Московский Государственный Университет имени М. В. Ломоносова

На правах рукописи

Быстрыгова Анастасия Викторовна

Параметро-эффективная расшифровка булевых функций

Специальность 1.1.5 —
«Математическая логика, алгебра, теория чисел и дискретная математика»

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2022

Работа выполнена на кафедре математической теории интеллектуальных систем Механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М. В.Ломоносова».

Научный руководитель: **Гасанов Эльяр Эльдарович**
доктор физико-математических наук, профессор.

Официальные оппоненты: **Вороненко Андрей Анатольевич,**
доктор физико-математических наук, профессор,
МГУ имени М. В. Ломоносова, факультет вычислительной математики и кибернетики, кафедра математической кибернетики,
профессор.

Золотых Николай Юрьевич,
доктор физико-математических наук, доцент,
ФГАОУ ВО ННГУ им. Н.И. Лобачевского,
директор института информационных технологий, математики и механики.

Перпер Евгений Михайлович,
кандидат физико-математических наук,
ООО НКБ "НИР",
старший инженер-математик.

Защита состоится 23 декабря 2022 г. в 16:45 на заседании диссертационного совета МГУ.011.4(МГУ.01.17) при ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» по адресу: Российская Федерация, 119991, Москва, Ленинские горы, д. 1, МГУ имени М. В. Ломоносова, механико-математический факультет, аудитория 12-29.
E-mail: sbgashkov@gmail.com

С диссертацией можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВО МГУ имени М.В. Ломоносова по адресу: Москва, Ломоносовский проспект, д. 27 и на сайте ИАС «ИСТИНА»: https://istina.msu.ru/dissertations/513079128/

Автореферат разослан 22 ноября 2022 года.

Ученый секретарь
диссертационного совета
МГУ.011.4(МГУ.01.17),
д. ф.-м.н., профессор Гашков Сергей Борисович

Общая характеристика работы

Актуальность темы. Практически полвека назад активно стало развиваться направление математики под названием теория расшифровки (computational learning theory), основополагающими работами в которой стали работы Коробкова[1], Валианта[2], Англуин[3], Дамашке[4], Литлстоуна[5]. Эта область остается актуальной и по сей день, поскольку связана с восстановлением оптимальным образом информации об исследуемом объекте на основе частичных сведений о нем. Более формально, под расшифровкой функции из заданного класса F понимают игру между *учеником* и *учителем*, в которой учитель загадывает одну функцию из класса F, а ученик, зная этот класс F полностью, но не зная выбор учителя, задает учителю запросы разрешенного типа, получает ответы от учителя и на основе этих ответов восстанавливает какую-то информацию про загаданную функцию.

При этом, существует несколько моделей расшифровки, и выбор модели определяет то, как происходит процесс расшифровки и что является его результатом. Наиболее популярны две модели:

- модель точной расшифровки (exact learning)
  В этой модели ученик сам выбирает запросы и его цель — полностью восстановить вектор значений загаданной функции.
- модель вероятно примерно точной расшифровки (probably approximately correct learning, PAC)
  В этой модели не ученик выбирает запрос, запрос выбирается в соответствии с заданным на множестве всех запросов вероятностным распределением. Цель — восстановить вектор значений загаданной функции так, чтобы вероятность ошибки была небольшой.

Чтобы оценить насколько быстро можно расшифровать функции из того или иного класса, вводят понятие *сложности расшифровки* как максимальное число запросов, которое надо задать учителю для расшифровки самой “плохой” функции. Иными словами, ученик выбирает “лучшую” стратегию восстановления функции, затем проверяется, а сколько запросов потребуется задать ученику, использующему эту стратегию, чтобы восстановить каждую функцию из класса, за сложность расшифровки принимают максимум среди этих значений.

---

[1] *Коробков, В. К.* О монотонных функциях алгебры логики / В. К. Коробков // Сб. Проблемы кибернетики. Т. 13. Москва : Наука, 1965. С. 5—28.

[2] *Valiant, L. G.* A theory of the learnable / L. G. Valiant // STOC '84. 1984. P. 436—445.

[3] *Angluin, D.* Queries and Concept Learning / D. Angluin // Machine Learning. 1988. Vol. 2. P. 319—342.

[4] *Damaschke, P.* Adaptive Versus Nonadaptive Attribute-Efficient Learning / P. Damaschke // Machine Learning. 2000. Vol. 41. P. 197—215.

[5] *Littlestone, N.* Learning Quickly When Irrelevant Attributes Abound: A New Linear-Threshold Algorithm / N. Littlestone // Machine Learning. 1988. Vol. 2. P. 285—318.

Довольно часто возникающие на практике функции зависят от большого числа переменных, но лишь небольшая их часть существенно влияет на поведение функции. Поэтому становится актуальной *параметро-эффективная расшифровка* данных классов, в которой при разработке алгоритмов восстановления векторов столбцов значений функций весомым образом используется факт, что существенных переменных очень мало.

Помимо того, что при расшифровке важен выбор модели расшифровки, учитывание факта, что число существенных параметров сильно мало по сравнению с общим числом параметров, также значителен и выбор типа(ов) используемых при расшифровке запросов. Чаще встречаются:

- запросы на значение, или membership query (Коробков[6], Золотых[7], Хофмейстер[8], Дамашке[9], Осокин[10], Уэхара и др.[11]): ученик выбирает набор, учитель говорит значение функции на выбранном наборе;
- запросы на сравнение (Гасанов[12], Хегай[13]): ученик выбирает пару наборов, а учитель возвращает в ответ знак разности значений функций на этих наборах;

[6] *Коробков, В. К.* О монотонных функциях алгебры логики / В. К. Коробков // Сб. Проблемы кибернетики. Т. 13. Москва : Наука, 1965. С. 5—28.

[7] *Золотых, Н. Ю.* Расшифровка пороговых функций k-значной логики / Н. Ю. Золотых, В. Н. Шевченко // Дискретный анализ и исследование операций. 1995. Т. 2, № 3. С. 18—23.

[8] *Hofmeister, T.* An Application of Codes to Attribute-Efficient Learning / T. Hofmeister // Proceedings of the 4th European Conference on Computational Learning Theory. 1999. P. 101—110. (EuroCOLT '99).

[9] *Damaschke, P.* Adaptive Versus Nonadaptive Attribute-Efficient Learning / P. Damaschke // Machine Learning. 2000. Vol. 41. P. 197—215.

[10] *Осокин, В. В.* О параллельной параметро-эфективной расшифровке псевдо-булевых функций / В. В. Осокин // Интеллектуальные системы. 2010. Т. 14, № 1—4. С. 429—458; *Осокин, В. В.* О расшифровке монотонных булевых функций с несущественными переменными / В. В. Осокин // Дискретная математика. 2010. Т. 22, № 3. С. 134—145.

[11] *Uehara, R.* Optimal Attribute-Efficient Learning of Disjunction, Parity and Threshold Functions / R. Uehara, K. Tsuchida, I. Wegener // Proceedings of the Third European Conference on Computational Learning Theory. 1997. P. 171—184. (EuroCOLT '97).

[12] *Гасанов, Э. Э.* Расшифровка линейных функций ранжирования / Э. Э. Гасанов // Материалы XI Международного семинара «Дискретная математика и ее приложения» (Москва, 18-23 июня 2012 г.) 2012. С. 332—334.

[13] *Хегай, С. И.* Расшифровка полиномиальных функций ранжирования / С. И. Хегай // Интеллектуальные системы. Теория и приложения. 2015. Т. 19, № 1. С. 213—230.

– запросы на ограниченную эквивалентность, или equivalence query (Англуин[14], Бертони[15], Бшоути и др.[16]): ученик выбирает функцию h из рассматриваемого класса, учитель отвечает "ДА", если $f \equiv h$, иначе выдает набор b, на котором значения функций h, f отличаются;
– запросы на расширенную эквивалентность, или extended equivalence query (Англуин[17]): ученик выбирает булеву функцию h, которая необязательно принадлежит рассматриваемому классу, учитель отвечает "ДА", если $f \equiv h$, иначе выдает набор b, на котором значения функций h, f отличаются;
– superset (subset) query (Англуин[18], Бшоути и др.[19]): ученик выбирает функцию h, учитель отвечает "ДА", если $f \Rightarrow h$ ($h \Rightarrow f$), иначе выдает набор b такой, что $h(b) \neq f(b) = 1$ ($h(b) \neq f(b) = 0$).

В теории расшифровки функций привычной практикой стало рассмотрение задачи расшифровки одного и того же класса функций разными типами запросов или даже разными комбинациями нескольких типов запросов (Англуин[20], Вороненко и Чистиков[21], Бертони и др.[22]). В 2004 году Англуин[23] ввела обозначения для запросов на значение MQ, на ограниченную EQ и расширенную эквивалентность XEQ, которые и используются в диссертационной работе.

