ФГБОУ ВО
Московский государственный университет
имени М. В. Ломоносова

На правах рукописи

ПОЛЯНСКИЙ Никита Андреевич

Коды, свободные от перекрытий

01.01.05 — теория вероятностей и математическая статистика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико–математических наук

Москва — 2016

Работа выполнена на кафедре теории вероятностей механико–математического факультета ФГБОУ ВО Московского государственного университета имени М. В. Ломоносова.

Научный руководитель:
доктор физико-математических наук, профессор
Дьячков Аркадий Георгиевич

Официальные оппоненты:
доктор физико-математических наук, профессор
Соловьева Фаина Ивановна, профессор кафедры теоретической кибернетики ФГАОУ ВО «Новосибирский национальный исследовательский государственный университет»,

кандидат физико-математических наук, старший научный сотрудник
Лебедев Владимир Сергеевич, старший научный сотрудник Добрушинской лаборатории ФГБУН «Институт проблем передачи информации имени А.А. Харкевича РАН»

Ведущая организация:
ФГУ «Федеральный исследовательский центр «Информатика и управление» РАН»

Защита диссертации состоится 30 сентября 2016 г. в 16^{45} на заседании диссертационного совета Д 501.001.85 на базе МГУ имени М.В. Ломоносова по адресу: 119234, Москва, ГСП–1, Ленинские горы, д. 1, МГУ имени М. В. Ломоносова, механико-математический факультет, аудитория 16–24.

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВО Московского государственного университета имени М.В. Ломоносова (Москва, Ломоносовский проспект, д. 27, сектор А, $8^{\text{й}}$ этаж), и на сайте http://mech.math.msu.ru/∼snark/index.cgi.

Автореферат разослан « » августа 2016 г.

Ученый секретарь диссертационного совета
Д 501.001.85 на базе МГУ им. М.В. Ломоносова,
доктор физико–математических наук, Власов
профессор Виктор Валентинович

Общая характеристика работы

Актуальность темы

Диссертационная работа посвящена вопросам теории дизъюнктивных кодов. В ней рассматриваются задачи, лежащие на стыке теории вероятностей, теории информации и комбинаторной теории кодирования.

Двоичный код называется ***дизъюнктивным*** s***-кодом****, если он является матрицей инцидентности семейства множеств, для которого никакое множество не содержится в объединении* s *любых других множеств данного семейства.*

Если множества данного семейства есть некоторые подмножества множества $\{1, 2 \ldots, N\}$, то число N назовем *длиной* кода, а мощность такого семейства – *объемом* кода, и будем обозначать через t. Определим *скорость* кода $R = \log_2 t/N$. Столбцы соответствующей матрицы инцидентности будем называть *кодовыми словами.*

Дизъюнктивные коды были введены У. Каутсом и Р. Синглтоном в 1964 году в основополагающей статье[1], где был описан ряд прикладных задач и построены некоторые важные конструкции таких кодов. Отметим, что многие авторы изучали вопросы, относящиеся к дизъюнктивным кодам, с принципиально разных точек зрения и зачастую проводили свои исследования независимо от других ученых. Именно поэтому многие результаты были сперва найдены в теории информации, а позднее были переоткрыты в комбинаторике или в теории группового тестирования, и наоборот. В подтверждение вышесказанного можно выделить статью[2], написанную в 1982 году П. Эрдешем и др., в которой вводится определение дизъюнктивного 2-кода, а позднее, в 1985 году, в своей следующей работе[3] авторы обобщили его уже для произвольного значения s.

Определим *асимптотическую скорость* дизъюнктивных s-кодов как

$$R(s, 1) = \varlimsup_{t\to\infty} \frac{\log_2 t}{N(t, s, 1)}, \tag{1}$$

где число $N(t, s, 1)$ равно минимальной длине дизъюнктивного s-кода объема t. Из определения сразу следует[1] теоретико-информационная верхняя граница скорости $R(s, 1) \leqslant 1/s$. В 1982 году П. Эрдеш доказал[2] оценки, из

[1] Kautz W. H., Singleton R. C., Nonrandom Binary Superimposed Codes // *IEEE Trans. Inform. Theory*, **10**:4 (1964), 363–377.

[2] Erdos P., Frankl P., Furedi Z., Families of Finite Sets in Which No Set Is Covered by the Union of two Others // *J. Combin. Theory*, Ser. A, **33** (1982), 158–166.

[3] 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.*, **51** (1985), 79–89.

которых следует, что

$$0.183 \leqslant R(2,1) \leqslant 0.322. \tag{2}$$

В том же году А.Г. Дьячковым и В.В. Рыковым независимо была построена[4] верхняя граница скорости $R(s,1)$, которая к настоящему моменту является наилучшей. Следует сказать, что они использовали собственную технику при выводе оценки. Эта граница при $s = 2$ совпадает с (2), а в случае произвольного s было доказано, что верна следующая граница

$$R(s,1) \leqslant \frac{2\log_2[e(s+1)/2]}{s^2}. \tag{3}$$

Отметим, что позднее, в 1994 году, М. Ружинко сумел привести[5] более простое доказательство этого факта, но уже в ослабленной форме

$$R(s,1) \leqslant \frac{8\log_2 s}{s^2}. \tag{4}$$

Нижняя граница скорости $R(s,1)$ была получена А.Г. Дьячковым и В.В. Рыковым в 1983 году в работе[6], в которой с помощью метода случайного кодирования на ансамбле двоичных кодов с независимыми компонентами показано, что асимптотика границы имеет вид

$$R(s,1) \geqslant \frac{\log_2 e}{s^2 e}(1+o(1)) = \frac{0.531}{s^2}(1+o(1)), \quad s \to \infty. \tag{5}$$

Определенный интерес представляет собой работы, написанные независимо П. Эрдешом[3] в 1985 году и Ф. Хуонгом[7] в 1987 году, которые, в частности, содержат следующую оценку

$$R(s,1) \geqslant \frac{\log_2 e}{4s^2}(1+o(1)) = \frac{0.361}{s^2}(1+o(1)), \quad s \to \infty. \tag{6}$$

В дальнейшем, была построена более точная границы снизу для $R(s,1)$. В 1989 году методом случайного кодирования на ансамбле двоичных равновесных кодов А.Г. Дьячков и др. показали[8], что асимптотика нижней

[4] Дьячков А. Г., Рыков В. В., Границы длины дизъюнктивных кодов // *Пробл. передачи информ.*, **18**:3 (1982), 7–13.

