На правах рукописи

Лебедев Владимир Сергеевич

Коды для каналов множественного доступа и задачи комбинаторного поиска

Специальность 05.13.17 — Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико–математических наук

Москва — 2021

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

Официальные оппоненты:

Дьячков Аркадий Георгиевич
доктор физико-математических наук, профессор кафедры теории вероятностей механико-математического факультета ФГБОУ ВО "Московский государственный университет имени М.В. Ломоносова".

Кротов Денис Станиславович
доктор физико-математических наук, профессор, главный научный сотрудник института математики им. С.Л. Соболева Сибирского отделения Российской академии наук, г. Новосибирск.

Леонтьев Владимир Константинович
доктор физико-математических наук, главный научный сотрудник Федерального исследовательского центра им. Дородницына ФИЦ "Информатика и управление" РАН (ВЦ ФИЦ ИУ РАН), г. Москва.

Ведущая организация:
Национальный исследовательский университет "Высшая школа экономики".

Защита состоится 18 октября 2021 г. в 11 час. 00 мин.

на заседании диссертационного совета Д 002.077.05 на базе ИППИ РАН Большой Каретный пер., д. 19, стр. 1, Москва, ГСП-4, 127994

С диссертацией можно ознакомиться в библиотеке ИППИ РАН и на сайте www.iitp.ru

Автореферат разослан «__»_____ 2021 г.

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

Общая характеристика работы

Актуальность темы

Разработка методов обеспечения высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации часто приводит к математическим моделям обработки информации, которые описываются каналом множественного доступа (КМД). Примерами таких задач являются, например, задачи криптографии по минимизации числа секретных ключей при фиксированном числе пользователей или, что тоже самое, по максимизации числа пользователей при фиксированном числе ключей или задачи группового поиска (планирования экспериментов). В зависимости от типа исследуемой задачи, необходимо получать соответствующие свойства КМД, описывающего рассматриваемую задачу.

Свойства КМД активно изучаются на протяжении многих десятилетий. Отметим исследования Бассалыго Л.А., Бурнашева М.В., Дьячкова А.Г., Зиновьева В.А., Зяблова В.В., Кабатянского Г.А., Леонтьева В.К., Пинскера М.С., Прелова В.В., Цыбакова Б.С., которые наиболее близки к тематике рассматриваемых в диссертации проблем. Вместе с тем, имеется и много нерешенных задач, актуальных для теории информации, которые описываются в терминах КМД и являются предметом рассмотрения настоящей диссертации. Напомним, что математическая КМД представляет из себя дискретный канал, имеющий d входов и один выход. Через КМД посимвольно передаются последовательности q-ичных символов из алфавита $\{0, 1, \ldots, q-1\}$ длины n, представляющие из себя закодированные сообщения. Набор из M таких сообщений мы будем называть кодом, если для любого набора из d сообщений, которые поступают на вход канала, их можно восстановить по последовательности длины n на выходе. Задача состоит в том, чтобы для фиксированного количества сообщений минимизировать длину n, или (что эквивалентно) при фиксированном n максимизировать число сообщений M.

Если мы рассмотрим двоичный канал, в котором возможны ошиб-

ки, но $d = 1$, то получим одну из задач обеспечения помехоустойчивости информационных коммуникаций для целей передачи информации. Данную задачу с безошибочной обратной связью называют задачей Улама, или задачей Реньи-Улама, и она имеет много важных приложений.

Впервые эту задачу сформулировал венгерский математик Альфред Реньи[1]. Большую роль в исследовании этой задачи сыграли результаты, полученные Берлекампом[2] и Зигангировым К.Ш..

Возникает вопрос, что будет при $q > 2$.

Для случая $d > 1$ активно изучались различные каналы, но уже без ошибок при передаче. Отметим исследования Алсведе Р., Дьячкова А.Г., Малютова М.Б., Сагаловича Ю.Л., Цитовича И.И.

Одной из самых распространенных является модель дизъюнктивного канала множественного доступа.

Благодаря значительному разнообразию приложений (групповое тестирование, поиск файлов в системах хранения, совокупные цифровые подписи и др.), коды для дизъюнктивного КМД достаточно хорошо изучены. Вместе с тем, многие задачи до конца не решены или позволяют рассматривать их обобщения, которые интересны с точки зрения КМД.

Также очень популярна задача для суммирующего КМД. В теории информации эта задача известна как однозначно декодируемые коды для суммирующего КМД.

В случае, когда нет ограничения на число активных пользователей, Линдстрем [3] получил асимптотически точный ответ о длине кода для двоичного случая. В 1966 году Кантор и Милс другим способом доказали этот же результат. Возникает вопрос изучения кодов, связанных с суммирующим каналом, для случая $q > 2$.

Следовательно, актуальной является задача разработки новых методов и алгоритмов кодирования информации в КМД, позволяющих на основании комбинаторного подхода получать более точные оцен-

[1]Renyi A., On a problem of information theory // MTA Mat. Kut. Int. Kozl. 1961. 68. P. 505-516.

[2]Berlekamp C.R., Block coding with noiseless feedback // Doctoral dissertation, MIT, 1964.

[3]Lindstrom B., On a combinatorial detection problem,I// Publ.Math. Inst. Hung. Acad.Sci, 1964. V.9. P. 195-207.

ки характеристик некоторых кодов, используемых для передачи и защиты информации.

Цель работы

Целью диссертационной работы является разработка методов получения более точных оценок характеристик некоторых кодов, используемых для передачи и защиты информации, в том числе обслуживающих некоторые КМД. Для этого необходимо:
—для задачи Улама получить новый подход с точки зрения КМД, позволяющий обобщить результаты Берлекампа на q-ичный случай $(q > 2)$;
—для дизъюнктивной модели ввести композиционное расстояние, чтобы применить подход из теории кодирования и КМД для получения более точных верхних границ для скорости кодов, свободных от (w, r)-перекрытий;
—для случая $d = 2$ в дизъюнктивной модели КМД построить алгоритм кодирования, дающий оптимальную константу при главном члене асимптотического разложения для числа пользователей;
—для суммирующего канала исследовать задачу, обобщающую двоичный суммирующий канал на q-ичный случай $(q > 2)$.

Основные положения, выносимые на защиту.

1. Для передачи информации по q-ичному каналу с безошибочной обратной связью предложен новый подход к исправлению ошибок, позволяющий обобщить результаты Берлекампа, полученные для двоичного канала.