Данная диссертационная работа посвящена некоторым вопросам параметро-эффективной точной расшифровки булевых функций разными типами запросов. В первой главе работы описываются классы функций

[14] *Angluin, D.* Queries and Concept Learning / D. Angluin // Machine Learning. 1988. Vol. 2. P. 319—342; *Angluin, D.* Queries Revisited / D. Angluin // Theoretical Computer Science. 2004. Vol. 313, no. 2. P. 175—194.

[15] *Bertoni, A.* Efficient learning with equivalence queries of conjunctions of modulo functions / A. Bertoni, N. Cesa-Bianchi, G. Fiorino // Information Processing Letters. 1995. Vol. 56, no. 1. P. 15—17.

[16] Oracles and Queries That Are Sufficient for Exact Learning / N. H. Bshouty [et al.] // Journal of Computer and System Sciences. 1996. Vol. 52, no. 3. P. 421—433.

[17] *Angluin, D.* Queries Revisited / D. Angluin // Theoretical Computer Science. 2004. Vol. 313, no. 2. P. 175—194.

[18] *Angluin, D.* Queries and Concept Learning / D. Angluin // Machine Learning. 1988. Vol. 2. P. 319—342.

[19] Oracles and Queries That Are Sufficient for Exact Learning / N. H. Bshouty [et al.] // Journal of Computer and System Sciences. 1996. Vol. 52, no. 3. P. 421—433.

[20] *Angluin, D.* Queries and Concept Learning / D. Angluin // Machine Learning. 1988. Vol. 2. P. 319—342; *Angluin, D.* Queries Revisited / D. Angluin // Theoretical Computer Science. 2004. Vol. 313, no. 2. P. 175—194.

[21] *Вороненко, А. А.* Расшифровка бесповторных функций запросами тождественности / А. А. Вороненко, Д. В. Чистиков // Проблемы теоретической кибернетики. Материалы XVI Международной конференции. 2011. С. 105—108.

[22] *Bertoni, A.* Efficient learning with equivalence queries of conjunctions of modulo functions / A. Bertoni, N. Cesa-Bianchi, G. Fiorino // Information Processing Letters. 1995. Vol. 56, no. 1. P. 15—17.

[23] *Angluin, D.* Queries Revisited / D. Angluin // Theoretical Computer Science. 2004. Vol. 313, no. 2. P. 175—194.

и типы запросов, для которых исследуется вопрос сложности расшифровки. В следующих трех ее главах приводятся результаты, полученные в результате исследования.

Вторая глава диссертационной работы основана на работах [3; 4] и посвящена исследованию параметро-эффективной расшифровки класса функций фиксированного веса для каждого из следующих четырех типов запросов в отдельности: на значение, на сравнение, на расширенную эквивалентность, на ограниченную эквивалентность. Для этого класса уже проведено исследование[24] функции Шеннона мощности плоских схем, реализующих такие функции. Но с точки зрении вопросов сложности расшифровки данный класс ранее никем не исследовался, если не брать в расчет результат Англуин[25] для функций веса 1 для трех из упомянутых типов запросов.

Третья и четвертая главы диссертационной работы, результаты которых опубликованы в работах [2] и [1; 5] соответственно, посвящены вопросам сложности расшифровки замкнутых классов Поста. Эти классы стали предметом изучения в разных задачах с 1930–1950 годов после того как Пост описал (рис. 1) все замкнутые классы двузначной логики в своих работах[26]. К настоящему времени уже известны результаты о сложности автоматной реализации этих классов[27], получены все спектры (множества длин базисов)[28], приведены оценки слоистости[29]. Помимо этого, исследован порядок функции Шеннона средней и максимальной мощности плоских схем для всех замкнутых классов[30] и рассмотрен вопрос о мощности генерирующих множеств по операциям из классов решетки Поста[31].

Отдельное направление исследований было связано с расшифровкой функций из этих классов запросами на значение. Одним из первых классов,

---

[24] *Калачев, Г. В.* Оценки мощности плоских схем, реализующих функции с ограниченным числом единиц / Г. В. Калачев // Интеллектуальные системы. Теория и приложения. 2017. Т. 21, № 1. С. 28—96.

[25] *Angluin, D.* Queries and Concept Learning / D. Angluin // Machine Learning. 1988. Vol. 2. P. 319—342.

[26] *Post, E.* Determination of all closed systems of truth tables / E. Post // Bull. Amer. Math. Soc. 1920; *Post, E.* Two-valued iterative systems of mathematical logic / E. Post // Annals of Mathematics studies, Princeton Univ. Press, Princeton. 1941. No. 5.

[27] *Кибкало, М. А.* Об автоматной сложности классов Поста булевых функций / М. А. Кибкало // Интеллектуальные системы. 2010. Т. 15, № 1—4. С. 379—400.

[28] *Блохина, Г. Н.* О спектрах классов Поста булевских функций / Г. Н. Блохина, В. Б. Кудрявцев // Интеллектуальные системы. 2010. Т. 14, № 1—4. С. 279—298.

[29] *Членова, Т. С.* О слоистости замкнутых классов булевых функций и функций k-значной логики / Т. С. Членова // Интеллектуальные системы. Теория и приложения. 2014. Т. 18, № 1. С. 259—262.

[30] *Калачев, Г. В.* Об оценках мощности плоских схем для замкнутых классов булевых функций / Г. В. Калачев // Интеллектуальные системы. Теория и приложения. 2016. Т. 20, № 3. С. 52—57.

[31] *Комков, С. А.* Мощности генерирующих множеств по операциям из классов решетки Поста / С. А. Комков // Дискретная математика. 2018. Т. 30, № 1. С. 19—38.

расшифровкой функций из которого занялись исследователи, стал класс монотонных функций. Задачу расшифровки этого класса в разных версиях рассматривали в своих работах Дамашке[32], Коробков[33], Ансель[34], Осокин[35] и Селезнева с Лю[36]. Ансель предложил алгоритм, благодаря которому он получил верхнюю оценку сложности расшифровки монотонных функций от n переменных, совпадающую с нижней оценкой, доказанной ранее Коробковым, и равную

$$C_n^{[n/2]} + C_n^{[n/2]+1}.$$

Селезенева с Лю показали, что эта оценка сохраняется даже в случае возможного одного неверного ответа учителя.

Осокина интересовал вопрос сложности расшифровки монотонных функций от n переменных, где не более k переменных существенные. Им в 2010 году был получен порядок сложности расшифровки монотонных функций

$$\frac{2^k}{\sqrt{k}} + k \log n.$$

Дамашке помимо расшифровки монотонных функций рассматривал и расшифровку всех функций алгебры логики в целом (класс C_1 решетки замкнутых классов Поста на рис. 1). Его работы показали, что задача расшифровки функций из замкнутых классов Поста нередко сводится к задаче построения binary covering array для заданных чисел: арности n, верхней оценки на число существенных переменных k.

Binary covering array являются частным случаем ортогональных массивов. Сам термин "covering array" был введен в 1993 году Слоаном[37] и с тех пор прижился. В русскоязычной литературе этот объект освещен мало. В своей работе[38] 2011 года авторы предлагают называть его *покрывающим набором*, но кажется более естественным называть его *покрывающей*

[32] *Damaschke, P.* Adaptive Versus Nonadaptive Attribute-Efficient Learning / P. Damaschke // Machine Learning. 2000. Vol. 41. P. 197—215; *Damaschke, P.* On parallel attribute-efficient learning / P. Damaschke // Journal of Computer Science. 2003. Vol. 67. P. 46—62.

[33] *Коробков, В. К.* О монотонных функциях алгебры логики / В. К. Коробков // Сб. Проблемы кибернетики. Т. 13. Москва : Наука, 1965. С. 5—28.

[34] *Ансель, Ж.* О числе монотонных булевых функций от n переменных / Ж. Ансель // Кибернетический сборник. Новая серия. Т. 5. Мир, 1968. С. 53—57.

[35] *Осокин, В. В.* О расшифровке монотонных булевых функций с несущественными переменными / В. В. Осокин // Дискретная математика. 2010. Т. 22, № 3. С. 134—145.

[36] *Селезнева, С. Н.* Расшифровка монотонных функций с исправлением одной ошибки / С. Н. Селезнева, Ю. Лю // Дискретная математика. 2019. Т. 31, № 4. С. 53—69.

[37] *Sloane, N. J. A.* Covering arrays and intersecting codes / N. J. A. Sloane // Journal of Combinatorial Designs. 1993. Vol. 1. P. 51—63.

[38] *Кулямин, В. В.* Обзор методов построения покрывающих наборов / В. В. Кулямин, А. А. Петухов // Программирование. Т. 37. Москва : Российская академия наук, 2011. С. 3—41.

матрицей, поэтому это название и используется в тексте диссертационной работы.