[5] Ruszinko M., On the upper bound of the size of the r-cover-free families // *J. Combin. Theory*, Ser. A., **66** (1994), 302–310.

[6] D'yachkov A. G., Rykov V. V., A Survey of Superimposed Code Theory // *Prob. of Control and Inform. Theory*, **12**:4 (1983), 229–242.

[7] Hwang F. K., Sos V. Z., Non adaptive hypergeometric group testing // *Studia Sci. Math. Hungarica*, **22** (1987), 257–263.

[8] D'yachkov A. G., Rykov V. V., Rashad A. M., Superimposed Distance Codes // *Prob. of Control and Inform. Theory*, **18**:4 (1989), 237–250.

границы имеет вид

$$R(s,1) \geqslant \frac{1}{s^2 \log_2 e}(1+o(1)) = \frac{0.693}{s^2}(1+o(1)), \quad s \to \infty. \tag{7}$$

В частности, при $s = 2$ полученная авторами оценка совпадает с (2).

Практически все классические проблемы теории дизъюнктивных кодов допускают обобщения. Одним из естественных таких обобщений является следующее определение.

Двоичный код называется ***свободным от перекрытий*** (s,ℓ)***-кодом****, если он является матрицей инцидентности семейства множеств, для которого пересечение любых ℓ множеств не покрывается объединением s любых других множеств данного семейства.*

Свободные от перекрытий коды были введены[9] К. Митчеллом и Ф. Пайпером в 1988 году в связи с криптографической задачей распределения ключей. Основные конструкции свободных от перекрытий кодов, построенные на укороченных кодах Рида-Соломона, были описаны[10] в 2002 году. Для малых значений параметров s и ℓ Ш.Х. Ким и В.С. Лебедев привели[11,12,13] оптимальные конструкции свободных от перекрытий (s,ℓ)-кодов, а также получили некоторые конструктивные оценки для минимальной длины таких кодов. В 2009 году была найдена[14] скорость конструкций свободных от перекрытий кодов, основанных на алгебро-геометрических кодах.

Аналогичным образом определим асимптотическую скорость свободных от перекрытий (s,ℓ)-кодов

$$R(s,\ell) = \varlimsup_{t\to\infty} \frac{\log_2 t}{N(t,s,\ell)}, \tag{8}$$

где число $N(t,s,\ell)$ равно минимальной длине дизъюнктивного свободного от перекрытия (s,ℓ)-кода объема t. Первые результаты исследования верхних границ скорости $R(s,\ell)$ для СП (s,ℓ)-кодов, $2 \leqslant \ell \leqslant s$, были получены

---

[9]Mitchell C. J., Piper F. C., Key storage in Secure Networks // *Discrete Applied Mathematics*, **21** (1988), 215–228.

[10]D'yachkov A., Vilenkin P., Macula A., Torney D., Families of Finite Sets in Which No Intersection of ℓ Sets Is Covered by the Union of s Others // *J. Combin. Theory*, Ser. A, **99** (2002), 195–218.

[11]Kim H., Lebedev V. S., On Optimal Superimposed Codes // *Journal of Combinatorial Designs*, **12**:2 (2004), 79–91.

[12]Ким Ш. Х., Лебедев В. С., Об оптимальности тривиальных кодов, свободных от (w,r)-перекрытий // *Пробл. передачи информ.*, **40**:3 (2004), 13–20.

[13]Kim H., Lebedev V., Oh D., Some new results on superimposed codes, *J. Combin. Des.*, **13**:4 (2005), 276—285.

[14]Сидельников В. М., Приходов О. Ю., О построении кодов, свободных от (w,r)-перекрытий // *Пробл. передачи информ.*, **45**:1 (2009), 36–40.

в 2000 году в работе[15] Д. Стинсона и др., а также в 2002 году в работе[10] А.Г. Дьячкова и др. Было показано[15], что выполняется следующая оценка

$$R(s,\ell) \leqslant \frac{20\log_2\binom{s+\ell}{s}}{7\binom{s+\ell}{s}(s+\ell)},$$

а также верно рекуррентное неравенство

$$\frac{1}{R(s,\ell)} \geqslant \frac{1}{R(s,\ell-1)} + \frac{1}{R(s-1,\ell)}. \tag{9}$$

В 2003 году В.С. Лебедев доказал[16] неравенство

$$R(s,\ell) \leqslant \frac{R(s-i,\ell-j)}{R(s-i,\ell-j)+\frac{(i+j)^{i+j}}{i^i\cdot j^j}}, \quad i\in[s-1],\ j\in[\ell-1], \tag{10}$$

которое представляет собой уточнение неравенства

$$R(s,\ell) \leqslant R(s-i,\ell-j)\frac{i^i\cdot j^j}{(i+j)^{i+j}}, \quad i\in[s-1],\ j\in[\ell-1], \tag{11}$$

ранее установленного[17] П. Энгелом в 1996 году. Рекуррентное неравенство (10) и верхняя граница (3) дают[18] для скорости $R(s,\ell)$, $2\leqslant\ell\leqslant s$ наилучшую известную верхнюю границу для $R(s,\ell)$, асимптотическое поведение которой при фиксированном $\ell\geqslant 2$ и $s\to\infty$ описывается следующим неравенством

$$R(s,\ell) \leqslant \frac{(\ell+1)^{\ell+1}}{2\,e^{\ell-1}}\frac{\log_2 s}{s^{\ell+1}}(1+o(1)). \tag{12}$$

Нижняя граница скорости $R(s,\ell)$, $2\leqslant\ell\leqslant s$, была получена[10] с помощью метода случайного кодирования на ансамбле с независимыми двоичными компонентами кодовых слов и на некотором специальном ансамбле с независимыми двоичными равновесными словами, предложенном[19] ранее

[15]Stinson D. R., Wei R., Zhu L., Some New Bounds for Cover-Free Families // *J. Combin. Theory*, Ser. A, **90** (2000), 224–234.

[16]Лебедев В. С., Асимптотическая верхняя граница скорости кодов, свободных от (w,r)-перекрытий // *Пробл. передачи информ.*, **39**:4 (2003), 3–9.

