. Общая кодовая книга, используемая пользователями, имеет длину n_1, что дает нам возможность использовать большую мощность передачи, а именно энергию $nP/n_1 = LP$ на один отсчет. Каждый пользователь случайно, равновероятно и независимо от

[40] *Polyanskiy Y.* A perspective on massive random-access // Information Theory (ISIT), 2017 IEEE International Symposium on. IEEE. 2017. P. 2523–2527.

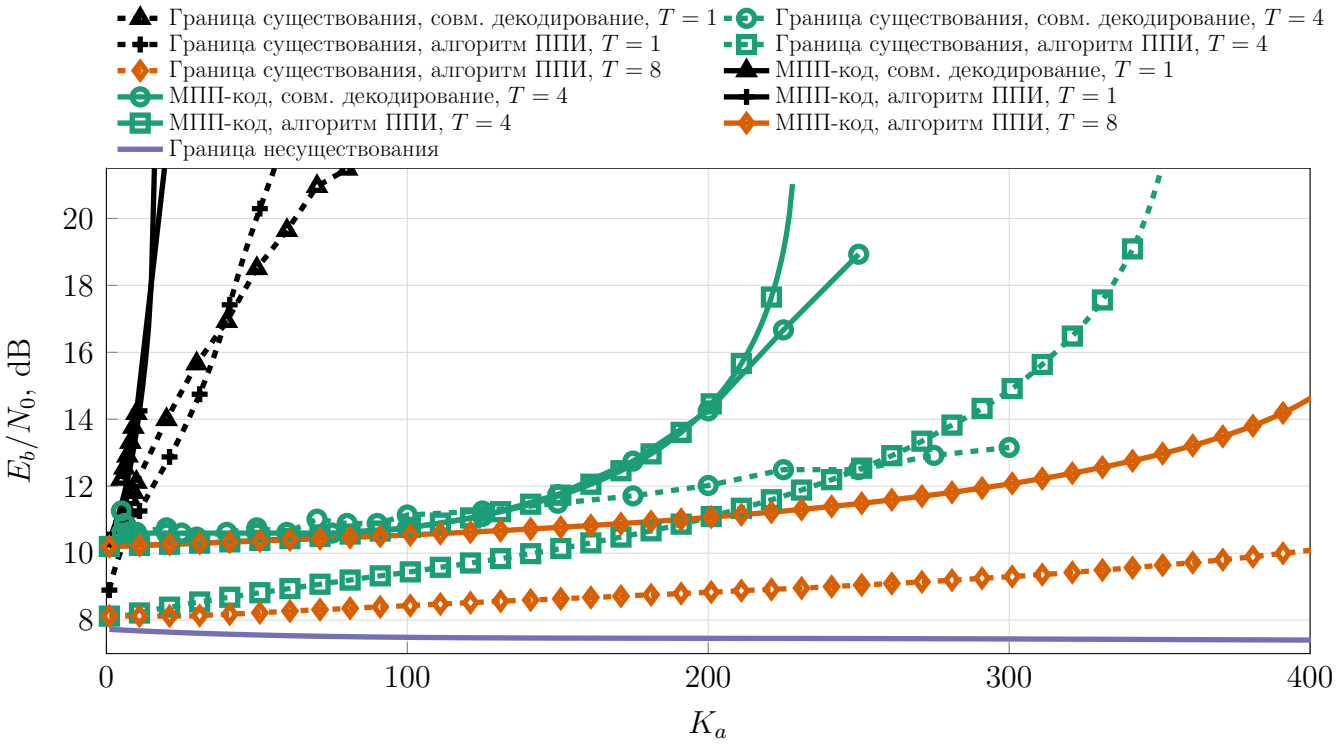

Рис. 12: Зависимости минимального E_b/N_0 от K_a (границы и практические схемы) при $\varepsilon = 0.1$, $n = 30000$, $k = 100$ для разных значений T.

остальных пользователей выбирает один из L слотов, в котором передает свое кодовое слово. Для разрешения коллизий используются схемы из раздела 4.4.3.