Бинарная покрывающая матрица (binary covering array) — это бинарная матрица, у которой n столбцов, обладающая свойством, что если зафиксировать любые k столбцов, то в этих зафиксированных столбцах будут содержаться все 2^k двоичных наборов-строк.

Изучение этих матриц представляет интерес в силу их разных применений. Причем в приложениях можно не ограничиваться алфавитом $\{0, 1\}$, а брать более мощный алфавит. Наиболее известное применение покрывающих матриц — это софтверное и хардверное тестирование, предложенное[39] еще в 1997 году. Предположим, у программы n входных параметров, где каждый аргумент может принимать v значений. Тогда рассмотрим покрывающую матрицу с n столбцами, где каждый элемент принимает значение от 0 до $v-1$ включительно и при фиксации любых k столбцов в строках встречаются все v^k комбинаций. Каждую строку такой матрицы можно рассматривать как тест. Благодаря такой матрице, можно проверить корректность работы программы на разных комбинациях любых k параметров. Ясно, что чем меньше строк в матрице, тем меньше тестов придется сделать.

Другое необычное приложение оценок на число строк покрывающих матриц заметил Хартман[40], изучая задачу о слепых роботах на прямой (blind dyslectic synchronized robots on a line), которую ранее рассматривала в своей работе[41] Лим. Благодаря своему замечанию он сумел понизить имеющуюся тогда оценку[42] для этой задачи на $]\log_2 n[$.

Как выяснилось, и в расшифровке функций находят свое применение покрывающие матрицы. Дамашке показал[43], что булеву функцию, зависящую от n переменных, не более k из которых существенные, можно расшифровать за не более $\alpha(n,k) + k\log n$ запросов на значение, также им была приведена тривиальная нижняя оценка $\alpha(n,k)$, где $\alpha(n,k)$ — минимальное число строк в бинарной покрывающей матрице для чисел n, k.

Хотелось бы оценить число $\alpha(n,k)$, но, к сожалению, на данный момент неизвестна асимптотика, или даже порядок этой функции, хотя вопрос построения бинарных покрывающих матриц для n, k с наименьшим

[39] The AETG System: An Approach to Testing Based on Combinatorial Design / D. M. Cohen [et al.] // IEEE TRANSACTIONS ON SOFTWARE ENGINEERING. 1997. Vol. 23, no. 7. P. 437—444.

[40] *Hartman, A.* Software and Hardware Testing Using Combinatorial Covering Suites / A. Hartman // Graph Theory, Combinatorics and Algorithms. Vol. 34. 2006. P. 237—266. (Operations Research/Computer Science Interfaces Series).

[41] *Lim, W. S.* Minimax rendezvous on the line / W. S. Lim, S. Alpern // SIAM J. Control and Optim. 1996. Vol. 34. P. 1650—1665.

[42] *Gal, S.* Rendezvous search on a line / S. Gal // Operations Research. 1999. Vol. 47. P. 974—976.

[43] *Damaschke, P.* Adaptive Versus Nonadaptive Attribute-Efficient Learning / P. Damaschke // Machine Learning. 2000. Vol. 41. P. 197—215.

числом строк $\alpha(n,k)$ изучается давно (Клейтман[44], Гаргано[45], Слоун[46], Годбол[47], Лоуренс[48], Саркар[49], Дас[50]), но пока лишь получены некие неравенства и соотношения.

1. В 1993 году получена[51] асимптотическая оценка при $n \to \infty$

$$\alpha(n,2) = \log_2 n(1+o(1)).$$

2. В 1996 году Годболу, Скипперу и Санли[52] удалось получить следующую верхнюю оценку для случая $k \geq 2, n \to \infty$

$$\alpha(n,k) \leq (1+o(1)))\frac{k-1}{\log_2 \frac{2^k}{2^k-1}} \cdot \log_2 n.$$

   В 2017 году было показано[53], что при $k \to \infty$ правая часть асимптотически равна $2^k(k-1)\ln 2 \cdot \log_2 n$.
3. $\alpha(n,k) \geq 2\alpha(n-1,k-1)$.
4. В 2016 году коллектив авторов[54] доказал, что для $k \geq 2$ при $n \to \infty$ верна нижняя оценка

$$\alpha(n,k) \geq 2^{k-2} \cdot \alpha(n-k+2,2) = 2^{k-2}\log_2(n-k+2)(1+o(1)).$$

5. $\alpha(n,1) = 2$ для любого натурального n.

---

[44] *Kleitman, D. J.* Families of k - independent sets / D. J. Kleitman, J. Spencer // Discrete Mathematics. 1973. Vol. 6. P. 255—262.

[45] *Gargano, L.* Sperner capacities / L. Gargano, J. Korner, U. Vaccaro // Graph. Combinator. 1993. Vol. 9. P. 31—46.

[46] *Sloane, N. J. A.* Covering arrays and intersecting codes / N. J. A. Sloane // Journal of Combinatorial Designs. 1993. Vol. 1. P. 51—63.

[47] *Godbole, A.* t-Covering Arrays: Upper Bounds and Poisson Approximations / A. Godbole, D. Skipper, R. Sunley // Combinatorics, Probability & Computing. 1996. Vol. 5. P. 105—117.

[48] A survey of Binary Covering Arrays / J. Lawrence [et al.] // The electronic journal of combinatorics. 2011. Vol. 18, no. 1. P. 1—30.

[49] Partial Covering Arrays: Algorithms and Asymptotics / K. Sarkar [et al.] // International Workshop on Combinatorial Algorithms IWOCA 2016: Combinatorial Algorithms. 2016. P. 437—448.

[50] *Das, S.* A Semi-Random Construction of Small Covering Arrays / S. Das, T. Mészáros. 2017.

[51] *Gargano, L.* Sperner capacities / L. Gargano, J. Korner, U. Vaccaro // Graph. Combinator. 1993. Vol. 9. P. 31—46.

[52] *Godbole, A.* t-Covering Arrays: Upper Bounds and Poisson Approximations / A. Godbole, D. Skipper, R. Sunley // Combinatorics, Probability & Computing. 1996. Vol. 5. P. 105—117.

[53] *Das, S.* A Semi-Random Construction of Small Covering Arrays / S. Das, T. Mészáros. 2017.

[54] Partial Covering Arrays: Algorithms and Asymptotics / K. Sarkar [et al.] // International Workshop on Combinatorial Algorithms IWOCA 2016: Combinatorial Algorithms. 2016. P. 437—448.

Помимо классов монотонных функций и класса всех булевых функций внимание исследователей с точки зрения расшифровки привлекали также линейные функции, логические суммы и селекторы. В 1997 году существенно в вопросе изучения сложности расшифровки этих классов продвинулся коллектив авторов Уэхара, Цутида, Вегенер[55]. Они показали, что сложность точной расшифровки запросами на значение класса функций арности n, равные логической сумме k своих переменных (класс S_1 на рис. 1), не меньше $\rceil \log_2 C_n^k \lceil$ и не больше $k\rceil \log(n/k)\lceil + 2k - 2$. Более того, они разработали алгоритмы расшифровки линейных функций с 1, 2, 3 существенными переменными и нулевым свободным членом, требующие не более $\rceil \log_2 n[$, $3\rceil \log_2 n[-2$ и $4\rceil \log_2 n[-3$ запросов соответственно для точной расшифровки функции. Заметим, что линейные функции с ровно одной существенной переменной и нулевым свободным членом и есть селекторы, поэтому авторами была получена точная оценка сложности расшифровки класса O_1 решетки Поста (рис. 1).

Случай линейных функций с произвольным числом существенных переменных был рассмотрен авторами в модели PAC. Ими было показано, что для класса линейных функций арности n, у которых ровно k существенных переменных, существует рандомизированный алгоритм расшифровки с нулевой ошибкой, сложность которого равна $k \log \frac{n}{k} + O(k)$ запросов. Вопрос точной расшифровки этого класс смог закрыть Хофмейстер[56] в 1999 году. Для получения верхней оценки $k \log_2 n + k$ сложности точной расшифровки он применил теорию построения линейных кодов и получил асимптотику сложности расшифровки функций класса L_3 решетки Поста, у которых из n переменных не более k являются существенными.

Таким образом, по задаче расшифровки запросами на значение функций из классов решетки Поста было много работ, поэтому вполне обоснована необходимость собрать все имеющиеся результаты и привести оценки для ранее не освещавшихся классов (классов самодвойственных функций и классов "счетной этажерки"), чтобы понять, насколько сложна расшифровка функций из разных классов, если в качестве запросов используются запросы на значение. Этому посвящена третья глава диссертационной работы. А четвертая же освещает данную задачу для запросов на сравнение. Запросы на сравнение были введены в литературу Гасановым сравнительно недавно[57], поэтому неудивительно, что еще не исследованы

[55] *Uehara, R.* Optimal Attribute-Efficient Learning of Disjunction, Parity and Threshold Functions / R. Uehara, K. Tsuchida, I. Wegener // Proceedings of the Third European Conference on Computational Learning Theory. 1997. P. 171—184. (EuroCOLT '97).