2. Границы для композиционного расстояния, полученные автором, позволяют для дизъюнктивной модели доказать оптимальность некоторых кодов, свободных от (w, r)-перекрытий, и улучшить верхнюю границу на скорость таких кодов.

3. Получен алгоритм поиска двух дефектных элементов, позволяющий получить оптимальную константу при главном члене

для общего числа элементов.

4. Для суммирующего канала обобщен результат Линдстрема на случай $q = 3$ и $q = 4$.

Научная новизна

работы состоит в том, что в ней впервые предложен комбинаторный подход рассмотрения задач поиска с точки зрения методов теории кодирования, позволивший получить новые научные результаты.

Предложен новый метод исправления ошибок для q-ичного канала с безошибочной обратной связью.

Впервые введено понятие композиционного расстояния и получена граница на скорость кодов с таким композиционным расстоянием.

Предложен новый алгоритм поиска двух дефектных элементов, позволяющий получить оптимальную константу при главном члене для общего числа элементов.

Для суммирующего канала обобщен результат Линдстрема на случай $q = 3$ и $q = 4$. (Результат для произвольного q недавно было доказан в работе [4]). .

Основные методы исследования

В работе используются методы комбинаторной теории кодирования.

Теоретическая и практическая ценность работы

Работа носит теоретический характер. Результаты работы могут применяться в дальнейших исследованиях в области теории кодирования, криптографии и комбинаторного поиска. Также результаты работы могут быть использованы в разных практических областях — в практической криптографии, медицине, биологии и др.

[4] Jiang, Z., Polyanskii N., On the metric dimension of Cartesian powers of a graph. // Journal of Combinatorial Theory, Series A, 2019. 165. P. 1-14.

Апробация диссертации

Результаты диссертации неоднократно докладывались автором на следующих научно-исследовательских семинарах:

1. по теории кодирования под рук. Л.А. Бассалыго в ИППИ РАН в 2002–2021 гг.;
2. по дискретной математике под рук. С.П. Тарасова в МИАН в 2010 г.;
3. по дискретной математике под рук. Ш.Кима (Пхоханский университет науки и технологии) в 2000-2003 г.;
4. по дискретной математике под рук. Р. Алсведе (Университет Билефельда) в 2001–2010 г.;
5. по дискретной математике под рук. Крамера (Мюнхенский технический университет) в 2017-2018 г.

Результаты диссертации докладывались автором на следующих международных конференциях.

1. Eighth International Workshop on Algebraic and Combinatorial Coding Theory, September 8-14. 2002, Tsarskoe Selo (Russia).
2. Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory. Kranevo, Bulgaria. June 19-25, 2004.
3. Tenth International Workshop on Algebraic and Combinatorial Coding Theory, September 3-9. 2006, Zvenigorod (Russia).
4. Eleventh Int. Workshop on Algebraic and Combinatorial Coding Theory. Pamporovo, Bulgaria. June 16-22, 2008.
5. Twelfth International Workshop on Algebraic and Combinatorial Coding Theory, September 5-11. 2010, Novosibirsk (Russia).
6. Thirteenth Int. Workshop on Algebraic and Combinatorial Coding Theory. Pomorie, Bulgaria. June 15-21, 2012.

7. Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory, September 7-13. 2014, Svetlogorsk (Russia).

8. Ninth International Workshop on Coding and Cryptography, Paris, France, 2015.

9. 15th International Workshop on Algebraic and Combinatorial Coding Theory, Albena, Bulgaria, 2016.

10. Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT 2018, Sep 2018, Svetlogorsk (Russia).

11. IEEE International Symposium on Information Theory (ISIT), July 7-12, Paris, 2019.

12. Algebraic and Combinatorial Coding Theory (ACCT), IEEE, Bulgaria, 2020.

13. IEEE International Symposium on Information Theory (ISIT), June 21-26, Los-Angeles, 2020.

Личный вклад автора

Основные результаты диссертации получены автором лично или при непосредственном его участии.

Структура и объем диссертации

Диссертация состоит из введения, четырех глав, заключения и списка литературы, который включает 175 наименований. Объем диссертации составляет 201 страницу.

Краткое содержание диссертации

Введение содержит обоснование актуальности диссертационной работы, формулировку целей и задач работы, основные положения,

выносимые на защиту. Определены основные объекты исследования, представлен краткий исторический обзор результатов, а также приведено краткое содержание данной диссертации.

В начале введения рассматриваются несколько популярных задач, которые имеют различные приложения.

Первая задача может быть сформулирована следующим образом. Сколько надо задать вопросов с ответами "да–нет", чтобы найти некоторое загаданное целое число от 1 до M, если среди ответов может быть не более t неправильных?

Если все вопросы задаются одновременно, а потом мы получаем одновременно все ответы, то подобный поиск называется неадаптивным. Если при выборе следующего вопроса мы можем использовать результаты предыдущих, то поиск называется адаптивным. Мы будем интересоваться только адаптивным поиском для данной задачи. (Отметим, что сформулированная задача с неадаптивным поиском эквивалентна классической задаче теории кодирования). Эта задача приобрела популярность после того, как в своей автобиографии "Приключения математика" американский математик Станислав Улам задал подобный вопрос для $M = 10^6$. Для данного значения M, точнее для $M = 2^{20}$, эта задача решена. Для произвольного значения M точный ответ известен только для небольших значений t. Асимптотически точный ответ для двоичного случая был получен в работе[5].

Возникает вопрос, можно ли обобщить известные результаты на случай $q > 2$, когда доля ошибок линейна по сравнению с кодовой длиной.

Вторая задача может быть сформулирована следующим образом. Рассмотрим множество, состоящее из M элементов и содержащее не более, чем d дефектных элементов. Требуется выявить все дефектные элементы на основании наименьшего числа групповых тестов. Каждый тест — это выбор тестируемой группы элементов. В дизъюнктивной модели результат теста положителен, если хоть один де-

[5]Зигангиров К.Ш., О числе исправляемых ошибок при передаче по ДСК с обратной связью // Проблемы передачи информации, 1976. Т. 12. № 2. С. 3-19.

фектный элемент попал в тестируемую группу. Также важна задача, когда результат теста показывает сколько дефектных элементов попало в тестируемую группу.

Для случая одной фальшивой монеты решения подобных задач давно известны. Удивительно, но уже для случая двух фальшивых монет точный ответ для большинства подобных задач до сих пор неизвестен.