На рис. 12 представлены полученные нами зависимости минимальной энергии на бит, необходимой для достижения вероятности ошибки $\epsilon = 0.1$ как функции K_a. Используемые параметры таковы: длина кадра $n = 30000$ отсчетов, а длина сообщения $k = 100$ бит. Начнем с результатов для случая совместного итеративного декодирования пользователей в слоте. Мы видим, что граница существования и результаты практической схемы очень близки и практически совпадают при $K_a \leq 150$. Теперь перейдем к практической схеме на основе алгоритма ППИ. Отметим, что результаты для практической схемы на основе алгоритма ППИ для $T = 4$ хуже аналогичных результатов для алгоритма совместного итеративного декодирования. Но в то же самое время эта схема значительно проще и есть возможность вычислить результаты для $T = 8$, которые существенно превосходят все остальные результаты. Также отметим, что результаты для практической схемы достаточно далеки от границы существования особенно при больших значениях K_a. Это связано с предположением об идеальном устранении интерференции, сделанным в границе. Результаты четвертой главы опубликованы в работах [4–8; 13; 16; 21; 26–30; 32; 33].

В пятой главе исследуются методы кодирования для систем распределенного хранения данных. Заметим, что наиболее частым видом ошибок в таких системах является выход из строя именно одного диска, поэтому возникает за-

дача построения кодов со свойством локального восстановления (ЛВ-кодов).

Пусть $[n] = \{1, 2, \ldots, n\}$. Будем говорить, что код $\mathcal{C} \subset \mathrm{GF}(q)^n$ имеет локальность r, если каждый символ кодового слова $c \in \mathcal{C}$ может быть восстановлен с использованием подмножества из r других символов c. Иными словами, это означает, что для каждой координаты $i \in [n]$ кодового слова существует подмножество координат $\mathcal{R}_i \subset [n] \backslash i, |\mathcal{R}_i| \leq r$, такое что ограничение кода $\mathcal{C}$ на подмножество $\mathcal{R}_i$ позволяет найти значение c_i. Подмножество $\mathcal{R}_i$ будем называть *восстанавливающим множеством* для символа c_i.

Обобщая предыдущее определение, потребуем, чтобы каждый символ можно было восстановить с использованием t непересекающихся восстанавливающих множеств размера r. Более формально, обозначим через $\mathcal{C}_I$ ограничение (проекцию) кода $\mathcal{C}$ на подмножество координат $I \subset [n]$. Для каждого $a \in \mathrm{GF}(q)$ введем обозначение $\mathcal{C}(i, a) = \{c \in \mathcal{C} : c_i = a\},\ i \in [n]$.

Определение 2. *Код $\mathcal{C}$ называется (r, t) ЛВ-кодом, если для любого $i \in [n]$ существуют t попарно непересекающихся восстанавливающих множеств $\mathcal{R}_i^1, \ldots, \mathcal{R}_i^t \subset [n] \backslash i$, таких что для всех $j = 1, \ldots, t$ и любой пары символов $a, a' \in GF(q), a \neq a'$ выполнено следующее условие*

$$\mathcal{C}(i, a)_{\mathcal{R}_i^j} \cap \mathcal{C}(i, a')_{\mathcal{R}_i^j} = \emptyset.$$

Рассмотрим обобщение (r, t) ЛВ-кодов, в котором восстанавливающие множества могут пересекаться не более, чем в x координатах. Дадим формальное определение

Определение 3. *Код $\mathcal{C}$ называется (r, t, x) ЛВ-кодом, если для каждого $i \in [n]$ найдутся t подмножеств $\mathcal{R}_i^1, \ldots, \mathcal{R}_i^t \subset [n] \setminus \{i\}$, таких что выполняются следующие условия*

1. *для любой пары индексов $l, l' \in [t]$, $l \neq l'$*

$$|\mathcal{R}_i^l \cap \mathcal{R}_i^{l'}| \leq x;$$

2. *для всех $j = 1, \ldots, t$ и любой пары символов $a, a' \in GF(q), a \neq a'$*

$$\mathcal{C}(i, a)_{\mathcal{R}_i^j} \cap \mathcal{C}(i, a')_{\mathcal{R}_i^j} = \emptyset.$$

В *разделе 5.2* приведена верхняя граница для скорости для (r, t) ЛВ-кодов.
Теорема 5.1. ([10]) *Пусть $\mathcal{C}$ – это (r, t) ЛВ-код длины n и размерности k, тогда для скорости кода $\mathcal{C}$ выполняется соотношение*

$$\frac{k}{n} \leq \frac{1}{\prod_{j=1}^{t}(1 + \frac{1}{jr})}.$$

В *разделе 5.3* приведена верхняя граница для минимального расстояния для (r,t) ЛВ-кодов.