[56] *Hofmeister, T.* An Application of Codes to Attribute-Efficient Learning / T. Hofmeister // Proceedings of the 4th European Conference on Computational Learning Theory. 1999. P. 101—110. (EuroCOLT '99).

[57] *Гасанов, Э. Э.* Расшифровка линейных функций ранжирования / Э. Э. Гасанов // Материалы XI Международного семинара «Дискретная математика и ее приложения» (Москва, 18-23 июня 2012 г.) 2012. С. 332—334.

ни классы решетки Поста, ни класс функций ограниченного веса с точки зрения сложности точной расшифровки их запросами на сравнение. Четвертая глава диссертационной работы посвящена закрытию этого пробела.

Целью данной работы является изучение в рамках модели точной расшифровки сложности параметро-эффективной расшифровки замкнутых классов Поста и класса функций ограниченного веса. Для класса функций ограниченного веса необходимо получить оценки сложности расшифровки для четырех типов запросов в отдельности: на значение, на сравнение, на расширенную или ограниченную эквивалентность. Для всех замкнутых классов Поста необходимо получить эти оценки для двух типов запросов в отдельности: на значение и сравнение. При этом в случае класса функций ограниченного веса ученику известна арность функции и верхняя оценка на количество единиц в векторе значений функции, которых значительно меньше, чем длина вектора значений. В случае замкнутых классов Поста ученику известна арность функции и верхняя оценка на количество существенных переменных, причем существенных переменных сильно меньше общего числа переменных.

Для достижения поставленной цели необходимо было решить следующие **задачи**:

1. Получить точные значения сложности расшифровки класса функций ограниченного веса для трех типов запросов в отдельности: на значение, на расширенную и ограниченную эквивалентность.
2. Оценить порядок сложности расшифровки класса функций ограниченного веса запросами на сравнение.
3. Оценить характер сложности расшифровки замкнутых классов Поста запросами на значение.
4. Оценить характер сложности расшифровки замкнутых классов Поста запросами на сравнение.

Научная новизна:

1. Впервые получены точные значения сложности расшифровки класса функций ограниченного веса для трех типов запросов в отдельности: на значение, на расширенную и ограниченную эквивалентность.
2. Впервые получены точные значения сложности расшифровки запросами на сравнение класса функций малого веса: 1, 2, 3.
3. Впервые получена практически точная оценка сложности расшифровки запросами на сравнение классов функций веса: ограниченного снизу нулем и ограниченного снизу единицей.
4. Впервые получен порядок сложности расшифровки запросами на сравнение класса функций ограниченного веса в случае, когда растет арность функции, а ее вес не меняется.

5. Впервые получены оценки сложности расшифровки запросами на значение замкнутых классов самодвойственных функций и классов “счетной этажерки” решетки Поста.
6. Впервые получены оценки сложности расшифровки запросами на сравнение всех замкнутых классов решетки Поста.

Теоретическая и практическая значимость. Диссертационная работа в основном носит теоретический характер. Результаты работы могут быть использованы в дальнейшем теоретическом исследовании оценок сложности расшифровки других классов булевых функций. Тем не менее приведенные в работе утверждения могут быть также применены на практике в задачах восстановления информации об объекте из частичных сведений о нем, если известно, какими свойствами обладает этот объект.

Методология и методы исследования. В работе используются методы дискретного анализа, комбинаторики, теории графов, а также математического анализа.

Основные положения, выносимые на защиту. На защиту выносятся обоснование актуальности проведенного исследования и его научной новизны, цели и поставленные задачи, методы исследования, примененные для получения результатов, а также следующие положения, которые подтверждаются результатами исследований, представленными в Заключении диссертации.

1. Значения сложности расшифровки класса функций ограниченного веса для трех типов запросов в отдельности: на значение, на расширенную и ограниченную эквивалентность.
2. Значения сложности расшифровки запросами на сравнение класса функций малого веса: 1, 2, 3.
3. Оценки сложности расшифровки запросами на сравнение класса функций веса, ограниченного сверху произвольным числом, а снизу либо единицей, либо нулем.
4. Порядок сложности расшифровки запросами на сравнение класса функций ограниченного веса в случае, когда арность функции растет, но вес не меняется.
5. Оценки сложности расшифровки запросами на значение замкнутых классов самодвойственных функций и классов “счетной этажерки” решетки Поста.
6. Оценки сложности расшифровки запросами на сравнение всех замкнутых классов решетки Поста.

Достоверность полученных результатов обеспечивается строгими математическими доказательствами. Результаты работы прошли апробацию на всероссийских и международных научных конференциях, научных

семинарах и опубликованы в рецензируемых научных журналах. Результаты других авторов, используемые в тексте данной диссертационной работы, приводятся с указанием выходных данных публикаций.

Апробация работы. Основные результаты работы докладывались на научном семинаре "Математические вопросы кибернетики" кафедр дискретной математики и математической теории интеллектуальных систем механико-математического факультета и кафедры математической кибернетики факультета вычислительной математики и кибернетики МГУ им. М. В. Ломоносова (2022), а также следующих семинарах механико-математического факультета МГУ им. М. В. Ломоносова: "Теория автоматов" под руководством академика, проф., д.ф.-м.н. В. Б. Кудрявцева (2020), "Вопросы сложности алгоритмов поиска" под руководством проф., д.ф.-м.н. Э. Э. Гасанова (2016–2022), "Кибернетика и информатика" под руководством академика, проф., д.ф.-м.н. В. Б. Кудрявцева и к.ф-м.н, с.н.с. А. В. Галатенко (2018).

Помимо этого, результаты работы были представлены на международной научной конференции студентов и аспирантов "Ломоносов" (2020) и конференции "Ломоносовские чтения", секция "Математика" (2016, 2018–2021), а также на X международной конференции "Дискретные модели в теории управляющих систем" (Красновидово, 2018), семинаре компании Huawei Moscow Research Center "Intelligent Systems Workshop" (г. Москва, 2020), XIX международной конференции "Проблемы теоретической кибернетики" (г. Казань, 2021).

Личный вклад. Все приводимые в работе результаты, за исключением специально выделенных, сформулированы и доказаны автором лично.

Публикации. Соискатель имеет 5 опубликованных работ [1—5], 5 из которых по теме диссертации, из них 2 опубликованы в периодических научных журналах, индексируемых Web of Science, Scopus и RSCI [2; 4], 3 опубликованы в рецензируемом научном издании из дополнительного списка, утвержденного ученым советом МГУ, в котором могут быть опубликованы научные результаты диссертаций по направлению физико-математические науки [1; 3; 5]. Работ, написанных в соавторстве, нет.

Диссертационная работа была выполнена в рамках работы Междисциплинарной научно-образовательной школы Московского университета "Мозг, когнитивные системы, искусственный интеллект".

Краткое содержание работы.

Во **введении** обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, приводится обзор научной литературы по изучаемой проблеме, формулируется цель, ставятся задачи работы, излагается научная новизна и научная значимость представляемой работы.

Первая глава состоит из трех разделов, в которых вводятся обозначения и определения, используемые на протяжении всей работы. В первом ее разделе перечисляются значения как распространенных обозначений (например, символы $|, \&$) для того, чтобы избежать неоднозначного их трактования в результатах, так и вводимых в работе функций $G(k,m) = k \cdot [m/(k+1)] + (m \bmod (k+1))$ и $S_{n,k} = \max_{p \in \mathbb{N}, 1 \leq p < k} (2^p - 1)\alpha(n-p, k-p)$, где $\alpha(n,k)$ — число строк в бинарных покрывающих матрицах, про которые говорилось выше.

Во втором разделе первой главы дается определение используемых в работе типов запросов: *запросы на значение (MQ), запросы на сравнение (CQ), запросы на расширенную эквивалентность (XEQ), запросы на ограниченную эквивалентность (EQ)*, а также приводится определение понятия *сложность расшифровки* $\varphi_T(M,n)$ *запросами типа* T, где $T \in \{MQ, CQ, XEQ, EQ\}$, а M — множество булевых функций арности n.

