МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

МЕХАНИКО–МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи
УДК 519.71

Осокин Виктор Владимирович

О РАСШИФРОВКЕ ЛОГИЧЕСКИХ ФУНКЦИЙ

01.01.09 — дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

МОСКВА — 2011

Работа выполнена на кафедре Математической теории интеллектуальных систем Механико-математического факультета Московского государственного университета имени М.В. Ломоносова.

Научный руководитель — доктор физико-математических наук, профессор
Эльяр Эльдарович Гасанов

Официальные оппоненты:

доктор физико-математических наук, профессор
Александр Александрович Михалев

кандидат физико-математических наук
Денис Владимирович Зайцев

Ведущая организация — Московский Энергетический Институт (Технический университет)

Защита диссертации состоится 10 июня 2011 г. в 16 ч. 45 м. на заседании диссертационного совета Д.501.001.84 при Московском государственном университете имени М.В.Ломоносова по адресу: Российская Федерация, 119991, Москва, ГСП-1, Ленинские горы, д.1, Московский государственный университет имени М.В. Ломоносова, Механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ имени М.В. Ломоносова (Главное здание, 14 этаж).

Автореферат разослан 27 апреля 2011 г.

Ученый секретарь диссертационного
совета Д.501.001.84 при МГУ
доктор физико-математических наук,
профессор

А.О.Иванов

Общая характеристика работы

Актуальность темы. Проблема расшифровки функций является ключевой задачей теории алгоритмического обучения, одного из активно развивающихся направлений современной дискретной математики. Расшифровка функций — это создание алгоритмов игры между учителем и учеником: учитель загадывает некоторую функцию из некоторого известного ученику класса, ученик, используя алгоритм, пытается отгадать загаданную функцию, сделав минимальное число вопросов. При этом, как в теоретической, так и в прикладной среде могут рассматриваться по крайней мере три следующих варианта учителя:

- активный учитель: ученик может сам выбирать, какие вопросы задавать учителю. Учитель отвечает на вопросы ученика. В прикладной среде такой подход называется *классификацией с активным учителем* (обучение у активного учителя);

- пассивный учитель: ученик никак не влияет на учителя, учитель сам генерирует возможные вопросы ученика и сам же отвечает на них. Другими словами, учитель генерирует примеры с ответами, и ученик должен обучиться по ним. В прикладной среде такой подход называется *классификацией с пассивным учителем* (обучением у пассивного учителя);

- учитель отсутствует. Ученик получает некоторое множество данных, выделяет в нем какие-либо закономерности и в соответствии с этими закономерностями разбивает множество на классы, такие что в одном классе содержатся «похожие» друг на друга элементы. В прикладной среде такой подход называется *кластеризацией*.

В диссертации исследуется сложность расшифровки дискретных функций из различных классов при активном учителе в *модели точной расшифровки при помощи запросов на значение функции* (Д.Англуин[1], Е.Н.Гильберт [2], В.К.Коробков[3]). Задачу расшифровки псевдо-булевских функций можно рассматривать как задачу расшифровки автоматов без памяти, т.е. как частную подзадачу более общей задачи расшифровки автоматов[4]. Модель точной расшифровки — это модель расшифровки, в которой

[1] D.Angluin *Queries and Concept Learning*, Machine Learning, Vol. 2, pp. 319-342, 1988.

[2] E.N.Gilbert *Lattice theoretic properties of frontal switching functions*, J. Math. Phys., 33 (1954), 57-97

[3] В.К.Коробков *О монотонных функциях алгебры логики*, Проблемы кибернетики, 13, 5-28, 1965

[4] В.Б.Кудрявцев, С.В.Алешин, А.С.Подколзин *Введение в теорию автоматов*, НАУКА, М., 1985

предполагается, что загаданную учителем функцию ученик должен отгадывать точно, а не приближенно с некоторой вероятностью (как, например, в *модели вероятно примерно точной расшифровки*). В модели точной расшифровки функция f от n переменных задана при помощи черного ящика и задача ученика (алгоритма расшифровки) состоит в том, чтобы расшифровать f, т.е. полностью восстановить ее таблицу значений. Чтобы расшифровать загаданную функцию, алгоритм расшифровки может делать *запросы на значение функции*, т.е. подавать произвольные наборы из области определения функции черному ящику. Алгоритм расшифровки подает запросы блоками, учитель одновременно отвечает на все вопросы из одного блока. В *стандартной постановке* алгоритм расшифровки должен расшифровать загаданную функцию, использовав по возможности наименьшее число запросов на значение функции. В *параллельной постановке* алгоритм расшифровки должен минимизировать число блоков, требуемых для расшифровки (П.Дамашке[5]).