[17]Engel K., Interval Packing and Covering in the Boolean Lattice // *Combinatorics Prob. and Computing*, **5** (1996), 373–384.

[18]D'yachkov A. G., Vilenkin P. A., Yekhanin S. M., Upper Bounds on the Rate of Superimposed (s,ℓ)-Codes Based on Engel's Inequality // *Proc. Eighth Int. Workshop «Algebraic and Combinatorial Coding Theory»*, Tsarskoe Selo, (2002), 95–99.

[19]Quang A. N., Zeisel T., Bounds on Constant Weight Binary Superimposed Codes // *Problems of Control and Inform. Theory*, **17**:4 (1988), 223–230.

Н. Куонгом и Т. Зейселем. При фиксированном $\ell \geqslant 2$ и $s \to \infty$ асимптотика этой границы имеет вид

$$R(s,\ell) \;\geqslant\; \frac{\ell^\ell \log_2 e}{e^\ell}\frac{1}{s^{\ell+1}}(1+o(1)). \tag{13}$$

Одним из следующих направлений в теории дизъюнктивных кодов стало вероятностное обобщение дизъюнктивного s-кода. В 2004 году Э. Макула и др. ввели[20] определение почти дизъюнктивных кодов. В недавней статье[21] А.Г. Дьячковым и др. было описано такое обобщение для более широкого класса дизъюнктивных кодов. Дадим основное определение.

Под плохим событием будем понимать следующее: «дизъюнктивная сумма некоторых s кодовых слов покрывает некоторое другое кодовое слово» (подмножество из s кодовых слов выбирается равновероятно). Тогда *пропускной способностью* $C(s,1)$ почти дизъюнктивных кодов будем называть точную верхнюю грань для скорости кодов, для которых вероятность плохого события убывает экспоненциально с ростом длины кода. Для пропускной способности почти дизъюнктивных кодов И. Воробьевым была доказана[21] следующая граница

$$C(s,1) \geqslant \frac{\ln 2}{s}(1+o(1)), \quad s \to \infty. \tag{14}$$

В недавней работе[22] была подсчитана асимптотическая граница для скорости некоторых конструкций[23] почти дизъюнктивных кодов, основанных на укороченных кодах Рида-Соломона.

Аналогичным образом можно обобщить определение для свободного от перекрытий (s,ℓ)-кода. В данном случае под плохим событием подразумевать следующее: «дизъюнктивная сумма некоторых s кодовых слов покрывает конъюнкцию некоторых других ℓ кодовых слов» (подмножество из s кодовых слов выбирается равновероятно). Тогда в схожей манере (см. случай $\ell = 1$) определим пропускную способность $C(s,\ell)$ почти свободных от перекрытий кодов. Отметим, что всякий код X является почти свободным от перекрытий (s,ℓ,ε)-кодом, где параметр $\varepsilon = \varepsilon(X)$ равен вероятности плохого события.

---

[20] Macula A. J., Rykov V. V., Yekhanin S., Trivial two-stage group testing for complexes using almost disjunct matrices // *Discrete Applied Mathematics*, **137**:1 (2004), 97—107.

[21] Дьячков А. Г., Воробьев И. В., Полянский Н. А., Щукин В. Ю., Почти дизъюнктивные коды со списочным декодированием // *Пробл. передачи информ.*, **51**:2 (2015), 27–49.

[22] Бассалыго Л. А., Рыков В. В., Гиперканал множественного доступа //*Пробл. передачи информ.*, **49**:4 (2013), 3–12.

[23] D'yachkov A. G., Macula A. J., Rykov V. V., New Applications and Results of Superimposed Code Theory Arising from the Potentialities of Molecular Biology // In the book «Numbers, Information and Complexit», *Kluwer Academic Publishers*, (2000), 265–282.

Одним из важных приложений свободных от перекрытий кодов является[24] задача поиска скрытого гиперграфа из семейства локализованных гиперграфов. Предположим, что задан скрытый гиперграф $H_{un} = (V, E)$, ребра которого нам неизвестны, но мы знаем, что этот гиперграф H_{un} принадлежит некоторому семейству $\mathcal{F}$ гиперграфов, имеющих особую структуру (например, $\mathcal{F}$ состоит из всевозможных гамильтоновых циклов на V). Наша цель – обнаружить ребра E этого гиперграфа, спросив N вопросов $Q(S)$, где множество S – это некоторое подмножество V, а ответ на вопрос положительный, т.е. $Q(S) = 1$ в случае, если множество S содержит полностью хотя бы одно ребро из E. В остальных случаях ответ на вопрос отрицательный, т.е. $Q(S) = 0$. Будем называть поиск неадаптивным, если все вопросы заранее спланированы и задаются одновременно. Если же вопросы задаются последовательно, и последующие вопросы зависят от ответов на предыдущие, то поиск называют адаптивным. Рассмотрим семейство гиперграфов $\mathcal{F}(t, s, \ell)$, которое будет состоять из таких гиперграфов $H = (V, E)$, что множество вершин $V = \{1, 2 \dots t\}$, множество ребер $E = \{e_1, e_2, \dots, e_{s'}\}$, $1 \leqslant s' \leqslant s$, и размер каждого ребра $1 \leqslant |e_i| \leqslant \ell$, причем никакое ребро не содержится ни в каком другом. Итак, пусть задан скрытый гиперграф $H_{un} = (V, E)$ и мы знаем, что $H_{un} \in \mathcal{F}(t, s, \ell)$. Будем говорить, что $\mathcal{A}$ является алгоритмом поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$, если он находит H_{un}, т.е. существует ровно один гиперграф из семейства $\mathcal{F}(t, s, \ell)$, который удовлетворяет всем заданным вопросам.

Обозначим через $N(\mathcal{A})$ максимальное количество вопросов алгоритма $\mathcal{A}$, необходимых для поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$. Определим асимптотическую скорость алгоритмов поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$ как

$$R_h(s, \ell) = \overline{\lim_{t \to \infty}} \frac{\log_2 t}{N_h(t, s, \ell)}, \tag{15}$$

где число $N_h(t, s, \ell)$ равно минимальному числу вопросов $N(\mathcal{A})$ среди всех алгоритмов $\mathcal{A}$ поиска скрытого гиперграфа из семейства $\mathcal{F}(t, s, \ell)$. Будем приписывать к величине $R_h(s, \ell)$ верхний индекс a и na в зависимости от адаптивности поиска.