В последнем разделе первой главы приводятся описания классов функций, расшифровка которых является целью диссертационной работы. В этом разделе вводится обозначение $F(n,k,i)$ для класса функций ограниченного веса, то есть множества булевых функций арности n, вес которых лежит в диапазоне $[i,k]$, $k \in (0, 2^n], i \in [0, 2^n)$, $i \leq k$. Помимо этого, в разделе предоставляется словесное описание всех замкнутых классов Поста (рис. 1) и уточняется, что классы из "правой" половины решетки Поста заведомо опускаются из рассмотрения, так как они являются двойственными к классам из "левой" половины, следовательно задача расшифровки классов из "правой" половины сводится к задаче расшифровки классов из "левой" половины. Также в этом разделе для удобства вводятся обозначение $\varphi_T(F,n,k,i)$ сложности расшифровки запросами типа T класса функций ограниченного веса и обозначение $\varphi_T(R,n,k)$ сложности расшифровки запросами типа T класса R, где R — один из замкнутых классов решетки Поста, а $R(n,k)$ — все функции из R, у которых арность n и не более k существенных переменных. Под $\varphi_T(F,n,k,i)$ понимается $\varphi_T(F(n,k,i),n)$, под $\varphi_T(R,n,k)$ — $\varphi_T(R(n,k),n)$.

В следующих трех главах излагаются результаты решения задач, поставленных в рамках диссертационной работы.

Во **второй главе** рассматривается точная расшифровка класса функций ограниченного веса для четырех типов запросов: на значение, на расширенную и ограниченную эквивалентность, а также на сравнение.

В первых трех разделах приводится доказательство теорем с точными значениями сложности расшифровки упомянутого класса для первых трех типов запросов.

Теорема 1. *Сложность расшифровки класса* $F(n,k,i)$ *запросами на значение равна*

$$\varphi_{MQ}(F,n,k,i) = \begin{cases} 2^n - 1 & \text{при } i = k, \\ 2^n & \text{при } i < k. \end{cases}$$

Теорема 2. *Сложность расшифровки класса* $F(n,k,i)$ *запросами на расширенную эквивалентность равна*

$$\varphi_{XEQ}(F,n,k,i) = \min(k, 2^n - i).$$

Теорема 3. *Сложность расшифровки класса* $F(n,k,i)$ *запросами на ограниченную эквивалентность равна*

$$\varphi_{EQ}(F,n,k,i) = \begin{cases} k & \text{при } i = 0, \\ 2^n - 1 & \text{при } 0 < i = k, \\ 2^n & \text{при } 0 < i < k < 2^n, \\ 2^n - i & \text{при } 0 < i < k = 2^n. \end{cases}$$

Из этих оценок видно, что для класса функций ограниченного веса лучшими с точки зрения наименьшей сложности расшифровки являются запросы на расширенную эквивалентность. Между тем использовать запросы на значение и запросы на ограниченную эквивалентность для этого класса нецелесообразно в силу того, что сложность расшифровки этими типами запросов почти всегда схожа с восстановлением всего вектора значений функций.

Вторую главу завершает раздел с оценками сложности расшифровки класса функций ограниченного веса запросами на сравнение.

В этом разделе вводятся понятия *класс можно (нельзя) расшифровать запросами на сравнение* и доказывается критерий того, когда класс булевых функций расшифровать можно, то есть в каком случае существует алгоритм расшифровки запросами на сравнение, который сможет восстановить функцию, загаданную учителем, независимо от того, какая функция им выбрана.

Теорема 4. *Класс булевых функций расшифровать запросами на сравнение нельзя тогда и только тогда, когда ему принадлежат обе константные функции* $0, 1$.

Далее в разделе приводится следующая верхняя оценка для функций фиксированного веса.

Теорема 5. *Пусть* $k \leq 2^{n-1}$ *и для целых положительных* $x_m, x_{m+1}, \ldots, x_{k-1}, x_k$, *где* $m = \left](k+1)/2\right[$, *верно равенство*

$$2^n = m \cdot x_m + (m+1) \cdot x_{m+1} + \ldots + (k-1) \cdot x_{k-1} + k \cdot x_k.$$

Тогда справедлива следующая верхняя оценка

$$\varphi_{CQ}(F,n,k,k) \le 2^n - (x_m + x_{m+1} + \ldots + x_{k-1} + x_k) + [\max(x_m, x_{m+1}, \ldots, x_{k-1}, x_k)/2].$$

Следующее следствие получается после подстановки определенных значений $x_m, x_{m+1}, \ldots, x_k$ в последнюю теорему.

Следствие 1. *Пусть* $3 \le k \le 2^{n-1}, m =](k+1)/2[, s = m + (m+1) + \ldots + (k-1) + k$, *верно равенство* $2^n = s \cdot q + r, r \in [0,s), q \ge m$, q, r — *целые положительные числа. Тогда справедлива следующая верхняя оценка*

$$\varphi_{CQ}(F,n,k,k) \le 2^n - (k-m+1)q - c + \Big[0.5 \cdot \max(q - r + (m+1)c, q + r - mc, q)\Big] \le 2^n - k/2 \cdot [2^n/s] + \Big[0.5 \cdot \big([2^n/s] + \big](k+1)/2\big[+ k^2\big)\Big],$$

где c *вычисляется следующим образом*
- $c = [2r/(2m+1)]$ *при* $2r \bmod (2m+1) \le m$,
- $c = [2r/(2m+1)] + 1$ *при* $2r \bmod (2m+1) > m$.

Для того, чтобы понять насколько лучше полученная в этом следствии оценка по сравнению с тривиальной — $(2^n - 1)$ запросов, приводится следующее следствие.

Следствие 2. *При* $2^n > k$ *справедлива следующая верхняя оценка*

$$\varphi_{CQ}(F,n,k,k) \le 2^n\big(1 - \frac{2k}{3(k+1)^2} + \frac{4}{3k^2}\big) + \frac{k^2}{2} + \frac{3k}{4} + 1.$$

Причем, при $k \ge 5$ *эта величина строго меньше* $2^n - 1$.

Далее доказываются точные оценки сложности класса функций малого веса: веса 1, 2, 3. Причем, для функций веса 1 точная оценка получается довольно просто, но для функций веса 2 и 3 уже требуется более сложный разбор возможных случаев.

Теорема 6. *Сложность расшифровки класса* $F(n,1,1)$ *запросами на сравнение равна* $\varphi_{CQ}(F,n,1,1) = 2^{n-1}$.

Теорема 7. *При* $n \ge 2$ *сложность расшифровки класса* $F(n,2,2)$ *запросами на сравнение равна* $\varphi_{CQ}(F,n,2,2) = [2^{n+1}/3]$.

Теорема 8. *При* $n \ge 6$ *сложность расшифровки класса* $F(n,3,3)$ *запросами на сравнение равна*

$$\varphi_{CQ}(F,n,3,3) = 2^n -]3/2 \cdot [2^n/5][- [(2^n \bmod 5)/2].$$

После этого приводится оценки для самых больших представителей класса функций ограниченного веса: веса неограниченного снизу и ограниченного снизу единицей.

Теорема 9. *При $n \geq 2, 2^{n-1} \geq k$ сложность расшифровки класса $F(n,k,0)$ запросами на сравнение равна*

$$\varphi_{CQ}(F,n,k,0) = G(k,2^n).$$

Теорема 10. *При $n \geq 2, 2^{n-1} \geq k \geq 1, 2^n \bmod (k+1) = k$ сложность расшифровки класса $F(n,k,1)$ запросами на сравнение равна*

$$\varphi_{CQ}(F,n,k,1) = G(k,2^n) - 1.$$

При $n \geq 2, 2^{n-1} \geq k \geq 1, 2^n \bmod (k+1) = 0$ сложность расшифровки класса $F(n,k,1)$ запросами на сравнение равна

$$\varphi_{CQ}(F,n,k,1) = G(k,2^n).$$

При $n \geq 2, 2^{n-1} \geq k \geq 1, 2^n \bmod (k+1) \in (0,k)$ сложность расшифровки класса $F(n,k,1)$ запросами на сравнение удовлетворяет следующим ограничениям:

$$G(k,2^n) - 1 \leq \varphi_{CQ}(F,n,k,1) \leq G(k,2^n).$$

Раздел, а вместе с ним и вторая глава, завершается теоремой про порядок сложности расшифровки функций ограниченного веса запросами на сравнение.

Теорема 11. *Для любого $k = k(n)$, такого, что $k \geq 2, k = o(2^n)$, сложность расшифровки класса $F(n,k,i)$ запросами на сравнение при $n \to \infty$ удовлетворяет следующим соотношениям:*

$$\begin{cases} 7/10 \cdot 2^n \lesssim \varphi_{CQ}(F,n,k,i) \lesssim k/(k+1) \cdot 2^n & \text{при } i \leq 3 \leq k, \\ 2/3 \cdot 2^n \lesssim \varphi_{CQ}(F,n,k,i) \lesssim k/(k+1) \cdot 2^n & \text{при } i > 3 \text{ или } k = 2. \end{cases}$$

В **третьей главе** данной работы рассматривается параметро-эффективная расшифровка запросами на значение всех замкнутых классов Поста. Глава начинается с раздела со вспомогательными определениями и утверждениями. Далее следуют семь разделов с описанием результатов для групп классов, объединенных по букве в их обозначении: $C_i, A_i, D_i, F_j^i, S_i, L_i, O_i$. Главу завершает раздел с двумя теоремами, описывающие результаты рассматриваемой задачи для всех замкнутых классов решетки Поста для двух случаев:

1. и арность n, и верхняя оценка на число существенных переменных k стремятся к бесконечности,

2. только n стремится к бесконечности, а k зафиксирован.