Приведем некоторые примеры прикладных задач, в которых задача расшифровки дискретных функций при активном учителе может играть ключевое значение.

Пример 1. Задачи по созданию и анализу интернет сайтов: размещение рекламы на интернет-сайтах, разбиение множества страниц сайтов по темам, автоматическое создание лент новостей по тематике, анализ истории посещения сайтов, определение спама. Указанные задачи много лет решаются при пассивном учителе. Возможность использования активного учителя (выбора, на каких запросах обучаться) позволяет понизить в этих задачах время обучения.

Пример 2. Распознавание речи и другие задачи распознавания, в которых «правильные ответы» учителя стоят очень дорого. Использование подхода с активным учителем позволяет минимизировать число запросов к учителю путем их оптимального выбора.

Пример 3. Задачи поиска, в частности, поиска в интернете. Уже несколько лет ведущие поисковые системы «расшифровывают» собственные функции ранжирования страниц сайтов в попытке сделать их наиболее точными. В данном случае расшифровка с активным учителем - снова единственная возможность: подбираются конкретные запросы (поисковые запросы) и ответы поисковых систем на них и только по

[5]P.Damaschke *On Parallel Attribute-Efficient Learning*, Journal of Computer and System Sciences, Volume 67, Issue 1, August 2003, 46-62

этим запросам специально обученные люди оценивают соответствие запросов и ответов (т.е., функцию ранжирования).

В описанных прикладных задачах существенную роль играют следующие два фактора.

Во-первых, число переменных (признаков), от которых существенно зависит расшифровываемая функция, во многих случаях мало по сравнению с общим числом переменных. Поэтому, на алгоритмы расшифровки приходится накладывать требование, чтобы их сложность зависела от числа существенных переменных и слабо зависела от числа несущественных переменных. Алгоритмы с таким свойством принято называть *параметро-эффективными*, а их работу — *параметро-эффективной расшифровкой.*

Во-вторых, нередка ситуация, когда учитель может одновременно отвечать на целое множество вопросов ученика. Поэтому, встает вопрос минимизации числа блоков вопросов, которые задает ученик учителю при расшифровке функции. В таких случаях говорят, что рассматривается задача *параллельной расшифровки.*

Неполный список исследований, проведенных в точности в рамках модели точной расшифровки при помощи запросов на значение функции, но не рассматривающих ни задачу параметро-эффективной расшифровки, ни задачу параллельной расшифровки, включает в себя следующие: С.Чой и др.[6], В.Торвик [7], Е.Борос и др.[8], Н.Ю.Золотых, В.Н.Шевченко[9], Б.Ковалерчук и др.[10], А.Накамура и др.[11], К.Макино и др.[12], Д.Н.Гайнанов[13], Н.А.Соколов[14].

Некоторые общие результаты по сложности параметро-эффективной (но не параллельной) расшифровки в модели точной расшифровки

---

[6]S.Choi, K.Jung, J.Kirn *Almost Tight Upper Bound for Finding Fourier Coefficients of Bounded Pseudo-Boolean Functions*, COLT 2008, 123-134

[7]V.I.Torvik *Data Mining and Knowledge Discovery: a Guided Approach based on Monotone Boolean Functions*, Ph.D. in Engineering Science, May 24, 2002, Louisiana State University

[8]E.Boros, P.Hammer, T.Ibaraki, K.Kawakami *Polynomial-Time Recognition of 2-Monotonic Positive Boolean Functions Given by an Oracle*, SIAM Journal on Computing, Volume 26, Issue 1, 93-109, 1997

[9]N.Yu.Zolotykh, V.N.Shevchenko *Lower Bounds for the Complexity of Learning Half-Spaces with Membership Queries*, ALT'98, Otzenhausen, Germany, October 8-10, 1998

[10]B.Kovalerchuck, E.Triantapliyllou, A.S.Deshpande, E.Vityaev *Interactive learning of monotone Boolean functions*, Information Sciences: an International Journal, Volume 94, Issue 1-4, 87 - 118, 1996

[11]A.Nakamura, N.Abe *Exact learning of linear combinations of monotone terms from function value queries*, Theoretical Computer Science, Volume 137, Issue 1, 159-176, 1995