Теорема 5.3. ([12]) *Пусть $t \geq 2$ и пусть $\mathcal{C}$ – это линейный $[n,k,d]$ (r,t) ЛВ-код над полем $GF(q)$. Для параметров этого кода выполняются следующие неравенства*

$$k \leq \min_{sr+1 \leq n-d} (1 + (r-1)s + k^*(q, n-1-sr, d)$$

и

$$d \leq \min_{1+(r-1)s<k} d^*(n-1-sr, k-1-(r-1)s).$$

Следствие 5.2. *Асимптотическая форма новой границы выглядит следующим образом*

$$R \leq \frac{r-1}{r}(1-\delta) - o(1).$$

В *разделе 5.4* приведены нижние границы для минимального расстояния для (r,t) ЛВ-кодов. Начнем с конструкции на основе графов-расширителей. Пусть $G = (V \cup C, E)$ – это двудольный граф со следующими свойствами: (a) $|V| = n$ и $\deg v = t$ для $v \in V$; (b) $|C| = \frac{nt}{r+1}$ и $\deg c = r+1$ для $c \in C$; (c) G является $(t, r+1, \alpha, t\gamma)$ расширителем; (d) $\mathrm{girth}(G) > 4$. Построим матрицу $\mathbf{H}_E = [h_{j,i}]$, $1 \leq j \leq m$, $1 \leq i \leq n$, над полем $\mathrm{GF}(q)$. Столбцы матрицы $\mathbf{H}_E$ поставим в соответствие вершинам из доли V, а строки – вершинам из доли C. Элемент $h_{j,i}$ является ненулевым тогда и только тогда, когда вершины v_i и c_j соединены ребром. Ненулевые элементы выбираются равновероятно и независимо из множества $\mathrm{GF}(q)\backslash\{0\}$. Через $\mathcal{C}_E$ обозначим код длины n над полем $\mathrm{GF}(q)$, заданный проверочной матрицей $\mathbf{H}_E$.

Рассмотрим каскадный код $\mathcal{C}_G \diamondsuit \mathcal{C}_E$ над полем $\mathbb{F}_{q^m}$, построенный следующим образом. Сначала $k_G = k$ информационных символов кодируются с использованием $[k_G, n_G, d_G = n_G - k_G + 1]$ кода Габидулина. Затем полученное слово кода Габидулина[41] кодируется $[n = \frac{r+1}{r+1-t} n_G, n_G]$ кодом $\mathcal{C}_E$.

Теорема 5.3. ([12]) *Обозначим относительное кодовое расстояние кода $\mathcal{C}_G \diamondsuit \mathcal{C}_E$ через δ. Для достаточно больших n и q выполняется следующее неравенство для скорости R кода $\mathcal{C}_G \diamondsuit \mathcal{C}_E$*

$$R \geq 1 - \frac{t}{r+1} - \max\{\delta(1-t\gamma), 0\} - o(1),$$

где $\gamma = \gamma(\delta, t, r+1)$.

Теперь рассмотрим каскадную конструкцию. Воспользуемся предложенной А. Вангом, З. Джангом и М. Лю конструкцией (r,t) ЛВ-кодов[42] со следующими параметрами: $n = \binom{r+t}{t}$, $R = \frac{r}{r+t}$ и $d = t+1$. Далее мы будем называть эти

[41] *Gabidulin E. M.* Theory of Codes with Maximum Rank Distance // Probl. Inf. Transm. 1985. Vol. 21, no. 1. P. 1–12.