Под условной асимптотической оценкой в формулировке приводимой теоремы будем понимать то, что оценка асимптотически равна величине, связанной с $\alpha(n,k)$, асимптотика которой неизвестна.

Теорема 12. *Замкнутые классы решетки Поста по характеру известной на данный момент сложности точной расшифровки запросами на значение разделены на четыре группы в случае* $n,k \to \infty$*:*

1. *точная оценка*
   - $\varphi_{MQ}(O_4,n,1) = \rceil \log_2 n \lfloor$ *при* $n>1$*;*
2. *асимптотика*
   - $\varphi_{MQ}(S_1,n,k) \sim k\log_2(n/k), n,k\to\infty, k=o(n)$*;*
   - $\varphi_{MQ}(S_3,n,k) \sim k\log_2(n/k), n,k\to\infty, k=o(n)$*;*
   - $\varphi_{MQ}(S_6,n,k) \sim k\log_2(n/k), n,k\to\infty, k=o(n)$*;*
   - $\varphi_{MQ}(L_1,n,k) \sim k\log_2 n, n,k\to\infty, \log_2 k = o(\log_2 n)$*;*
   - $\varphi_{MQ}(L_2,n,k) \sim k\log_2 n, n,k\to\infty, \log_2 k = o(\log_2 n)$*;*
   - $\varphi_{MQ}(L_3,n,k) \sim k\log_2 n, n,k\to\infty, \log_2 k = o(\log_2 n)$*;*
   - $\varphi_{MQ}(L_4,n,k) \sim k\log_2 n, n,k\to\infty, \log_2 k = o(\log_2 n)$*;*
   - $\varphi_{MQ}(L_5,n,k) \sim k\log_2 n, n,k\to\infty, \log_2 k = o(\log_2 n)$*;*
   - $\varphi_{MQ}(O_5,n,1) \sim \log_2 n, n\to\infty$*;*
   - $\varphi_{MQ}(O_6,n,1) \sim \log_2 n, n\to\infty$*;*
   - $\varphi_{MQ}(O_8,n,1) \sim \log_2 n, n\to\infty$*;*
   - $\varphi_{MQ}(O_9,n,1) \sim \log_2 n, n\to\infty$*;*
3. *условная асимптотика*
   - $\varphi_{MQ}(C_1,n,k) = \alpha(n,k)\cdot(1+o(1))$ *при* $k,n\to\infty, k=o(n)$*;*
   - $\varphi_{MQ}(C_2,n,k) = \alpha(n,k)\cdot(1+o(1))$ *при* $k,n\to\infty, k=o(n)$*;*
   - $\varphi_{MQ}(C_4,n,k) = 2\alpha(n-1,k-1)\cdot(1+o(1))$ *при* $k,n\to\infty, k=o(n)$*;*
   - $\varphi_{MQ}(D_3,n,k) = \alpha(n-1,k-1)\cdot(1+o(1))$ *при* $k,n\to\infty, k=o(n)$*;*
   - $\varphi_{MQ}(D_1,n,k) = \alpha(n-1,k-1)\cdot(1+o(1))$ *при* $k,n\to\infty, k=o(n)$*;*
   - *если* $i>1$ *или* $i=\infty$*, то* $\varphi_{MQ}(F_4^i,n,k) = \alpha(n,k)\cdot(1+o(1))$ *при* $k,n\to\infty, k=o(n)$*,* $k\geq 2$*;*
   - *если* $i>1$ *или* $i=\infty$*, то* $\varphi_{MQ}(F_1^i,n,k) = S_{n,k}\cdot(1+o(1))$ *при* $k,n\to\infty, k=o(n)$*;*
4. *порядок*
   - $\varphi_{MQ}(A_1,n,k) \asymp \frac{2^k}{\sqrt{k}} + k\log n$ *при* $k,n\to\infty$*;*
   - $\varphi_{MQ}(A_2,n,k) \asymp \frac{2^k}{\sqrt{k}} + k\log n$ *при* $k,n\to\infty$*;*
   - $\varphi_{MQ}(A_4,n,k) \asymp \frac{2^k}{\sqrt{k}} + k\log n$ *при* $k,n\to\infty$*;*
   - $\varphi_{MQ}(D_2,n,k) \asymp \frac{2^k}{\sqrt{k}} + k\log n$ *при* $k,n\to\infty$*;*

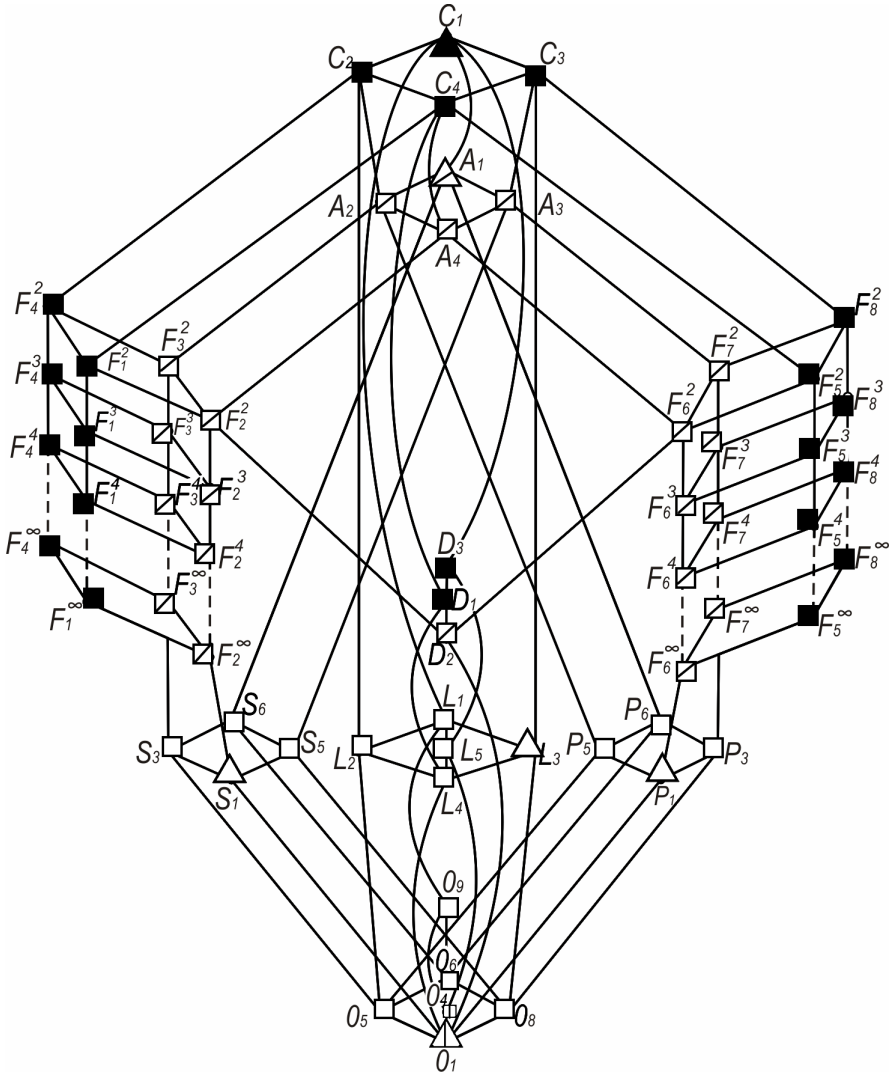

Рис. 1 — Результаты сложности расшифровки замкнутых классов Поста запросами на значение при $n, k \to \infty$.

- *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{MQ}(F_2^i, n, k) \asymp k \log n + \frac{2^k}{\sqrt{k}}$ *при* $k, n \to \infty$;
- *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{MQ}(F_3^i, n, k) \asymp k \log n + \frac{2^k}{\sqrt{k}}$ *при* $k, n \to \infty$.

На рисунке 1 схематично приведены результаты этой теоремы. Если класс выделен вертикальной чертой в квадрате или треугольнике, то имеется точная оценка. Если класс выделен белым, то для него получена асимптотическая оценка, если обозначен косой линией внутри квадрата или треугольника, то оценка по порядку, если черным, то условная асимптотическая оценка. Если класс выделен треугольником, то это результат, полученный ранее в других работах, все такие результаты в третьей главе будут называться утверждениями с указанием источника и автора. Если класс выделен квадратом, то результат ранее в литературе не встречался и впервые получен автором диссертационной работы, такие результаты в работе будут называться теоремами.