В 2002 году А.Г. Дьячков и др. показали[10], что задача неадаптивного поиска скрытого гиперграфа и свободные от перекрытия коды сильно связаны между собой, в частности, выполнены следующие неравенства

$$R_h^{na}(s, \ell) \leqslant R(s, \ell) \leqslant \min\left(R_h^{na}(s-1, \ell), R_h^{na}(s, \ell-1)\right). \tag{16}$$

[24] Angluin D., Chen J., Learning a hidden hypergraph // *Journal of Machine Learning Research*, **7** (2006), 2215–2236.

Естественной теоретико-информационной границей для скорости адаптивного поиска служит следующее неравенство

$$R_h^a(s,\ell) \leqslant \frac{1}{s\ell}.$$

Отметим, что при $\ell = 1$ данная задача вырождается в довольно известную задачу поиска дефектов. Известно[25], что адаптивный поиск дефектов достигает теоретико-информационную границу, т.е.

$$R_h^a(s,1) = \frac{1}{s}. \tag{17}$$

Для задачи поиска скрытого графа, т.е. при $\ell = 2$, в 2008 году Д. Англуин и Ж. Чен привели[26] близкий к оптимальному алгоритм поиска скрытого графа, из которого следует, что

$$R_h^a(s,2) \geqslant 1/(12s).$$

Для произвольных значений s и ℓ в 2014 году Х. Абаси и др. недавно показали[27], что

$$R_h^a(s,\ell) \geqslant 1/(2s\ell).$$

Рассмотрим следующее вероятностное обобщение. Под плохим событием будем понимать: «алгоритм поиска скрытого гиперграфа не находит скрытый гиперграф» (скрытый гиперграф выбирается равновероятно в семействе $\mathcal{F}(t,s,\ell)$). Тогда пропускной способностью $C_h(s,\ell)$ будем называть точную верхнюю грань для скорости алгоритмов поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$, для которых вероятность плохого события стремиться к нулю с ростом числа вершин t. Также будем приписывать к величине $C_h(s,\ell)$ верхний индекс a и na в зависимости от адаптивности алгоритма поиска.

Классическим результатом для теории планирования экспериментов является следующее равенство, доказанное[28] М.Б. Малютовым и В.Л Фрейдлиной:

$$C_h^a(s,1) = C_h^{na}(s,1) = \frac{1}{s}.$$

[25]Du D. Z., Hwang F. K., Combinatorial Group Testing and Its Applications, 2nd ed., *Series on Applied Mathematics*, **12** (2000).

[26]Angluin D., Chen J., Learning a hidden graph using $O(\log n)$ queries per edge // *J. Comput. Syst. Sci.*, **74** (2008), 546–556.

[27]Abasi H., Bshouty N. H., Mazzawi H., On Exact Learning Monotone DBF from Membership Queries // *Lecture Notes in Artificial Intelligence*, (2014), 111–124.

[28]Малютов М. Б., Фрейдлина В. Л., О применении теории информации к одной задаче выделения значимых факторов // *Теория вероятностей и ее применения*, **18**:2 (1973), 432-–444.

Цель работы

Целью диссертационной работы являются:

- построение более точных оценок снизу для асимптотической скорости свободных от перекрытий кодов;
- построение оценок снизу и сверху для пропускной способности почти свободных от перекрытий кодов;
- исследование алгоритмов поиска скрытого гиперграфа из семейства локализованных гиперграфов.

Научная новизна

Все результаты работы являются новыми. В диссертации получены следующие основные результаты.

1. Доказаны новые границы снизу для асимптотической скорости $R(s, \ell)$ свободных от перекрытий кодов при $\ell \geqslant 2$, улучшающие наилучшие ранее известные границы, установленные[10] А.Г. Дьячковым и др.
2. Предложена конструкция свободных от перекрытия кодов, обобщающая ранее известную конструкцию дизъюнктивных кодов, полученную[29] Э. Макулой.
3. Впервые получены границы снизу и сверху для пропускной способности $C(s, \ell)$ почти свободных от перекрытий кодов при $\ell \geqslant 2$.
4. Доказана новая граница снизу для асимптотической скорости $R_h^a(s, \ell)$ адаптивного поиска скрытого гиперграфа, достигающая теоретико-информационную границу и улучшающая результаты работы[27] Х. Абаси и др.
5. Впервые получена граница снизу для пропускной способности $C_h^{2\text{-st}}(s, \ell)$ двухступенчатой процедуры поиска скрытого гиперграфа, достигающая теоретико-информационную границу.

[29] Macula A. J., A simple construction of d-disjunct matrices with certain constant weights // *Discrete Math.*, Ser. A, **162**:1-3 (1996), 311–312.

Основные методы исследования

В работе используются классические теоретико-вероятностные методы для вычисления асимптотики важных теоретико-информационных характеристик, в частности, при оценивании вероятностей больших уклонений в методе случайного кодирования для ансамбля равновесных кодов; методы выпуклого анализа; аналитические методы; методы комбинаторной теории кодирования.

Теоретическая и практическая ценность работы

Результаты диссертации носят теоретический характер. Они могут быть полезны специалистам, работающим в теории информации и комбинаторной теории кодирования.

Апробация диссертации

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

1. Семинар по теории кодирования под рук. Л.А. Бассалыго в 2011–2016 гг., Институт проблем передачи информации им. А.А. Харкевича РАН.

2. Семинар «Проблемы современной теории информации» в 2010–2016 гг. под рук. А.Г. Дьячкова, кафедра теории вероятностей, механико-математический факультет, Московский государственный университет им. М.В. Ломоносова.

3. Семинар по дискретной математике под рук. М.В. Вялого и С.П. Тарасова в 2016 г., Вычислительный центр им. А.А. Дородницына РАН.

Результаты диссертации докладывались автором на следующих конференциях:

1. International workshop «*Search Methodologies III*», Bielefeld, Germany, 2012.

2. Международная научная конференция студентов, аспирантов и молодых учёных «*Ломоносов-2013*», Москва, Россия, 2013.

3. 14th International Workshop «*Algebraic and Combinatorial Coding Theory*», Svetlogorsk, Russia, 2014.