[42] *Wang A., Zhang Z., Liu M.* Achieving Arbitrary Locality and Availability in Binary Codes // Proceedings IEEE International Symposium on Information Theory (ISIT). 06/2015. P. 1866–1870.

коды WZL-кодами. Закодируем информационные символы за два шага. Сначала k информационных символов из поля $\mathbb{F}_{2^m}$ кодируются кодом Габидулина. Полученное кодовое слово длины n_G разбивается на блоки длины k_I, и каждый из блоков кодируется с помощью двоичного $[n_I, k_I]$ WZL-кода. Далее мы предполагаем, что $k_I | n_G$.

Нижняя граница для каскадной конструкции сформулирована в виде Теоремы 5.4. Здесь же мы приведем только ее асимптотическую форму

Следствие 5.3. *Асимптотическая форма границы выглядит следующим образом*

$$R \geq \frac{r}{r+t}(1-\delta) - o(1).$$

В *разделе 5.5* приведена верхняя граница для скорости для (r,t,x) ЛВ-кодов. Пусть $j \in [t]$ и $s = \min\{j, \lfloor r/x \rfloor + 1\}$, тогда $\frac{(2r-(s-1)x)}{2} s = \underline{N}(r,j,x) \leq \left| \bigcup_{l=1}^{j} \mathcal{R}_i^l \right| \leq \overline{N}(r,j,x) = jr$. Введем следующую функцию

$$f(r,t,x) = \sum_{j=1, j=1 \bmod 2}^{t} \binom{t}{j} \frac{1}{\overline{N}(r,j,x)+1} - \sum_{j=1, j=0 \bmod 2}^{t} \binom{t}{j} \frac{1}{\underline{N}(r,j,x)+1}.$$

Теорема 5.5. ([12]) *Для скорости (r,t,x) ЛВ-кода $\mathcal{C}$ справедлива следующая граница*

$$R(\mathcal{C}) \leq R^*(r,t,x) = 1 - f(r,t,x).$$

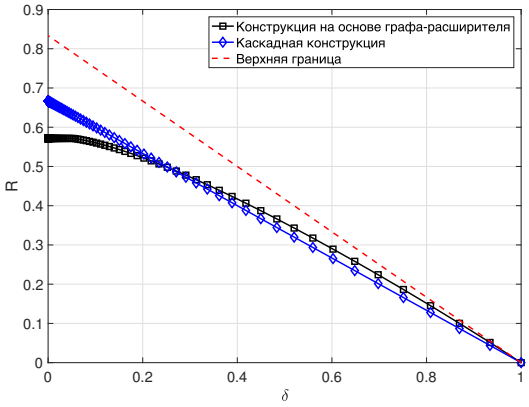

Рис. 13: $t = 3$, $r = 6$

В *разделе 5.6* приведена нижняя граница для скорости для (r,t,x) ЛВ-кодов. Для этого мы предлагаем довольно простую конструкцию. Построим проверочную матрицу линейного (r,t,x) ЛВ-кода следующим образом. Начнем с проверочной матрицы $(\tilde{r}, \tilde{t})$ WZL-кода. Обозначим эту матрицу $\mathbf{H}_{\text{WZL}}$. Матрица $\mathbf{H}$ (r,t,x) ЛВ-кода строится следующим образом

$$\mathbf{H} = \mathbf{H}_{\text{WZL}} \otimes \underbrace{[11\ldots1]}_{x+1} \tag{12}$$

где $\otimes$ обозначает произведение Кронекера.

Скорость полученного кода может быть вычислена следующим образом

$$R = \frac{r + (t-1)x}{r + t + (t-1)x}.$$

Таблица 3: Сравнение верхние и нижних границ для скорости (r, t, x) ЛВ-кодов. В скобках указан объем служебной информации.