Различные авторы исследовали константу при главном члене асимптотического разложения максимального числа элементов, среди которых можно найти 2 дефектных элемента за n тестов, при $n \to \infty$. В работе[6] авторы доказали, что эта константа больше 0.95. Этот результат был улучшен в[7] , где предложенный алгоритм давал оценку 0.983, и, более того, доказывалось существование такого n_0, что константа больше 0.995 для $n \geq n_0$. Возникает вопрос о построении алгоритма, который бы дал константу, равную единице.

Дизъюнктивные коды тесно связаны с задачей нахождения дефектных элементов в дизъюнктивной модели поиска.

Дизъюнктивные s-коды были введены У. Каутсом и Р. Синглетоном в 1964 году в основополагающей статье[8], где были получены первые нетривиальные свойства и некоторые конструкции таких кодов, а также описан ряд прикладных задач, использующих такие коды.

Двоичная матрица $C = \|c_{ij}\|$ размера $n \times M$ называется дизъюнктивным s-кодом, если для любого столбца с номером k и любого подмножества $J \subset [M]$ мощности $|J| = s$, не содержащего в себе k, существует координата $i \in [n]$ такая, что $c_{ik} = 1$ и $c_{ij} = 0$ для всех $j \in J$.

Напомним, что асимптотической скоростью кода называют величину

[6]Chang G.J., Hwang F.K., and Lin S., Group testing with two defectives // Discrete Applied Math. 1982. V. 4. N. 2. P. 97-102.

[7]Chang G.J., Hwang F.K., and Weng J.F., Group testing with two and three defectives // Graph Theory and Its Applications: East and West, ed.Capobianco M.F.,Guan M., Hsu D.F. and Tian T. (The New York Academy of Sciences, New York, 1989), P. 86-96.

[8]Kautz W.H., Singleton R.S., Nonrandom Binary Superimposed Codes// IEEE Trans. Inform. Theory, 1964. V. IT-10. N. 3. P. 363-377.

$$R = \lim_{n\to\infty} \frac{\log_2 M}{n},$$

где M максимальный объем кода длины n.

В случае $s = 2$ в 1982 году П. Эрдеш и др. доказали оценки, из которых следуют наилучшие известные до настоящего времени нижние и верхние границы для скорости кода.

В том же 1982 году А.Г. Дьячков и В.В. Рыков[9] иным методом вывели верхнюю границу, которая в случае $s = 2$ совпадает с границей Эрдеша, а при $s \to \infty$ дает хорошую верхнюю оценку скорости кода.

Нижняя граница скорости $R(s)$ была получена в 1983 году А.Г. Дьячковым и В.В. Рыковым:

$$R(s) \geq \frac{\log_2 e}{es^2}(1 + o(1)) = \frac{0.531...}{s^2}(1 + o(1)), \quad s \to \infty.$$

Определенный интерес представляют собой работы, написанные независимо П. Эрдешом и др. в 1985 году [10] и Ф. Хвангом и В. Сосом в 1987 году[11], где получена оценка

$$R(s) \geq \frac{\log_2 e}{4s^2}(1 + o(1)) = \frac{0.361...}{s^2}(1 + o(1)), \quad s \to \infty.$$

А.Г. Дьячков и др. [12] впоследствии улучшили результат 1983 года, и в 1989 году новым методом доказали нижнюю границу для скорости $R(s)$, из которой при $s = 2$ следует левая часть неравенства Эрдеша, а при $s \to \infty$ асимптотическое неравенство, улучшающее прежние результаты.

---

[9]Дьячков А.Г., Рыков В.В., Границы длины дизъюнктивных кодов // Проблемы передачи информации, 1982. Т. 18. № 3. С. 7-13.

[10]Erdos P., Frankl P., Furedi Z., Families of Finite Sets in Which No Set Is Covered by the Union of r Others // Israel J. Math., 1985. 51. P. 79-89.

[11]Hwang F. K., Sos V. Z., Non adaptive hypergeometric group testing // Studia Sci. Math. Hungarica, 1987. 22. P. 257-263.

[12]Dyachkov A. G., Rykov V. V., Rashad A. M., Superimposed Distance Codes // Problems of Control and Information Theory, 1989. V.18. N.4. P. 237-250.

$$R(s) \geq \frac{1}{s^2 \log_2 e}(1 + o(1)) = \frac{0.693...}{s^2}(1 + o(1)), \quad s \to \infty.$$

В приводимой ниже терминологии это соответствует исследованию $(1, s)$-кодов. Естественное обобщение $(1, s)$-кодов на случай (w, r)-кодов (w и r — натуральные числа) появилось в работе[13], в которой подобные коды рассматривались в связи с проблемами криптографии.

Третья задача, описанная во введении, формулирует одну из подобных проблем. Пусть имеется T пользователей и N секретных ключей. Каждый пользователь имеет свой набор ключей. Группа пользователей может вести обмен информацией, если найдется общий для всей группы секретный ключ. Мы хотим, чтобы для любой группы из w пользователей и группы из r других пользователей нашелся такой ключ, что все пользователи первой группы имеют этот ключ и, тем самым, могут вести обмен информацией, тогда как ни у одного из r пользователей второй группы этого ключа нет. Тем самым, пользователи первой группы могут обмениваться информацией секретно от пользователей второй группы.

Естественно, что нам хотелось бы минимизировать число секретных ключей N при фиксированном числе пользователей или, что тоже самое, максимизировать число пользователей при фиксированном числе ключей.

Двоичная матрица $C = \|c_{ij}\|$ размера $N \times T$ называется кодом, свободным от (w, r)-перекрытий, если для любой пары непересекающихся подмножеств $J_1, J_2 \subset [T]$ мощности $|J_1| = w$ и $|J_2| = r$ существует координата $i \in [N]$ такая, что $c_{ij} = 1$ для всех $j \in J_1$ и $c_{ij} = 0$ для всех $j \in J_2$.

В 2002 году в работе[14] была описана конструкция свободных от перекрытий кодов, построенных на укороченных кодах Рида-Соломона,

[13]Mitchell C.J., Piper F.C., Key storage in secure networks // Discrete Applied Mathematics, 1988. V.21. P. 215-228.

[15]D'yachkov A.D., Macula A., Torney D., Vilenkin P., Families of Finite Sets in which No Intersection of l Sets is Covered by the Union of s Others // Journal Combinatorial Theory Ser. A, 2002. V.99. P. 195-218.

и получена нижняя граница скорости $R(w,r)$ с помощью метода случайного кодирования на ансамбле с независимыми двоичными компонентами кодовых слов.