4. IEEE International Symposium on Information Theory, Honolulu, USA, 2014.

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

6. IEEE International Symposium on Information Theory, Hong Kong, China, 2015.

7. Международная научная конференция студентов, аспирантов и молодых учёных «*Ломоносов-2016*», Москва, Россия, 2016.

8. 15th International Workshop «*Algebraic and Combinatorial Coding Theory*», Albena, Bulgaria, 2016.

9. IEEE International Symposium on Information Theory, Barcelona, Spain, 2016.

Публикации

Результаты автора по теме диссертации опубликованы в 10 работах, список которых приведен в конце автореферата. Среди них 3 работы [1]-[3] в журналах из перечня ВАК и 7 работ [4]-[10] в рецензируемых трудах международных конференций.

Структура и объем диссертации

Диссертация состоит из оглавления, введения, трех глав, заключения и списка литературы, который включает 46 наименований. Объем диссертации составляет 79 страниц.

Краткое содержание диссертации

Во **введении** сформулированы основные объекты исследования, дан краткий исторический обзор предыдущих результатов, а также приведено основное содержание работы и ее апробация.

Первая глава состоит из пяти разделов, посвященных вопросам свободных от перекрытий кодов.

В первом разделе первой главы даны основные определения, используемые в следующих разделах.

Во втором разделе первой главы для доказательства нижних границ $R(s, \ell)$ мы исследуем ансамбль $E(N, t, Q)$ двоичных $(N \times t)$-матриц X с N

строками и t столбцами, где столбцы выбираются независимо и равновероятно из множества столбцов фиксированного веса $\lfloor QN \rfloor$, $0 \leqslant Q \leqslant 1$. Рассматривается вероятность $P_0(N, Q, s, \ell)$ плохого события «пара $(\boldsymbol{x}(\mathcal{S}), \boldsymbol{x}(\mathcal{L}))$ является (s, ℓ)-плохой», т.е. для непересекающихся наборов столбцов с номерами $\mathcal{S}$ и $\mathcal{L}$ не выполнено условие: существует строка $i \in [N]$ такая, что $x_i(j) = 0$ для $j \in \mathcal{S}$ и $x_i(j) = 1$ для $j \in \mathcal{L}$. Далее показано, что

$$R(s, \ell) \geqslant \underline{R}(s, \ell) \triangleq \frac{1}{s + \ell - 1} \max_{0<Q<1} A(s, \ell, Q), \qquad 2 \leqslant \ell \leqslant s,$$

где

$$A(s, \ell, Q) \triangleq \varliminf_{N\to\infty} \frac{-\log_2 P_0(N, Q, s, \ell)}{N}, \quad 0 < Q < 1.$$

В результате мы исследуем величину $A(s, \ell, Q)$. Используя терминологию типов последовательностей, удается свести задачу к поиску минимума функционала

$$F = F(\tau, \upsilon, Q) \triangleq \sum_{\mathbf{a}\in\{0,1\}^s} \tau(\mathbf{a}) \log_2 [\tau(\mathbf{a})] + \sum_{\mathbf{b}\in\{0,1\}^\ell} \upsilon(\mathbf{b}) \log_2 [\upsilon(\mathbf{b})] - (1 - \tau(\boldsymbol{0}))h\left(\frac{\upsilon(\boldsymbol{1})}{1 - \tau(\boldsymbol{0})}\right) + (s + \ell)h(Q) + h(\upsilon(\boldsymbol{1})).$$

в области с линейными ограничениями на распределения τ и υ. Применяя стандартный метод множителей Лагранжа и используя выпуклость функции F в рассматриваемой задаче с ограничениями, можно представить распределения τ и υ, на которых достигается минимум в задаче, как функции переменных z и u. Используя полученные результаты, мы доказываем следующую теорему (далее нумерация утверждений совпадает с их нумерацией в соответствующих главах диссертационной работы).

Теорема 1.2.2. (Граница случайного кодирования $\underline{R}(s, \ell)$.) *Имеют место следующие три утверждения.*

1. *Пусть $2 \leqslant \ell \leqslant s$. Тогда скорость СП (s, ℓ)-кодов*

$$R(s, \ell) \geqslant \underline{R}(s, \ell) \triangleq \frac{1}{s + \ell - 1} \max_{\substack{(20)\\ 0<z,\,u<1}} T(z, u, s, \ell), \tag{18}$$

где функция $T(z, u, s, \ell)$ определена следующим образом

$$T(z, u, s, \ell) \triangleq \frac{su}{1 - (z - u)} \log_2 \left[\frac{z}{u}\right] + \frac{\ell(1 - z)}{1 - (z - u)} \log_2 \left[\frac{1 - u}{1 - z}\right] + (s + \ell - 1) \log_2 [1 - (z - u)], \tag{19}$$

а параметры z *и* u, $0 < z, u < 1$, *связаны между собой посредством следующего равенства*

$$z - u = z^s(1-u)^\ell. \tag{20}$$

2. *Если* $s \to \infty$ *и* $\ell \geqslant 2$ *фиксировано, то для нижней границы* $\underline{R}(s,\ell)$ *справедливо асимптотическое равенство*

$$R(s,\ell) \geqslant \underline{R}(s,\ell) = \frac{e^{-\ell}\ell^\ell \log_2 e}{s^{\ell+1}}(1+o(1)), \quad \ell = 2,3,\ldots, \quad s \to \infty. \tag{21}$$

3. *Если* $s \to \infty$, *то для скорости* $R(s,s)$ *справедливо асимптотическое неравенство*

$$R(s,s) \geqslant \frac{\log_2 e}{s2^{2s+1}}(1+o(1)), \quad s \to \infty. \tag{22}$$

В третьем разделе первой главы мы напоминаем наилучшие верхние границы $R(s,\ell)$.

В четвертом разделе первой главы мы приводим сводную таблицу с численными значениями для полученных нижних границ $R(s,\ell)$, а также ранее известных верхних границ.

В пятом разделе первой главы мы предлагаем новую конструкцию свободных от перекрытий кодов, которую мы описываем как матрицу инцидентности некоторой системы множеств. Данное семейство свободных от перекрытий кодов является обобщением ранее известной конструкции дизъюнктивных кодов из работы[29] Э. Макулы. Также мы напоминаем конструкцию свободных от перекрытий кодов, основанную на укороченных кодах Рида-Соломона и для некоторых значений s и ℓ приводим таблицы с конструктивными верхними оценками для $N(t,s,\ell)$.