(r, t)	$x = 0$ (WZL)	$R^*(r, t)$	$x = 1$	$R^*(r, t, x = 1)$
(3, 2)	0.6000 (66.7 %)	0.6000 (66.7 %)	0.6667 (49.9 %)	0.6667 (49.9 %)
(5, 2)	0.7143 (39.9 %)	0.7143 (39.9 %)	0.7500 (33.3 %)	0.7667 (30.4 %)
(7, 2)	0.7778 (28.6 %)	0.7778 (28.6 %)	0.8000 (25 %)	0.8214 (21.7 %)
(3, 3)	0.5000 (100 %)	0.5548 (80.2 %)	0.6250 (60 %)	0.6500 (53.8 %)
(5, 3)	0.6250 (60 %)	0.6705 (49.1 %)	0.7000 (42.9 %)	0.7375 (35.6 %)
(7, 3)	0.7000 (42.9 %)	0.7373 (35.6 %)	0.7500 (33.3 %)	0.7938 (25.9 %)

В *разделе 5.7* приведены численные результаты. Сравнение верхних и нижних границ для различных (r, t) ЛВ-кодов приведено на рис. 13. В области высоких скоростей каскадная конструкция лучше конструкции на основе графов-расширителей. В области низких скоростей ситуация противоположная. В таблице 3 представлено сравнение полученной нами нижней границы ($x = 1$) и скорости WZL-кода с теми же значениями r и t. Для полноты картины также добавлены верхние границы. Мы видим, что для $r = 3$, $t = 2$ и $x = 1$ нижняя граница точна и она лучше верхней границы для случая $r = 3$, $t = 2$ и $x = 0$. Результаты пятой главы опубликованы в работах [10; 12; 14; 20; 22; 23].

Основные результаты:

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

2. Предложен итеративный мажоритарный алгоритм декодирования МПП-кодов над полем GF(q) с жестким решением, имеющий малую сложность реализации. Предложена многопороговая модификация данного алгоритма. Проведено теоретическое исследование предложенных алгоритмов и выведены нижние асимптотические оценки на радиусы декодирования, реализуемые данными алгоритмами.

3. Предложен алгоритм построения проверочных матриц квазициклических МПП-кодов над полем GF(q).

4. Предложен новый алгоритм декодирования МПП-кодов на основе глубоких нейронных сетей. Найдена архитектура сети, позволяющая производить обучение только на нулевом кодовом слове. Разреженные связи и общие на циркулянт веса позволяют значительно сократить время обучения.

5. Получены асимптотические верхние и нижние оценки относительной (на один подканал) пропускной способности для Б-канала при координированной и некоординированной передаче. Проведено сравнение с оценками относительной пропускной способности для А-канала.

6. Предложена схема кодирования для А-канала, позволяющая обеспечить асимптотическую относительную суммарную скорость передачи сколь угодно близкую к пропускной способности.

7. Предложена схема кодирования на основе МПП-кодов и совместного итеративного алгоритма декодирования для суммирующего канала с АБГШ. Предложен метод построения МПП-кодов. С помощью имитационного моделирования показано, что результирующая схема лучше схем, представленных в литературе, и близка к неасимптотической границе случайного кодирования для данного канала.

8. Установлены неасимптотические верхние и нижние границы на вероятность ошибки для многопользовательского канала Рэлея.

9. Предложена схема кодирования на основе МПП-кодов для многопользовательского канала Рэлея и алгоритм совместного итеративного декодирования. С помощью имитационного моделирования показано, что граница существования и результаты практической схемы очень близки и практически совпадают при $K_a \leq 150$.

10. Предложен алгоритм последовательного погашения интерференции (ППИ), имеющий значительно меньшую вычислительную сложность по сравнению с алгоритмом совместного итеративного декодирования. В то же самое время с помощью имитационного моделирования показано, что алгоритм ППИ имеет практически такие же корректирующие свойства.

11. С помощью имитационного моделирования продемонстрирована эффективность предложенных схем на основе МПП-кодов в сочетании с протоколом T-кратная слотированная АЛОХА (СА) в сценарии массового случайного доступа. Разработанная схема требует значительно меньшей энергии, затрачиваемой на передачу одного информационного бита (E_b/N_0) при фиксированной вероятности ошибки, в сравнении с классическим протоколом СА ($T = 1$).

12. Получены новые нижние и верхние границы на скорость и минимальное кодовое расстояние ЛВ-кодов с несколькими непересекающимися восстанавливающими множествами. Показано, что новые границы улучшают известные.