Верхняя граница для скорости $(2,2)$ кодов была получена Сагаловичем[15] , который использовал идею рассмотрения кода, длина которого является кодовым расстоянием другого кода. Возникает вопрос обобщения этой идеи на случай произвольных (w,r).

Описание других интересных моделей комбинаторного поиска и группового тестирования можно найти в [16] В диссертации рассматриваются эти задачи с точки зрения КМД.

Первая глава диссертации состоит из пяти разделов и посвящена исследованию задачи Реньи-Берлекампа-Улама, обобщенной на q-ичный случай.

Рассмотрим множество, состоящее из M элементов. Мы разбиваем множество $[M]$ на q подмножеств $S_0, S_1, \ldots, S_{q-1}$. Результат теста показывает в какой группе находится загаданное число. Требуется найти, сколько потребуется тестов, чтобы найти это загаданное число от 1 до M, если среди результатов тестов может быть не более t неправильных?

Ставится задача построения алгоритма тестирования, позволяющего обобщить результаты Берлекампа на q-ичный случай.

Пропускная способность канала $C_q(\tau)$ определяется как супремум скорости кода при стремлении к бесконечности длины кода n (число тестов), где $\tau = t/n$ — это доля ошибок в канале.

Предлагается новый метод решения данной задачи, отличный от методов, используемых Берлекампом. Этот метод появился благодаря тому, что задача поиска рассматривается с точки зрения методов теории кодирования и КМД. Основная идея состоит в том, что кодер при возникновении ошибок прекращает передачу информационных символов и занимается исправлением этих ошибок. После того, как

[15]Сагалович Ю.Л., Разделяющие системы // Проблемы передачи информации 1994. Т. 30. № 2. С. 14-35.

[16] *Du D.Z. and Hwang F.K.*, Combinatorial Group Testing and its Applications, 2nd edition, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, Series on Applied Mathematics, 12, 2000.

появившиеся ошибки исправлены, передача информации возобновляется.

Для исправления ошибок используется нулевой символ, который стирает символ, идущий перед ним. Такой алгоритм называется алгоритмом 1-удаления, и он показывает, что для $\frac{1}{q} \leq \tau \leq \frac{1}{2}$ справедливо равенство

$$C_q(\tau) = (1 - 2\tau) \log_q(q - 1).$$

Асимптотически точный ответ для произвольного значения t получить не удалось.

Заметим, что если рассматривать канал передачи, в котором ошибка меняет передаваемый символ не произвольным образом, а, к примеру, увеличивает значение не более, чем на x (по модулю q), то получается асимптотически точный ответ для произвольного значения t. Доказано, что для $1 \leq x \leq q/2 - 1$ справедливо равенство

$$C_q^x(\tau) = 1 - h(\tau) \log_q 2 - \tau \log_q x$$

для $\tau \leq x/(x + 1)$ и

$$C_q^x(\tau) = 1 - \log_q(x + 1)$$

для $\tau > x/(x + 1)$.

Вернемся к классическому случаю передачи по q-ичному каналу. Имеется последовательность значений t, для которых алгоритм, близкий к алгоритму 1-удаления, дает асимптотически точный ответ.

Второй раздел первой главы посвящен описанию алгоритма r-удаления для передачи сообщений для q-ичного канала с обратной связью, в котором может произойти не более t ошибок. Вместо одного нуля для удаления используются r нулей, идущих подряд. Это асимптотически дает прямые на плоскости, выходящие из точек $(1/(r+1), 0)$, и являющиеся касательными к асимптотической границе Хэмминга, если по оси абсцисс откладывать долю ошибок, а по оси ординат асимптотическую скорость кода.

Дадим более формальное описание данного алгоритма. Поставим каждому передаваемому сообщению $m \in [M]$ в соответствие

информационную последовательность $m = (m_1, m_2, \ldots, m_{n-(r+1)t})$, не содержащую блока из r нулей, идущих подряд. Алгоритм построения кодовой последовательности $x_1, x_2, \ldots, x_i$ состоит в том, что кодер посылает в канал либо элемент $x_i = m_{p(i)}$ из последовательности m, либо нулевой элемент, если он находится в состоянии исправления ошибок. После того как будет передана последовательность $m = (m_1, m_2, \ldots, m_{n-(r+1)t})$ (если произошло меньшее, чем t, число ошибок) кодер может передавать любой ненулевой элемент, например 1, для определенности. Для определения состояния кодера, когда он исправляет ошибки, важнейшую роль играет процесс r-удаления. Для последовательности $b_1, b_2, \ldots, b_k$ определим процесс r-удаления следующим образом: ищется подпоследовательность $b_i, b_{i+1}, \ldots, b_{i+r-1}$ с минимальным возможным i так, что

$$b_i = b_{i+1} = \ldots = b_{i+r-1} = 0.$$

После этого из последовательности $b_1, b_2, \ldots, b_k$ получаем последовательность $b_1, b_2, \ldots, b_{i-2}, b_{i+r}, \ldots, b_k$, если $i > 2$, и последовательность $b_{i+r}, \ldots, b_k$, если $i = 1$ или $i = 2$. Далее продолжаем процесс r-удаления для новой полученной последовательности. Таким образом, процесс r-удаления состоит из итераций удалений, описанных выше.

Основная идея алгоритма состоит в том, что кодер передает 0 до тех пор, пока в процессе r-удаления не будут удалятся все ошибочные символы. Также в разделе 2 доказывается описанный выше результат, что алгоритм 1-удаления является асимптотически оптимальным, когда $n \leq tq$.

Теорема 1.[17] *Для* $\frac{1}{q} \leq \tau \leq \frac{1}{2}$ *справедливо равенство*

$$C_q(\tau) = (1 - 2\tau) \log_q(q - 1).$$

В третьем разделе изучаются задачи, связанные с отношением слово-подслово для q-ичных последовательностей. Эти задачи связаны с возможными обобщениями алгоритма r-удаления. При этом в

[17]Нумерация теорем соответствует их нумерации в тексте диссертации

третьем разделе первой главы подсчитывается число последовательностей, содержащих подблок 00 фиксированное число раз, а общие результаты для отношения слово-подслово выделены в отдельный, пятый раздел.

В четвертом разделе предложен обобщенный алгоритм 1-удаления. Рассмотрим описанный выше алгоритм при $r = 1$. Раньше информационная последовательность $(m_1, m_2, \ldots, m_{n-2t})$ не содержала нулей, а $2t$ позиций использовались для исправления ошибок.

В обобщенном алгоритме 1-удаления рассмотрим информационную последовательность $m = (m_1, m_2, \ldots, m_{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil})$, содержащую ровно z нулей.