Вторая глава состоит из пяти разделов, посвященных вопросам почти свободных от перекрытий кодов.

В первом разделе второй главы даны основные определения, используемые в следующих разделах.

Во втором разделе второй главы для доказательства нижних границ $C(s,\ell)$ мы исследуем ансамбль $E(N,t,Q)$ двоичных $(N \times t)$-матриц X с N строками и t столбцами, где столбцы выбираются независимо и равновероятно из множества столбцов фиксированного веса $\lfloor QN \rfloor$, $0 \leqslant Q \leqslant 1$. Рассматриваются вероятности двух событий:

1. условная вероятность события «дизъюнктивная сумма s кодовых слов покрывает конъюнкцию некоторых других ℓ кодовых слов» при усло-

вии, что «вес дизъюнктивной суммы s кодовых слов равен k»:

$$\mathcal{P}_1^{(N)}(\ell, Q, k) \triangleq \Pr\left\{ \bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i) \succcurlyeq \bigwedge_{j\in\mathcal{L}} \boldsymbol{x}(j) \;\Big/\; \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\};$$

2. вероятность события «вес дизъюнктивной суммы s кодовых слов равен k»

$$\mathcal{P}_2^{(N)}(s, Q, k) \triangleq \Pr\left\{ \left|\bigvee_{i\in\mathcal{S}} \boldsymbol{x}(i)\right| = k \right\}, \quad \lfloor QN \rfloor \leqslant k \leqslant \min\{N, s\lfloor QN \rfloor\}.$$

Далее показано, что

$$C(s,\ell) \geqslant \underline{C}(s,\ell) \triangleq \sup_{\substack{(24),\\ 0\leqslant Q\leqslant 1}} R, \tag{23}$$

где точная верхняя грань взята по таким R, что

$$\min_{Q<q<\min\{1,sQ\}} \left\{ \mathcal{A}(s,Q,q) + [\mathcal{D}(\ell,Q,q) - \ell\, R]^+ \right\} > 0, \tag{24}$$

а функции $\mathcal{A}(s,Q,q)$ и $\mathcal{D}(\ell,Q,q)$ являются логарифмическими асимтотиками соответствующих вероятностей:

$$\mathcal{D}(\ell,Q,q) \triangleq \lim_{N\to\infty} \frac{-\log_2\left[\mathcal{P}_1^{(N)}(\ell,Q,k)\right]}{N}, \qquad k = \lfloor qN \rfloor,$$

и

$$\mathcal{A}(s,Q,q) \triangleq \lim_{N\to\infty} \frac{-\log_2\left[\mathcal{P}_2^{(N)}(s,Q,k)\right]}{N}, \qquad k = \lfloor qN \rfloor.$$

Используя аналогичные соображения, что и при доказательстве нижней границы для $R(s,\ell)$ в главе 1, мы доказываем следующие леммы. Пусть $\hat{q} \triangleq 1-(1-Q)^s$.

Лемма 2.2.1. *Функция $\mathcal{A}(s,Q,q)$ параметра q, $Q<q<\min\{1,sQ\}$, может быть записана в параметрической форме*

$$\mathcal{A}(s,Q,q) \triangleq (1-q)\log_2(1-q) + q\log_2\left[\frac{Qy^s}{1-y}\right] + sQ\log_2\frac{1-y}{y} + sh(Q),$$

$$q = Q\frac{1-y^s}{1-y}, \qquad 0<y<1.$$

Более того, функция $\mathcal{A}(s,Q,q)$ является $\cup$-выпуклой, монотонно убывающей в интервале $(Q, 1-(1-Q)^s)$, монотонно возрастающей в интервале $(1-(1-Q)^s, \min\{1, sQ\})$ и свой единственный минимум, равный 0, достигает в точке $q=\hat{q}$, т.е.

$$\min_{Q<q<\min\{1,sQ\}} \mathcal{A}(s,Q,q) \,=\, \mathcal{A}(s,Q,\,\hat{q}) = 0, \quad 0<Q<1.$$

Лемма 2.2.2. *Для $\ell \geqslant 2$, значение функции $\mathcal{D}(\ell,Q,q)$ в точке $q=\hat{q}$ равно*

$$\mathcal{D}(\ell,Q,\hat{q}) \triangleq (1-Q)\ell \log_2 z - (1-\hat{q})\log_2[1-(1-z)^\ell] \tag{25}$$
$$+\ell\left(\frac{(1-Q)}{z}(1-z) - \left(\frac{(1-Q)}{z}-\hat{q}\right)(1-z)^\ell\right)\log_2[1-z] + \ell h(Q),$$

где z единственным образом определяется из следующего уравнения

$$Q = \frac{(1-z)(1-(1-z)^\ell) - (1-\hat{q})z(1-z)^\ell}{1-(1-z)^\ell},$$

а $h(x)$ является функцией двоичной энтропии.

Используя утверждения лемм 2.2.1 и 2.2.2, а также установленное равенство (23), мы доказываем следующую теорему.

Теорема 2.2.2. (Граница случайного кодирования $\underline{C}(s,\ell)$). *Имеют место следующие два утверждения.*

1. *Для $\ell \geqslant 2$ пропускная способность $C(s,\ell)$ ПСП (s,ℓ)-кодов*

$$C(s,\ell) \geqslant \underline{C}(s,\ell) \triangleq \frac{1}{\ell}\max_{0\leqslant Q\leqslant 1}\mathcal{D}(\ell,Q,\hat{q}), \tag{26}$$

где функция $\mathcal{D}(\ell,Q,\hat{q})$ задана посредством (25).