13. Предложено обобщение ЛВ-кодов с несколькими непересекающимися восстанавливающими множествами, в котором восстанавливающие множества могут пересекаться по небольшому числу позиций. Получены границы для скорости таких кодов. Показано, что такие коды имеют значительно большую скорость и удовлетворяют требованию сбалансированной нагрузки на диски.

Основные публикации по теме диссертации

1. *Фролов А. А.*, *Зяблов В. В.* Асимптотическая оценка доли ошибок, исправляемых q-ичными МПП-кодами // Пробл. передачи информ. — 2010. — т. 46, № 2. — с. 47—65.
2. *Зяблов В. В.*, *Рыбин П. С.*, *Фролов А. А.* Алгоритм декодирования с вводом стираний для МПП-кодов, построенных над полем GF(q) // Информационно-Управляющие Системы. — 2011. — т. 50, № 1. — с. 62—68.
3. *Фролов А. А.*, *Зяблов В. В.* Границы минимального кодового расстояния для недвоичных кодов на двудольных графах // Пробл. передачи информ. — 2011. — т. 47, № 4. — с. 27—42.
4. *Zyablov V.*, *Frolov A.* A signal-code construction for a multiple-access system using a vector channel with an additive white Gaussian noise // J. Commun. Technol. Electron. — 2012. — Vol. 57. — P. 953–957.
5. *Осипов Д. С.*, *Фролов А. А.*, *Зяблов В. В.* Система множественного доступа для векторного дизъюнктивного канала // Пробл. передачи информ. — 2012. — т. 48, № 3. — с. 52—59.
6. *Осипов Д. С.*, *Фролов А. А.*, *Зяблов В. В.* О пропускной способности для пользователя системы множественного доступа в векторном дизъюнктивном канале при наличии ошибок // Пробл. передачи информ. — 2013. — т. 49, № 4. — с. 13—27.
7. *Фролов А. А.*, *Зяблов В. В.* О пропускной способности многопользовательского векторного суммирующего канала // Пробл. передачи информ. — 2014. — т. 50, № 2. — с. 20—30.
8. *Frolov A.*, *Zyablov V.* A coding technique for Q-frequency S-user gaussian channel // J. Commun. Technol. Electron. — 2014. — Vol. 59. — P. 1483–1488.
9. *Фролов А. А.* Верхняя граница минимального кодового расстояния для МПП-кодов над полем GF(q) на основе подсчета числа синдромов // Пробл. передачи информ. — 2016. — т. 52, № 1. — с. 8—15.
10. *Tamo I.*, *Barg A.*, *Frolov A.* Bounds on the Parameters of Locally Recoverable Codes // IEEE Transactions on Information Theory. — 2016. — Vol. 62, no. 6. — P. 3070–3083.
11. *Frolov A.*, *Zyablov V.* On the multiple threshold decoding of LDPC codes over GF(q) // Advances in Mathematics of Communications. — 2017. — Vol. 11, no. 1. — P. 123–137.
12. *Kruglik S.*, *Nazirkhanova K.*, *Frolov A.* New Bounds and Generalizations of Locally Recoverable Codes With Availability // IEEE Transactions on Information Theory. — 2019. — Vol. 65, no. 7. — P. 4156–4166.

13. Energy Efficient Coded Random Access for the Wireless Uplink / S. S. Kowshik, K. Andreev, A. Frolov, Y. Polyanskiy // IEEE Transactions on Communications. — 2020. — Vol. 68, no. 8. — P. 4694–4708.

14. *Kruglik S.*, *Frolov A.* An Information-Theoretic Approach for Reliable Distributed Storage // J. Commun. Technol. Electron. — 2020. — Vol. 65. — P. 1505–1516.

15. *Frolov A.*, *Zyablov V.* Upper and lower bounds on the minimum distance of expander codes // 2011 IEEE International Symposium on Information Theory Proceedings. — 2011. — P. 1397–1401.

16. On a multiple-access in a vector disjunctive channel / A. Frolov, V. Zyablov, V. Sidorenko, R. Fischer // 2013 IEEE International Symposium on Information Theory. — 2013. — P. 211–215.