Теорема 13. *Замкнутые классы решетки Поста по характеру известной на данный момент сложности точной расшифровки запросами на значение в случае, когда n растет, а k не меняется, разделены на три группы:*

1. *точная оценка*
   - $\varphi_{MQ}(O_4, n, 1) = \rceil \log_2 n \lfloor$ *при* $n > 1$;
2. *асимптотика*
   - $\varphi_{MQ}(O_5, n, 1) \sim \log_2 n, n \to \infty$;
   - $\varphi_{MQ}(O_6, n, 1) \sim \log_2 n, n \to \infty$;
   - $\varphi_{MQ}(O_8, n, 1) \sim \log_2 n, n \to \infty$;
   - $\varphi_{MQ}(O_9, n, 1) \sim \log_2 n, n \to \infty$;
3. *порядок*
   - $\varphi_{MQ}(C_1, n, k) \asymp \log n, n \to \infty, k \geq 2$;
   - $\varphi_{MQ}(C_2, n, k) \asymp \log n, n \to \infty, k \geq 2$;
   - $\varphi_{MQ}(C_4, n, k) \asymp \log n, n \to \infty, k \geq 2$;
   - $\varphi_{MQ}(A_1, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{MQ}(A_2, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{MQ}(A_4, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{MQ}(D_1, n, k) \asymp \log n$ *при* $n \to \infty, k \geq 2$;
   - $\varphi_{MQ}(D_2, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{MQ}(D_3, n, k) \asymp \log n$ *при* $n \to \infty, k \geq 2$;
   - *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{MQ}(F_1^i, n, k) \asymp \log n$ *при* $n \to \infty$, $k \geq 2$;
   - *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{MQ}(F_2^i, n, k) \asymp \log n$ *при* $n \to \infty$;
   - *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{MQ}(F_3^i, n, k) \asymp \log n$ *при* $n \to \infty$;
   - *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{MQ}(F_4^i, n, k) \asymp \log n$ *при* $n \to \infty$, $k \geq 2$;
   - $\varphi_{MQ}(S_1, n, k) \asymp \log n, n \to \infty$;
   - $\varphi_{MQ}(S_3, n, k) \asymp \log n, n \to \infty$;
   - $\varphi_{MQ}(S_6, n, k) \asymp \log n, n \to \infty$;
   - $\varphi_{MQ}(L_1, n, k) \asymp \log n, n \to \infty$;
   - $\varphi_{MQ}(L_2, n, k) \asymp \log n, n \to \infty$;

– $\varphi_{MQ}(L_3, n, k) \asymp \log n, n \to \infty$;
– $\varphi_{MQ}(L_4, n, k) \asymp \log n, n \to \infty$;
– $\varphi_{MQ}(L_5, n, k) \asymp \log n, n \to \infty$.

Содержательную часть работы завершает **четвертая глава**, в которой рассматривается параметро-эффективная расшифровка запросами на сравнение всех замкнутых классов Поста. Глава начинается с раздела во вспомогательными определениями и утверждениями. В этом разделе приводится следствие, которое разделяет классы решетки Поста на две группы: которые можно и которые нельзя расшифровать запросами на сравнение.

Следствие 3. *Если* $F \in \{C_1, A_1, L_1, S_6, O_9, O_6\}$, *то расшифровать запросами на сравнение класс* F *невозможно. Если* $F \in \{C_2, C_3, C_4, A_2, A_3, A_4, F_1^i, F_2^i, F_3^i, F_4^i, D_1, D_2, D_3, S_1, S_3, S_5, L_2, L_3, L_4, L_5, O_1, O_4, O_5, O_8\}$, *то класс* F *можно расшифровать.*

Но чтобы не терять полностью из рассмотрения замкнутые классы $C_1, A_1, L_1, S_6, O_9, O_6$ лишь по тому, что они содержат обе константы, предлагается все же их рассматривать, но без константы 0, и обозначать символом *. Причем обращается внимание, что замыкание класса C_1^* совпадает с C_1, L_1^* — с L_1, O_9^* — с O_9, а $A_1^* = A_2, S_6^* = S_3, O_6^* = O_5$, поэтому для классов C_1^*, L_1^*, O_9^* будет приводится отдельно оценка сложности расшифровки, а для остальных — нет.

Далее следуют семь разделов с описанием результатов для групп классов, объединенных по букве в их обозначении: $C_i, A_i, D_i, F_j^i, S_i, L_i, O_i$. Глава завершается разделом с двумя теоремами, в которые объединены результаты всех предыдущих разделов главы для двух случаев: оба параметра n, k стремятся к бесконечности, только n стремится к бесконечности, а k зафиксирован.

Под условной оценкой по порядку, встречающейся в формулировке теоремы, будем понимать то, что оценка по порядку равна величине, связанной с $\alpha(n, k)$, порядок и асимптотика которой неизвестны.

Теорема 14. *Замкнутые классы решетки Поста по характеру известной на данный момент сложности точной расшифровки запросами на сравнение разделены на четыре группы в случае* $n, k \to \infty$:

1. *точная оценка*
   – $\varphi_{CQ}(O_1, n, 1) = \rceil \log_3 n \lceil$;
2. *асимптотика*
   – $\varphi_{CQ}(O_4, n, 1) \sim \log_3 n$ *при* $n \to \infty$;
   – $\varphi_{CQ}(O_5, n, 1) \sim \log_3 n$ *при* $n \to \infty$;
   – $\varphi_{CQ}(O_8, n, 1) \sim \log_3 n$ *при* $n \to \infty$;
   – $\varphi_{CQ}(O_9^*, n, 1) \sim \log_3 n$ *при* $n \to \infty$;
3. *условный порядок*

- $\varphi_{CQ}(C_1^*, n, k) \asymp \alpha(n, k)$ *при* $n, k \to \infty, k = o(n)$;
- $\varphi_{CQ}(C_2, n, k) \asymp \alpha(n, k)$ *при* $n, k \to \infty, k = o(n)$;
- $\varphi_{CQ}(C_4, n, k) \asymp \alpha(n-1, k-1)$ *при* $n, k \to \infty, k = o(n)$;
- $\varphi_{CQ}(D_1, n, k) \asymp \alpha(n-1, k-1)$ *при* $n, k \to \infty, k = o(n)$;
- $\varphi_{CQ}(D_3, n, k) \asymp \alpha(n-1, k-1)$ *при* $n, k \to \infty, k = o(n)$;
- *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{CQ}(F_1^i, n, k) \asymp S_{n,k}$ *при* $n, k \to \infty, k = o(n)$;
- *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{CQ}(F_4^i, n, k) \asymp \alpha(n, k)$ *при* $n, k \to \infty, k = o(n)$;

4. порядок

- $\varphi_{CQ}(A_2, n, k) \asymp \frac{2^k}{\sqrt{k}} + k \log n$ *при* $n, k \to \infty$;
- $\varphi_{CQ}(A_4, n, k) \asymp \frac{2^k}{\sqrt{k}} + k \log n$ *при* $n, k \to \infty$;
- $\varphi_{CQ}(D_2, n, k) \asymp \frac{2^k}{\sqrt{k}} + k \log n$ *при* $n, k \to \infty$;
- *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{CQ}(F_2^i, n, k) \asymp k \log n + \frac{2^k}{\sqrt{k}}$ *при* $n, k \to \infty$;
- *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{CQ}(F_3^i, n, k) \asymp k \log n + \frac{2^k}{\sqrt{k}}$ *при* $n, k \to \infty$;
- $\varphi_{CQ}(S_1, n, k) \asymp k \log (n/k)$ *при* $n, k \to \infty, k = o(n)$;
- $\varphi_{CQ}(S_3, n, k) \asymp k \log (n/k)$ *при* $n, k \to \infty, k = o(n)$;
- $\varphi_{CQ}(S_5, n, k) \asymp k \log (n/k)$ *при* $n, k \to \infty, k = o(n)$;
- $\varphi_{CQ}(L_1^*, n, k) \asymp k \log n$ *при* $n, k \to \infty, \log k = o(\log n)$;
- $\varphi_{CQ}(L_2, n, k) \asymp k \log n$ *при* $n, k \to \infty, \log k = o(\log n)$;
- $\varphi_{CQ}(L_4, n, k) \asymp k \log n$ *при* $n, k \to \infty, \log k = o(\log n)$;
- $\varphi_{CQ}(L_5, n, k) \asymp k \log n$ *при* $n, k \to \infty, \log k = o(\log n)$.

На рисунке 2 схематично приведены основные результаты четвертой главы. Если класс выделен квадратом с обеими диагоналями, тогда этот класс нельзя расшифровать запросами на сравнение. Если класс выделен вертикальной чертой в квадрате, то имеется точная оценка. Если класс выделен белым, то для него получена асимптотическая оценка, если обозначен косой линией внутри квадрата, то оценка по порядку, если черным, то условная оценка по порядку.