2. *Для фиксированного параметра $\ell \geqslant 2$ и при $s\to\infty$ нижняя асимптотическая граница для $C(s,\ell)$ имеет вид*

$$C(s,\ell) \,\geqslant\, \frac{\ell^{\ell-1}}{e^\ell}\frac{\log_2 e}{s^\ell}\,(1+o(1)). \tag{27}$$

В третьем разделе второй главы при выводе верхней границы $C(s,\ell)$ мы сначала получаем границу типа Плоткина. Пусть X – произвольный код объема t и длины N, а $\mathcal{U}$, $|\mathcal{U}| = u$, и $\mathcal{V}$, $|\mathcal{V}| = v$, – два непересекающихся подмножества множества $[t]$. Для X, $\mathcal{U}$ и $\mathcal{V}$ определим множество строк кода, для которых выполнено следующее условие $x_i(j)=0$ для любого $j\in\mathcal{U}$ и $x_i(k)=1$ для любого $k\in\mathcal{V}$, которое обозначим через

$D_{u,v}(\mathcal{U},\mathcal{V},X)\subset[N]$. Далее мы рассматриваем среднюю (по всевозможным выборам упорядоченной пары $\mathcal{U}$ и $\mathcal{V}$) мощность величины $D_{u,v}(\mathcal{U},\mathcal{V},X)$ и исследуем максимальную среднюю мощность по всем кодам X объема t и длины N

$$\overline{D}_{u,v}(t,N)\triangleq\max_{X}\sum_{\substack{\mathcal{U}\in\mathcal{P}_u(t),\,\mathcal{V}\in\mathcal{P}_v(t),\\ \mathcal{U}\cap\mathcal{V}=\varnothing}}\frac{|D_{u,v}(\mathcal{U},\mathcal{V},X)|}{\binom{t}{u+v}\cdot\binom{u+v}{u}}.$$

Лемма 2.3.1. (Граница Плоткина) *Выполнено следующее асимптотическое неравенство*

$$\varlimsup_{t\to\infty}\frac{\overline{D}_{u,v}(t,N(t))}{N(t)}\leqslant\max_{0\leqslant z\leqslant 1}\{z^u(1-z)^v\}=\frac{u^uv^v}{(u+v)^{u+v}},$$

где $N(t)$ – произвольная целочисленная функция.

Определим минимальную длину почти свободных от перекрытий (s,ℓ,ε)-кодов, имеющих объем t, и обозначим ее через $N_\varepsilon(s,\ell,t)$. Далее мы доказываем вспомогательную лемму.

Лемма 2.3.2. *Для любого фиксированного $\delta>0$ и $t\geqslant t(\delta)$ длина ПСП (s,ℓ,ε)-кода*

$$N_{\varepsilon'}(s-u,\ell-v,t-u-v)\leqslant(1+\delta)\cdot N_\varepsilon(s,\ell,t)\cdot\frac{u^uv^v}{(u+v)^{u+v}},$$

где $\varepsilon'<C(\delta)\cdot\varepsilon$.

Верхняя теоретико-информационная граница для $C(s,1)$ представлена в следующей лемме.

Лемма 2.3.3. *Для любого фиксированного s выполнено неравенство*

$$C(s,1)\leqslant\frac{1}{s}.$$

Используя леммы 2.3.1, 2.3.2 и 2.3.3, мы доказываем следующую теорему.

Теорема 2.3.1. (Верхняя граница $\overline{C}(s,\ell)$). *Имеют место следующие два утверждения.*

1. *Для любого s и ℓ пропускная способность $C(s,\ell)$ ПСП (s,ℓ)-кодов*

$$C(s,\ell)\leqslant\overline{C}(s,\ell),\tag{28}$$

где $\overline{C}(s,\ell)$ определяется из начального условия

$$\overline{C}(s,1)\triangleq\frac{1}{s}\tag{29}$$

и рекуррентного уравнения

$$\overline{C}(s,\ell) = \min_{\substack{i\in[s-1]\\ j\in[\ell-1]}} \left\{ \overline{C}(s-i,\ell-j)\frac{i^i j^j}{(i+j)^{i+j}} \right\}. \tag{30}$$

2. *Для фиксированного параметра $\ell \geqslant 1$ и при $s \to \infty$ верхняя асимптотическая граница для $C(s,\ell)$ имеет вид*

$$C(s,\ell) \leqslant \frac{\ell^\ell}{e^{\ell-1}} \cdot \frac{1}{s^\ell}(1+o(1)). \tag{31}$$

В четвертом разделе второй главы мы приводим сводную таблицу с численными значениями для полученных нижних и верхних границ границ $C(s,\ell)$.

В пятом разделе второй главы мы сравниваем асимптотическую скорость $R(s,\ell)$ свободных от перекрытий кодов и пропускную способность $C(s,\ell)$ почти свободных от перекрытий кодов.

Третья глава состоит из трех разделов, посвященных алгоритмам поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$.

В первом разделе третьей главы даны основные определения, используемые в следующих разделах.

Во втором разделе третьей главы мы приводим детерминированный алгоритм адаптивного поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$. Приведенный алгоритм использует три следующих алгоритма:

1. бинарный поиск новой вершины, входящей в какое-либо ребро скрытого гиперграфа, по заданному вопросу;

2. исчерпывающий поиск ребер по вершинам, входящим в какие-либо ребра скрытого гиперграфа;

3. исчерпывающий поиск вопроса по найденным ребрам скрытого гиперграфа;

Используя полученные результаты, мы доказываем следующую теорему.

Теорема 3.2.3. *Скорость $R_h^a(s,\ell)$ удовлетворяет неравенству*

$$R_h^a(s,\ell) \geqslant \frac{1}{s\ell}.$$

В третьем разделе третьей главы мы доказываем существование двухступенчатой процедуры поиска скрытого гиперграфа из семейства $\mathcal{F}(t,s,\ell)$,

являющейся оптимальной в терминах пропускной способности. На первом шаге предложенного алгоритма мы показываем, что существует такой неадаптивный алгоритм, с помощью которого для почти всех гиперграфов $H = (V, E)$ из семейства $\mathcal{F}(t, s, \ell)$ можно получить разбиение множества вершин V на непересекающиеся доли $V_1, \ldots, V_s$ такие, что $\mathbf{e}_i \in V_i$, $i \in [s]$. При этом число вопросов на первом шаге является незначительным по сравнению с $\log_2 t$. Заметим, что существует двойственность между задачами поиска скрытого гиперграфа из семейств $\mathcal{F}(t, s, 1)$ и $\mathcal{F}(t, 1, s)$. Пользуясь этим фактом и классическим результатом $C_h^{na}(s, 1) = 1/s$, на втором шаге предложенного алгоритма мы ищем одновременно в каждой доле V_i скрытое ребро $\mathbf{e}_i$. Используя полученные результаты, мы доказываем следующую теорему.