Теорема 2. *Обобщенный алгоритм 1-удаления передает*

$$\binom{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil}{z} \cdot (q-1)^{n-2t-\lceil \log_{q-1} \binom{z+t}{z} \rceil - z}$$

сообщений.

Касательные к границе Хэмминга, выходящие из точек $(1/2, 0)$ и $(1/3, 0)$, пересекаются при

$$\tau^* = \frac{\log_q \lambda - \log_q (q-1)}{3 \log_q \lambda - 2 \log_q (q-1)},$$

где $\lambda = \frac{(q-1)+\sqrt{(q-1)(q+3)}}{2}$.

Доказано, что обобщенный алгоритм улучшает алгоритмы r-удаления на интервале $(\tau^*, 1/(q+1))$, и, следовательно, является наилучшим, из известных на данный момент, асимптотическим алгоритмом на данном интервале.

Также в диссертации приведены некоторые численные значения, показывающие, что для этих значений обобщенный алгоритм улучшает предыдущий, а для больших значений q дает результаты, близкие к границе Хэмминга.

В пятом разделе первой главы рассматриваются задачи, связанные с отношением слово-подслово. Как уже отмечалось выше, эти задачи изучались в связи с алгоритмами удаления.

Рассмотрим множество $\mathcal{X}^k$ слов $x^k = x_1 x_2 \cdots x_k$ длины k над алфавитом $\mathcal{X} = \{0, 1, \ldots, q-1\}$.

Для слова $a^k = a_1 a_2 \cdots a_k \in \mathcal{X}^k$ определим левую тень

$$shad^L(a^k) = a_2 \cdots a_k,$$

которая состоит из подслова, получающегося в результате удаления первого символа a_1 из a^k, и определим правую тень

$$shad^R(a^k) = a_1 \cdots a_{k-1},$$

которая состоит из подслова, получающегося в результате удаления последнего символа a_k из a^k.

Определим тень слова a^k:

$$shad(a^k) = shad^L(a^k) \cup shad^R(a^k).$$

Определяется базисное множество $\mathcal{B}(k, l, r)$ из $\mathcal{X}^k$ как следующее объединение:

$$\mathcal{B}(k, l, r) = \bigcup_{s=0}^{l-r} \mathcal{X}^{l-s} 0^m \mathcal{X}^{r+s}.$$

В пятом разделе первой главы исследуются свойства базисных множеств.

Во **второй главе** изучается дизъюнктивный КМД.

Как уже отмечалось, задачи для КМД эквивалентны задачам комбинаторного поиска. В классической модели группового тестирования мы имеем множество $[N] := \{1, \ldots, N\}$ элементов, содержащих некоторое подмножество $D \subset [N]$ дефектных элементов. Основная задача группового тестирования заключается в нахождении множества D за минимальное число тестов. Каждый тест является некоторым подмножеством множества $[N]$. При этом подразумевается, что имеется некая тестовая функция, которая для каждого подмножества $S \subset [N]$ позволяет выяснить наличие дефектных элементов в этом подмножестве (дает ответ на тест). Формально тестовая функция $f_S : 2^{[N]} \to \{0, 1\}$ может быть определена следующим

образом:

$$f_S(\mathcal{D}) = \begin{cases} 0, & \text{если} \quad |\mathcal{S} \cap \mathcal{D}| = 0; \\ 1, & \text{если} \quad |\mathcal{S} \cap \mathcal{D}| > 0. \end{cases} \tag{1}$$

Набор тестов образует алгоритм поиска. Назовем алгоритм поиска успешным, если, после его применения мы однозначно определяем $\mathcal{D}$ по ответам $f_{\mathcal{S}_1}, \ldots, f_{\mathcal{S}_t}$.

Для случая одного дефекта решение этой задачи давно известно. Удивительно, но уже для случая двух дефектных элементов точный ответ до сих пор неизвестен. Другими словами, $N_n(1) = 2^n$, а нахождение значения $N_n(2)$ является трудной комбинаторной проблемой, где $N_n(d)$ — максимальное число элементов, среди которых можно найти d дефектных элементов за n тестов.

В первом разделе второй главы описывается адаптивный алгоритм нахождения двух дефектных элементов, который уточняет и улучшает известные для этой задачи результаты.

Теорема 3. *Для адаптивного алгоритма w справедливо*

$$w_n(2) = \lfloor 2^{\frac{n+1}{2}} - n2^{\frac{n}{4}} \rfloor,$$

где через $w_n(2)$ обозначено максимальное число элементов, среди которых можно найти 2 дефектных элемента за n тестов с помощью данного алгоритма.

Во втором разделе второй главы изучается задача нахождения одного из нескольких активных пользователей. Получен оптимальный ответ для задачи поиска только одного дефектного элемента для классической модели поиска, когда известно, что дефектных элементов ровно d.

Третья глава состоит из девяти разделов и посвящена изучению кодов, свободных от (w, r)-перекрытий.

В первом разделе второй главы вводятся основные обозначения и даются определения исследуемых объектов. Напомним, что двоичная матрица $C = \|c_{ij}\|$ размера $N \times T$ называется кодом, свободным от (w, r)-перекрытий, если для любой пары непересекающихся подмножеств $J_1, J_2 \subset [T]$ мощности $|J_1| = w$ и $|J_2| = r$ существует

координата $i \in [N]$ такая, что $c_{ij} = 1$ для всех $j \in J_1$ и $c_{ij} = 0$ для всех $j \in J_2$.

Отметим, что основной задачей для кодов, свободных от (w, r)-перекрытий, является нахождение минимальной длины (минимального числа строк) $n = N(T, w, r)$ для заданного числа столбцов T.

Для целых положительных w и r величина

$$R(w, r) = \lim_{T \to \infty} \frac{\log_2 T}{N(T; w, r)}$$

называется асимптотической скоростью кода, свободного от (w, r)-перекрытий.

Второй раздел посвящен конструкциям кодов, свободных от (w, r)-перекрытий. Напомним, что супер-простая блок схема — это (v, k, t, λ) тактическая конфигурация, у которой пересечение любых двух ее блоков содержит не более t элементов. Понятие супер-простой блок схемы было впервые введено в работе[18].

Теорема 5. *Супер-простая (v, k, t, λ) блок схема является кодом, свободным от $(t, \lambda - 1)$ перекрытий, размера $N \times v$, где $N = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}$.*

В третьем разделе доказывается оптимальность некоторых кодов, свободных от (w, r)-перекрытий.