Теорема 15. *Замкнутые классы решетки Поста по характеру известной на данный момент сложности точной расшифровки запросами на сравнение в случае, когда* n *растет, а* k *не меняется, разделены на три группы:*

1. точная оценка

- $\varphi_{CQ}(O_1, n, 1) = \rceil \log_3 n \lceil$;

2. асимптотика

- $\varphi_{CQ}(O_4, n, 1) \sim \log_3 n$ *при* $n \to \infty$;
- $\varphi_{CQ}(O_5, n, 1) \sim \log_3 n$ *при* $n \to \infty$;

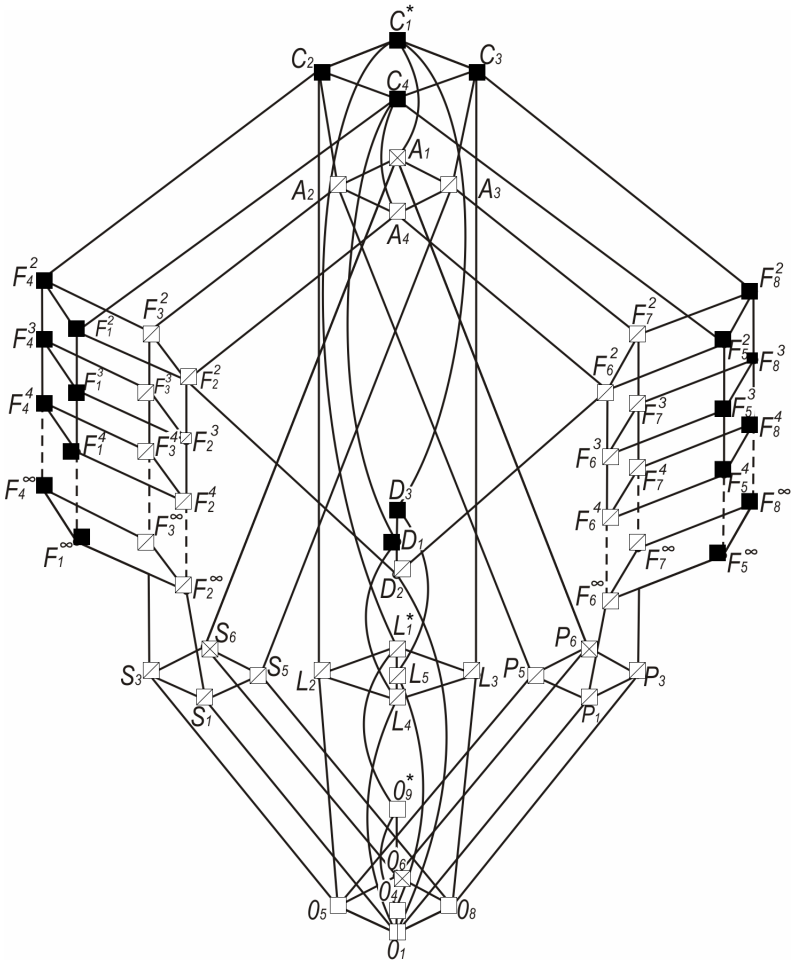

Рис. 2 — Результаты сложности расшифровки замкнутых классов Поста запросами на сравнение при $n, k \to \infty$.

- $\varphi_{CQ}(O_8, n, 1) \sim \log_3 n$ *при* $n \to \infty$;
- $\varphi_{CQ}(O_9^*, n, 1) \sim \log_3 n$ *при* $n \to \infty$;

3. *порядок*
   - $\varphi_{CQ}(C_1^*, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(C_2, n, k) \asymp \log n$ *при* $n \to \infty, k \geq 2$;
   - $\varphi_{CQ}(C_4, n, k) \asymp \log n$ *при* $n \to \infty, k \geq 2$;
   - $\varphi_{CQ}(A_2, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(A_4, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(D_1, n, k) \asymp \log n$ *при* $n \to \infty, k \geq 2$;
   - $\varphi_{CQ}(D_2, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(D_3, n, k) \asymp \log n$ *при* $n \to \infty, k \geq 2$;
   - *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{CQ}(F_1^i, n, k) \asymp \log n$ *при* $n \to \infty$, $k \geq 2$;
   - *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{CQ}(F_2^i, n, k) \asymp \log n$ *при* $n \to \infty$;
   - *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{CQ}(F_3^i, n, k) \asymp \log n$ *при* $n \to \infty$;
   - *если* $i > 1$ *или* $i = \infty$, *то* $\varphi_{CQ}(F_4^i, n, k) \asymp \log n$ *при* $n \to \infty$, $k \geq 2$;
   - $\varphi_{CQ}(S_1, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(S_3, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(S_5, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(L_1^*, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(L_2, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(L_4, n, k) \asymp \log n$ *при* $n \to \infty$;
   - $\varphi_{CQ}(L_5, n, k) \asymp \log n$ *при* $n \to \infty$.

Работу завершает **заключение**, в котором излагаются следующие основные результаты проведенного исследования.

1. Получены значения сложности параметро-эффективной точной расшифровки класса функций ограниченного веса для трех типов запросов в отдельности: на значение, на расширенную и ограниченную эквивалентность.
2. Получены значения сложности точной расшифровки запросами на сравнение класса функций малого веса: 1, 2, 3.
3. Получена практически точная оценка сложности расшифровки запросами на сравнение классов функций веса ограниченного снизу нулем и ограниченного снизу единицей.
4. Доказан порядок сложности точной расшифровки запросами на сравнение класса функций ограниченного веса в случае, когда растет арность функций, а ее вес не меняется.
5. Доказаны оценки сложности параметро-эффективной точной расшифровки запросами на значение замкнутых классов самодвойственных функций и классов “счетной этажерки” решетки Поста.

6. Доказаны оценки сложности параметро-эффективной точной расшифровки запросами на сравнение всех замкнутых классов решетки Поста.

Благодарности. Автор приносит благодарность профессорско-преподавательскому составу Ташкентского филиала МГУ имени М. В. Ломоносова и механико-математического факультета МГУ имени М. В. Ломоносова, а особенно коллективу кафедры математической теории интеллектуальных систем, за опыт и знания, полученные от них на протяжении всего периода обучения.

Особую признательность автор выражает доктору физико-математических наук, профессору Эльяру Эльдаровичу Гасанову за научное руководство и неугасаемое внимание к работе, а также Тимуру Рашидовичу Сытдыкову и кандидату физико-математических наук Александру Павловичу Пивоварову, чьи ценные замечания и предложения способствовали существенному улучшению текстов статей, которые стали основой данной работы.

Автор благодарит своих родителей: Быстрыгову Светлану Викторовну и Быстрыгова Виктора Николаевича — за поддержку и веру в успех на академическом и научном поприще, а также своего школьного учителя математики Кирееву Тамару Михайловну и преподавателя математики в колледже Ильину Наталию Ивановну за занятия, которые привили интерес к математике, а также их внимание и раннее приобщение к олимпиадной деятельности.

Список публикаций автора по теме диссертации

1. *Быстрыгова, А. В.* Запросы на сравнение в задаче параметро-эффективной расшифровки булевых функций / А. В. Быстрыгова // Интеллектуальные системы. Теория и приложения. — 2019. — Т. 23, № 4. — С. 115—124. — (Импакт-фактор РИНЦ 2020 год: 0.127).

2. *Быстрыгова, А. В.* Параметро-эффективная расшифровка булевых функций из замкнутых классов Поста / А. В. Быстрыгова // Дискрет. матем. — 2019. — Т. 31, № 2. — С. 34—58. — (Импакт-фактор РИНЦ 2019 год: 0.685).

3. *Быстрыгова, А. В.* Расшифровка булевых функций фиксированного веса / А. В. Быстрыгова // Интеллектуальные системы. Теория и приложения. — 2020. — Т. 24, № 3. — С. 63—96. — (Импакт-фактор РИНЦ 2020 год: 0.127).

4. *Быстрыгова, А. В.* Расшифровка булевых функций ограниченного веса / А. В. Быстрыгова // Вестник Московского университета. Серия 1: Математика. Механика. — 2021. — № 6. — С. 14—20. — (Импакт-фактор РИНЦ 2020 год: 0.367).

5. *Быстрыгова, А. В.* Запросы на сравнение в задаче точной расшифровки замкнутых классов Поста / А. В. Быстрыгова // Интеллектуальные системы. Теория и приложения. — 2022. — Т. 26, № 3. — С. 88—108. — (Импакт-фактор РИНЦ 2020 год: 0.127).

Быстрыгова Анастасия Викторовна

Параметро-эффективная расшифровка булевых функций

Автореф. дис. на соискание ученой степени канд. физ.-мат. наук

Подписано в печать ___.___._____. Заказ № _____
Формат 60×90/16. Усл. печ. л. 1. Тираж 100 экз.
Типография _____