Теорема 3.3.4. *Пропускная способность $C_h^{2\text{-}st}(s, \ell)$ удовлетворяет неравенству*

$$C_h^{2\text{-}st}(s, \ell) \geqslant \frac{1}{s\ell}.$$

Заключение

В диссертационной работе были исследованы и получены более точные нижние границы для асимптотической скорости $R(s, \ell)$ свободных от перекрытий кодов, а также доказаны новые оценки для пропускной способности $C(s, \ell)$ почти свободных от перекрытий кодов. Также было проведено исследование некоторых алгоритмов поиска скрытого гиперграфа. В частности, была найдена в точности асимптотическая скорость $R_h^a(s, \ell)$ адаптивного поиска скрытого гиперграфа и пропускная способность $C_h^{2\text{-st}}(s, \ell)$ двухступенчатой процедуры поиска скрытого гиперграфа.

Дальнейшее исследование темы диссертации может быть связано с доказательством или опровержением гипотезы, что пропускная способность неадаптивного поиска скрытого гиперграфа из семейства локализованных гиперграфов достигает теоретико-информационную границу. Кроме того, большой интерес представляет порядок главного члена асимптотики $R(s, 1)$ при $s \to \infty$. На текущий момент мы имеем две гипотезы, следующие из доказанных верхних и нижних границ: $1/s^2$ и $\ln s/s^2$.

Благодарности

Автор глубоко благодарен и признателен своему научному руководителю профессору Аркадию Георгиевичу Дьячкову за постановку интересных задач, обсуждение результатов и постоянное внимание к работе, а также слу-

шателям и докладчикам семинара по теории кодирования в ИППИ РАН за полезные замечания и предложения.

Работы автора по теме диссертации

[1] Дьячков А. Г., Воробьев И. В., Полянский Н. А., Щукин В. Ю., Границы скорости дизъюнктивных кодов // *Пробл. передачи информ.*, **50**:1 (2014), 31–63. [Дьячкову А. Г. принадлежат постановка задачи, теорема 3, предложения 1–3; Воробьеву И. В. — теоремы 1 и 6; Полянскому Н. А. — теоремы 2, 4 и 5; Щукину В. Ю. — теорема 7]

[2] Дьячков А. Г., Воробьев И. В., Полянский Н. А., Щукин В. Ю., Почти дизъюнктивные коды со списочным декодированием // *Пробл. передачи информ.*, **51**:2 (2015), 27–49. [Дьячкову А. Г. принадлежат постановка задачи и предложение 1; Воробьеву И. В. — предложение 2, пункты 1 (о пропускной способности) и 2 теоремы 4; Полянскому Н. А. — пример 1, предложение 3 и теорема 1; Щукину В. Ю. — теорема 2, пункты 1 (об экспоненте ошибки) и 3 теоремы 4]

[3] Полянский Н. А., Почти свободные от перекрытий коды // *Пробл. передачи информ.*, **52**:2 (2016), 46–60.

[4] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Almost Disjunctive List-Decoding Codes // *Proc. 14th Int'l Workshop «Algebraic and Combinatorial Coding Theory»*, Svetlogorsk, (2014), 115–126. [Дьячкову А. Г. принадлежит постановка задачи; Воробьеву И. В. — пункты 1 (о пропускной способности) и 2 теоремы 2, лемма 1; Полянскому Н. А. — раздел 3 (о конструкциях); Щукину В. Ю. — пункты 1 (об экспоненте ошибки) и 3 теоремы 2, лемма 2]

[5] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Bounds on the Rate of Superimposed Codes // *Proc. IEEE Int'l Symp. Inf. Theory*, Honolulu, (2014), 2341–2345. [Дьячкову А. Г. принадлежат постановка задачи, теорема 3 и предложения 1–3; Воробьеву И. В. — теоремы 1 и 6; Полянскому Н. А. — теоремы 2, 4 и 5; Щукину В. Ю. — теорема 7]

[6] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Almost Cover-Free Codes and Designs // *Proc. IEEE Int'l Symp. Inf. Theory*, Hong Kong, (2015), 2899–2903. [Дьячкову А. Г. принадлежат постановка задачи и предложение 1; Воробьеву И. В. — пример 1 и теоремы 1; Полянскому Н. А. — теоремы 2, 3; Щукину В. Ю. — пример 2, предложение 2 и 3]

[7] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Cover-Free Codes and Separating System Codes // *Proc. IEEE Int'l Symp. Inf. Theory*, Hong Kong, (2015), 2894–2898. [Дьячкову А. Г. принадлежат постановка задачи и предложения 1–2; Воробьеву И. В. — предложение 3, теоремы 1 и 1', пункты 1–3 теоремы 2, лемма 1; Полянскому Н. А. — лемма 2, пункты 4 и 6 теоремы 2; Щукину В. Ю. — лемма 3, пункт 5 теоремы 2]

[8] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., Symmetric Disjunctive List-Decoding Codes // *Proc. IEEE Int'l Symp. Inf. Theory*, Hong Kong, (2015), 2236–2240. [Дьячкову А. Г. принадлежат постановка задачи и предложение 3; Воробьеву И. В. — пункт 1 теоремы 2, следствие 1'; Полянскому Н. А. — теорема 1; Щукину В. Ю. — следствия 2' и 3', пункты 2 и 3 теоремы 2, теорема 3]

[9] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., On Multistage Learning a Hidden Hypergraph // *Proc. IEEE Int'l Symp. Inf. Theory*, Barcelona, 2016. [Дьячкову А. Г. принадлежат постановка задачи, разделы 1 и 2; Воробьеву И. В. — принадлежат разделы 4 и 5 (общий алгоритм и алгоритм поиска 2 дефектов); Полянскому Н. А. — раздел 3 (поиск s дефектов); Щукину В. Ю. — раздел 6 (оптимизация алгоритма)]

[10] D'yachkov A. G., Vorobyev I. V., Polyanskii N. A., Shchukin V. Yu., On a Hypergraph Approach to Multistage Group Testing Problems // *Proc. IEEE Int'l Symp. Inf. Theory*, Barcelona, 2016. [Дьячкову А. Г. принадлежит постановка задачи; Воробьеву И. В. — теорема 2; Полянскому Н. А. —- теорема 3; Щукину В. Ю. — теорема 1]