Теорема 6. *Для кодов, свободных от (w, r)-перекрытий, имеем*

$$N(8, 2, 2) = 14,$$

$$N(9, 2, 2) = 18,$$

$$N(10, 2, 3) = 30,$$

$$N(11, 3, 3) = 66.$$

[18]Зиновьев В.А, Семаков Н.В. Равновесные коды и тактические конфигурации // Проблемы передачи информации, 1969. Т.5. №.3. С. 28–36.

В четвертом разделе доказывается, что некоторые из этих оптимальных кодов являются единственными (с точностью до перестановки строк и столбцов кодовой матрицы).

Теорема 7. *Код, свободный от* $(1,2)$*-перекрытий, размера* 9×12*, код свободный от* $(2,2)$*-перекрытий, размера* 14×8*, код свободный от* $(2,3)$*-перекрытий, размера* 30×10*, являются единственными.*

Изучению асимптотических границ для скорости кодов, свободных от (w,r)-перекрытий, посвящен пятый раздел. Вводится композиционное расстояние для произвольного двоичного кода C размера $N\times T$.

Рассмотрим целые положительные x и y. Зафиксируем набор I, состоящий из $x+y$ кодовых слов, и обозначим подматрицу матрицы C, образованную этими кодовыми словами, через $C_{x,y}(I)$. Таким образом матрица $C_{x,y}(I)$ имеет размер $N\times(x+y)$. Назовем композиционным расстоянием для набора I число строк матрицы $C_{x,y}(I)$, имеющих вес x. Обозначим это число через $d(C_{x,y}(I))$.

Другими словами, $d(C_{x,y}(I))$ равно числу строк i матрицы $C_{x,y}(I)$ таких, что

$$\sum_{j=1}^{x+y} c_{ij} = x$$

Определение 7. *Минимальным композиционным расстоянием для двоичного кода* C *назовем величину* $d_{x,y} = \min_{I=x+y} d(C_{x,y}(I))$.

Получена оценка на мощность кода с данным композиционным расстоянием.

Обозначим через R_d скорость двоичного кода длины N с минимальным композиционным расстоянием $d_{x,y}$.

Утверждение 31. *Для двоичного кода* C *длины* N *с минимальным композиционным расстоянием* $d_{x,y}$ *справедливо неравенство*

$$R_d \le 1 - \frac{(x+y)^{x+y} d_{x,y}}{x^x y^y \binom{x+y}{x} N}.$$

С учетом этой оценки, доказано рекуррентное неравенство для скорости кодов, свободных от (w,r)-перекрытий. Это неравенство

позволяет получать наилучшие на данное время асимптотические верхние границы для скорости кодов, свободных от (w, r)-перекрытий.

Теорема 8. *Для скорости кодов, свободных от (w, r)-перекрытий, справедлива асимптотическая граница*

$$R(w, r) \leq \min_{0<x<w} \min_{0<y<r} \frac{R(w-x, r-y)}{R(w-x, r-y) + (x+y)^{x+y}/(x^x y^y)}.$$

Результаты для тривиальных кодов, свободных от (w, r)-перекрытий (когда в кодовой матрице берутся все различные строки веса w), выделены в самостоятельный раздел. В шестом разделе доказана

Теорема 9. *Для любых $w \geq 2$ и $r \geq \frac{(w-1)(w+\sqrt{18w+81}+9)}{2}$ справедливо неравенство*

$$TR(w, r) \geq \frac{w+1}{w-1} r - \sqrt{\frac{36r}{w-1}},$$

где через $TR(w, r)$ обозначено такое максимальное T, при котором $n = N(T, w, r) = \binom{T}{w}$.

В седьмом разделе изучаются коды с ограничениями на возможные коалиции. Рассматривается криптографическая задача распределения секретных ключей, описанная ранее. Предположим, что нам задано множество S, состоящее из w-элементных подмножеств $[T]$, показывающих какие наборы пользователей могут войти в группу пользователей, имеющих общий секретный ключ.

Двоичная матрица $C = \|c_{ij}\|$ размера $N \times T$ называется кодом, свободным от (w, r)-перекрытий, с ограничениями S ($S \subset 2^T$) на возможные коалиции, если для любой пары непересекающихся подмножеств $J_1 \in S$, $J_2 \subset [T]$ мощности $|J_1| = w$ и $|J_2| = r$ существует $i \in [N]$ такое, что $c_{ij} = 1$ для всех $j \in J_1$ и $c_{ij} = 0$ для всех $j \in J_2$.

Доказано утверждение, которое переносит результат теоремы 9 на этот случай.

В восьмом разделе третьей главы изучается новая модель группового тестирования, связанная с разделяющими кодами и кодами, свободными от (w, r)-перекрытий.

Пусть тестовое множество S является произвольным подмножеством множества $[T]$. Обозначим: $S_1 = S$ и $S_0 = T \setminus S$. Однако результаты тестов мы теперь будем рассматривать такие:

$$f_S(D) = \begin{cases} 1, & \text{если } |S_1 \cap D| \geq |S_0 \cap D|; \\ 0, & \text{если } |S_1 \cap D| < |S_0 \cap D|. \end{cases} \quad (2)$$

Теорема 10. *Пусть имеется (w, w) разделяющий код размера $N \times T$. Тогда за N тестов можно найти все дефектные элементы, если $d = 2w - 1$, а результаты тестов получаются согласно (2).*

В девятом разделе третьей главы изучается обобщение на q-ичный случай кодов, свободных от перекрытий.

Матрица $C = \|c_{ij}\|$ размера $N \times T$ является $(r_0, r_1, \ldots, r_{q-1})$ кодом, свободным от перекрытий, если для любых подмножеств $R_0, R_1, \ldots, R_{q-1} \subset [T]$ размера $|R_s| = r_s$ существует координата $i \in [N]$ такая, что $c_{ij} = s$ для всех $j \in R_s$, где $s = 0, 1, \ldots, q-1$.

Рассмотрим q-ичную матрицу $C_X(I)$ размера $N \times X$. Назовем "X-расстоянием" для набора I число строк матрицы $C_X(I)$, таких что каждая строка содержит x_s элементов, имеющих значение s для всех s от 0 до $q-1$. Обозначим это число через $d(C_X(I))$.

Минимальным "X-расстоянием" для q-ичного кода C назовем величину $d_X = \min_{|I|=X} d(C_X(I))$. Обозначим через $R^N(d_X)$ скорость q-ичного кода длины N с минимальным "X-расстоянием" d_X.