17. *Frolov A.*, *Zyablov V.* A new coding method for a multiple-access system with a large number of active users // 2015 IEEE Information Theory Workshop (ITW). — 2015. — P. 1–5.

18. *Frolov A.*, *Zyablov V.* On the multiple threshold decoding of LDPC codes over GF(q) // 2015 IEEE International Symposium on Information Theory (ISIT). — 2015. — P. 2673–2677.

19. *Frolov A.* An upper bound on the minimum distance of LDPC codes over GF(q) // 2015 IEEE International Symposium on Information Theory (ISIT). — 2015. — P. 2885–2888.

20. *Kruglik S.*, *Frolov A.* Bounds and constructions of codes with all-symbol locality and availability // 2017 IEEE International Symposium on Information Theory (ISIT). — 2017. — P. 1023–1027.

21. On LDPC Code Based Massive Random-Access Scheme for the Gaussian Multiple Access Channel / A. Glebov, L. Medova, P. Rybin, A. Frolov // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. — Springer International Publishing, 2018. — P. 162–171.

22. On one generalization of LRC codes with availability / S. Kruglik, M. Dudina, V. Potapova, A. Frolov // 2017 IEEE Information Theory Workshop (ITW). — 2017. — P. 26–30.

23. *Kruglik S.*, *Nazirkhanova K.*, *Frolov A.* On Distance Properties of (r, t, x)-LRC Codes // 2018 IEEE International Symposium on Information Theory (ISIT). — 2018. — P. 1336–1339.

24. *Kruglik S.*, *Potapova V.*, *Frolov A.* A Method for Constructing Parity-Check Matrices of Quasi-Cyclic LDPC Codes Over GF(q) // J. Commun. Technol. Electron. — 2018. — Vol. 63. — P. 1524–1529.

25. *Rybin P.*, *Frolov A.* On the Decoding Radius Realized by Low-Complexity Decoded Non-Binary Irregular LDPC Codes // 2018 International Symposium on Information Theory and Its Applications (ISITA). — 2018. — P. 384–388.

26. Achievability Bounds for T-Fold Irregular Repetition Slotted ALOHA Scheme in the Gaussian MAC / A. Glebov, N. Matveev, K. Andreev, A. Frolov, A. Turlikov // 2019 IEEE Wireless Communications and Networking Conference (WCNC). — 2019. — P. 1–6.

27. Energy efficient random access for the quasi-static fading MAC / S. S. Kowshik, K. Andreev, A. Frolov, Y. Polyanskiy // 2019 IEEE International Symposium on Information Theory (ISIT). — 2019. — P. 2768–2772.

28. A Polar Code Based Unsourced Random Access for the Gaussian MAC / E. Marshakov, G. Balitskiy, K. Andreev, A. Frolov // 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall). — 2019. — P. 1–5.

29. Low Complexity Energy Efficient Random Access Scheme for the Asynchronous Fading MAC / K. Andreev, S. S. Kowshik, A. Frolov, Y. Polyanskiy // 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall). — 2019. — P. 1–5.

30. Efficient Concatenated Same Codebook Construction for the Random Access Gaussian MAC / D. Ustinova, A. Glebov, P. Rybin, A. Frolov // 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall). — 2019. — P. 1–5.

31. *Ustinova D.*, *Rybin P.*, *Frolov A.* On the Analysis of T-Fold Coded Slotted ALOHA for a Fixed Error Probability // 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). — 2019. — P. 1–5.

32. Short-Packet Low-Power Coded Access for Massive MAC / S. S. Kowshik, K. Andreev, A. Frolov, Y. Polyanskiy // 2019 53rd Asilomar Conference on Signals, Systems, and Computers. — 2019. — P. 827–832.

33. *Andreev K.*, *Marshakov E.*, *Frolov A.* A Polar Code Based TIN-SIC Scheme for the Unsourced Random Access in the Quasi-Static Fading MAC // 2020 IEEE International Symposium on Information Theory (ISIT). — 2020. — P. 3019–3024.