Теорема 12. *Для q-ичного кода C длины N с минимальным "X-расстоянием" d_X справедлива следующая асимптотическая граница:*

$$R^N(d_X) \leq (1 - \frac{X^X x_0! x_1! \cdots x_{q-1}! d_X}{x_0^{x_0} x_1^{x_1} \cdots x_{q-1}^{x_{q-1}} X! N})(1 - \log_q(q-1)).$$

Теорема 13. *Для скорости кодов, свободных от $(r_0, r_1, \ldots, r_{q-1})$ перекрытий, справедлива асимптотическая граница:*

$$R \leq \frac{R(r_0 - x_0, r_1 - x_1, \ldots, r_{q-1} - x_{q-1})}{\dfrac{R(r_0 - x_0, \ldots, r_{q-1} - x_{q-1})}{1 - \log_q(q-1)} + \dfrac{X^X}{x_0^{x_0} \cdots x_{q-1}^{x_{q-1}}}}.$$

В **четвертой главе** рассматриваются задачи, связанные с суммирующим КМД.

Множество q-ичных векторов $\{h_1, \ldots, h_r\}$ в n-мерном евклидовом пространстве называется обнаруживающим множеством, если любой q-ичный вектор $x = (x(1), \ldots, x(n)), x(i) \in \{0, 1, \ldots, q-1\}$ однозначно определяется своими скалярными произведениями с векторами $\{h_1, \ldots, h_r\}$. Иными словами, для $r \times n$-матрицы H, строками которой являются векторы h_i, в синдромном соотношении все q^n синдромов s различны.

Линдстрем нашел асимптотически точный (при $n \to \infty$) ответ для задачи восстановления q-ичного вектора x по скалярным произведениям (x, h_i), при этом построенные векторы h_i являются двоичными векторами, не ухудшая асимптотический ответ, а именно, минимальное $r = \frac{2n}{\log_q n}(1 + o(1))$.

Отметим, что в двоичном случае имеется простая связь между скалярным произведением и расстоянием Хэмминга

$$d(x, h) = wt(x) + wt(h) - 2(x, h),$$

где $wt(a)$ — это число ненулевых координат вектора a (вес Хэмминга). Поэтому строки разрешающей $m \times n$-матрицы вместе с добавленным вектором $\mathbf{1}$ являются разрешающим множеством в пространстве H_2^n. К сожалению, подобного соотношения нет в случае $q > 2$.

В первом разделе четвертой главы изучается задача определения метрической размерности $m_{n,q}$ недвоичного пространства Хэмминга.

Множество $B = \{b_1, \ldots, b_m\}$ метрического пространства $\mathcal{B}$ называется разрешающим множеством, если любая точка x пространства определяется однозначно расстояниями $\rho_1 = d(x, b_1), \ldots, \rho_m = d(x, b_m)$ до точек B. Иначе говоря, из того, что $d(x, b_i) = d(y, b_i)$ для всех $i = 1, \ldots, m$, следует $x = y$. Минимальная мощность разрешающего множества называется *метрической размерностью* пространства $\mathcal{B}$.

Формулируется предположение о том, что метрическая размер-

ность пространства Хэмминга равна

$$m_{n,q} = \frac{2n}{\log_q n}(1 + o(1)). \tag{3}$$

Это предположение доказывается для случаев $q = 3$ и $q = 4$.

Теорема 14. *Для метрической размерности четверичного пространства Хэмминга справедливо асимптотическое равенство*

$$m_{n,4} = \frac{2n}{\log_4 n}(1 + o(1)).$$

Отметим еще раз, что задача определения метрической размерности недвоичного пространства Хэмминга тесно связана с задачами для суммирующего КМД.

Случай поиска одного из d дефектных элементов для аддитивной модели изучается во втором разделе четвертой главы. Обозначим через $N_{(Add)}(n, d)$ максимальное число элементов, среди которых мы можем найти один из d дефектных за n тестов, когда результатом теста является число дефектных элементов в тестируемом множестве.

Теорема 15. Имеем

$$N_{(Add)}(n, d) = 2^n + d - 1.$$

Завершается четвертая глава задачей нахождения максимального числа элементов, среди которых мы можем найти j-ый по счету дефектный элемент за n вопросов, для аддитивной модели.

Заключение

В диссертации предложен новый подход к некоторым задачам комбинаторной теории поиска. Эти задачи рассматриваются с точки зрения КМД. Благодаря этому подходу удалось перенести некоторые результаты для двоичного канала с обратной связью на q-ичный случай и для дизъюнктивной модели получить более точные верхние

границы для скорости кодов, свободных от (w, r)-перекрытий. Основные результаты, полученные в диссертации, перечислены ниже.

1. Предложен алгоритм передачи информации по q-ичному каналу с безошибочной обратной связью, который является оптимальным для большой доли ошибок в канале.

2. Предложен алгоритм поиска двух дефектных элементов, улучшающий ранее известные алгоритмы.

3. Построены коды, свободные от (w, r)-перекрытий, и доказана оптимальность и единственность некоторых из них.

4. Введено понятие композиционного расстояния и получена граница на скорость кодов с таким композиционным расстоянием.

5. Получена верхняя граница на скорость кодов, свободных от (w, r)-перекрытий.

6. Для суммирующего канала обобщен результат Линдстрема на случай $q = 3$ и $q = 4$.

7. Получен оптимальный ответ для задачи поиска только одного дефектного элемента для классической и суммирующей модели поиска, когда известно, что дефектных элементов ровно d.

Этот подход может быть применен для дальнейших исследованиях в области теории кодирования, криптографии и комбинаторного поиска. Также результаты работы могут быть использованы в разных практических областях — в практической криптографии, медицине, биологии и др.

Работы автора по теме диссертации

Статьи, опубликованные в рецензируемых журналах из списка ВАК.

1. Алсведе, Р. Обнаружение одного из D дефектных элементов в некоторых моделях группового тестирования / Р. Алсведе, К. Деппе, В. С. Лебедев // Пробл. передачи информ. – 2012. – Т.48, No.2. – С. 100-109.

2. Алсведе, Р. Тени, задаваемые отношением слово-подслово / Р. Алсведе, В. С. Лебедев // Пробл. передачи информ. – 2012. – Т.48, No.1. – С. 37-53.

3. Деппе, К. Задача группового тестирования с двумя дефектами / К. Деппе, В. С. Лебедев // Пробл. передачи информ. – 2013. – Т.49, No.4. – С. 87-94.

4. Кабатянский, Г. А. О метрической размерности недвоичных пространств Хэмминга / Г. А. Кабатянский, В. С. Лебедев // Пробл. передачи информ. – 2018. – Т.54, No.1. – С. 54-62.

5. Ким, Ш. Х. Об оптимальности тривиальных кодов, свободных от (w,r)-перекрытий / Ш. Х. Ким, В. С. Лебедев // Пробл. передачи информ. – 2004. – Т.40, No.3. – С. 13-20.

6. Лебедев, В.С. Асимптотическая верхняя граница для скорости кодов, свободных от (w,r) -перекрытий / В. С. Лебедев // Пробл. передачи информ. – 2003. – Т.39, No.4. – С. 3-9.

7. Лебедев, В.С. Замечание о единственности кодов, свободных от (w,r)-перекрытий / В. С. Лебедев // Пробл. передачи информ. – 2005. – Т.41, No.3. – С. 17-22.

8. Лебедев, В.С. Асимптотические границы для скорости окрашенных кодов, свободных от перекрытий / В. С. Лебедев // Пробл. передачи информ. – 2008. – Т.44, No.2. – С. 46-53.

9. Лебедев, В.С. О перечислении q-ичных последовательностей, содержащих подблок 00 фиксированное число раз / В. С. Лебедев // Пробл. передачи информ. – 2010. – Т.46, No.4. – С. 116-121.

10. Лебедев, В.С. Разделяющие коды и новая модель комбинаторного поиска / В. С. Лебедев // Пробл. передачи информ. – 2010. – Т.46, No.1. – С. 3-8.

11. Лебедев, В.С. Кодирование при наличии бесшумной обратной связи / В. С. Лебедев // Пробл. передачи информ. – 2016. – Т.52, No.2. – С. 3-14.

12. Лебедев, В.С. Адаптивный поиск одного дефектного элемента

для аддитивной модели группового тестирования / В. С. Лебедев // Пробл. передачи информ. – 2017. – Т.53, No.3. – С. 78-83.

13. Ahlswede, R. Non-binary error correcting codes with noiseless feedback, localized errors, or both / R. Ahlswede, C. Deppe, V. Lebedev // Annals of the European Academy of Sciences. – 2005. – No. 1. – P. 285-309.

14. Deppe, C. Bounds for the capacity error function for unidirectional channels with noiseless feedback / C. Deppe, V. Lebedev, G. Maringer // Theoretical Computer Science. –2021. – 856. – P. 1-13.

15. Deppe, C. Algorithms for q-ary error-correcting codes with limited magnitude and feedback / C. Deppe, V. Lebedev // Discrete Mathematics. –2021. – V. 344, N 2. – P. 112199.

16. Kim, H.K. On Optimal Superimposed Codes / H.K. Kim , V. S. Lebedev // J. Combin. Des. – 2004. – V. 12, N 2. – P. 79-91.

17. Kim, H.K. Some New Results on Superimposed Codes / H.K. Kim , V. S. Lebedev, D.Y. Oh // J. Combin. Des. – 2005. – V. 13. – P. 276-285.

Тезисы и материалы конференций.

18. Ahlswede, R. Non-binary error correcting codes with noiseless feedback / R. Ahlswede, C. Deppe, V. Lebedev // Proc. Tenth International Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod (Russia), September 3-9. – 2006. – P. 7-10.

19. Ahlswede, R. Shadows under the word-subword relation / R. Ahlswede, V. Lebedev // Proc. Twelfth International Workshop on Algebraic and Combinatorial Coding Theory, Novosibirsk (Russia), September 5-11. – 2010. – P. 16-19.

20. Ahlswede, R. Bounds for threshold and majority group testing / R. Ahlswede, C. Deppe, V. Lebedev // 2011 IEEE International Symposium on Information Theory, Sankt-Peterburg, Russia, Aug. 1-5. – 2011. – P. 69-73.

21. Ahlswede, R. Finding one of D defective elements in some group testing models / R. Ahlswede, C. Deppe, V. Lebedev // Proc. Thirteenth Int. Workshop on Algebraic and Combinatorial Coding Theory. Pomorie, Bulgaria. June 15-21. – 2012. – P. 15-20.

22. Deppe, C. Multiaccess problem with two active users / C. Deppe, V. Lebedev // Proc. Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk (Russia), September 7-13. – 2014. – P. 133-138.

23. Deppe, C. Optimal Algorithms for Q-ary Error-Correcting Feedback Codes with Limited Magnitude / C. Deppe, V. Lebedev // Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT. – 2018. – P. 64-67.

24. Deppe, C. Q-ary Error-Correcting Codes with Feedback / C. Deppe, V. Lebedev // Sixteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT. – 2018. – P. 68-71.

25. Deppe, C. Algorithms for Q-ary Error-Correcting Codes with Partial Feedback and Limited Magnitude / C. Deppe, V. Lebedev // International Symposium on Information Theory (ISIT), IEEE, Jul. – 2019. – P. 2244-2248.

26. Deppe, C. How to apply the rubber method for channels with feedback / C. Deppe, V. Lebedev, G. Maringer // Proc. Algebraic and Combinatorial Coding Theory (ACCT), IEEE. – 2020. – P. 73-76.

27. Deppe, C. Bounds for the capacity error function for unidirectional channels with noiseless feedback / C. Deppe, V. Lebedev, G. Maringer // IEEE International Symposium on Information Theory (ISIT), IEEE, Jun – 2020. – P. 2061-2066.

28. Kabatianski, G. The Mastermind game and the rigidity of the Hamming space / G. Kabatianski, V. Lebedev, J. Thorpe // Proc. IEEE Int. Symp. Inform. Theory. – 2000. P. 375.

29. Kim, H.K. Uniqueness of Some Optimal Superimposed Codes / H.K. Kim , V. S. Lebedev // Proc. Ninth Int. Workshop on Algebraic and Combinatorial Coding Theory. Kranevo, Bulgaria. June 19-25. – 2004. – P. 241-246.

30. Lebedev, V. S. Some tables for (w,r) superimposed codes / V. S. Lebedev // Proc. Eighth International Workshop on Algebraic and Combinatorial Coding Theory, Tsarskoe Selo (Russia), September 8-14. – 2002. – P. 185-189.

31. Lebedev, V. S. Colored Superimposed Codes / V. S. Lebedev //

Proc. Eleventh Int. Workshop on Algebraic and Combinatorial Coding Theory. Pamporovo, Bulgaria. June 16-22. – 2008. – P. 177-180.