[12]K.Makino, T.Ibaraki *The maximum latency and identification of positive Boolean functions*, SIAM Journal on Computing, Volume 26, Issue 5, 1363 - 1383, 1997

[13]Д.Н.Гайнанов *Об одном критерии оптимальности алгоритма расшифровки монотонных булевых функций*, USSR Computational Mathematics and Mathematical Physics, Volume 24, Issue 4, 1985, Pages: 176-181

[14]Н.А.Соколов *On the optimal evaluation of monotonic Boolean functions*, USSR Computational Mathematics and Mathematical Physics, Volume 22, Issue 2, 1982, Pages 207-220

при помощи запросов на значение функции получены Н.Бшаути и др.[15]. И.Вегенер и др.[16] получили точные оценки сложности параметро-эффективной расшифровки некоторых классов булевских функций в этой модели.

Параллельная (но не параметро-эффективная) расшифровка в модели точной расшифровки при помощи запросов на значение функции исследовалась Н.Бшаути[17]. Наконец, параллельная параметро-эффективная расшифровка в этой модели рассматривалась в работах П.Дамашке[18,19].

В большинстве упомянутых работ рассматривается расшифровка булевских функций. В настоящей диссертации исследована задача параллельной параметро-эффективной расшифровки псевдо-булевских функций. Основные свойства псевдо-булевских функций описаны в работе Е.Борос, П.Хаммер[20]. Некоторые классы псевдо-булевских функций описаны в работе С.Фолдс, П.Хаммер[21].

Параметро-эффективная расшифровка (иначе, расшифровка хунт) исследовалась в рамках нескольких моделей стимулирующего обучения и обучения с учителем. Параметро-эффективный алгоритм расшифровки пороговых функций в рамках модели ограниченной ошибки стимулирующего обучения предложил Н.Литтлстоун[22]. Впоследствии различные аспекты параметро-эффективной расшифровки рассматривали А.Блюм и др.[23]. Пассивное обучение с учителем, т.е. расшифровка по случайной выборке обычно изучается в рамках так называемой модели вероятно примерно точной расшифровки[24]. Параметро-эффективная расшифровка по случайной равномерно распределенной выборке в PAC модели является открытой проблемой[25]. Для ознакомления с недавними результатами по пассивной

[15]N.Bshouty, L.Hellerstein Attribute efficient learning in query and mistake-bound models, Journal of Computer and System Sciences, 56: 310-319, 1998

[16]R.Uehara, K.Tsuchida, I.Wegener *Optimal attribute-efficient learning of disjunction, parity, and threshold functions*, Lecture Notes In Computer Science; Vol. 1208, 1997

[17]N.Bshouty *Exact learning of formulas in parallel*, Machine Learning. Volume 26. Issue I, 25-41, 1997

[18]P.Damaschke *Adaptive versus nonadaptive attribute-efficient learning*,Machine Learning 41 (2000), 197-215

[19]P.Damaschke *Parallel Attribute-Efficient Learning of Monotone Boolean Functions*, Lecture Notes in Computer Science, Algorithm Theory - SWAT 2000, 473-479

[20]E.Boros, P.Hammer *Pseudo-boolean optimization*, Discrete Applied Mathematics, Volume 123, Issue 1-3, 155-225, 2002

[21]S.Foldes, P.Hammer *Monotone, Horn and Quadratic Pseudo-Boolean Functions*, J. UCS, Volume 6, Number 1, 97-104, 2000

[22]N.Littlestone *Learning Quickly When Irrelevant Attributes Abound: A New Linear-threshold Algorithm*, Machine Learning, 2(4): 285-318, 1987

[23]A.Blum, L.Hellerstein, N.Littlestone *Learning in the presence of finitely or infinitely many irrelevant attributes*, Journal of Computer and System Sciences, 50: 32-40, 1995

[24]L.Valiant *A theory of the learnable*, ACM Press New York, NY, USA, Volume 27, Issue II, 1134-1142

[25]A.Blum *Learning a Function of r Relevant Variables*, COLT 2003, Open problems

расшифровке хунт см. Д.Арпе и др.[26], М.Колоунтзакис и др.[27], Е.Моссель и др.[28]. Параллельную расшифровку рассматривали Д.Бальказар и др.[29], Д.Виттер и др.[30].

Среди направлений, близких к рассматриваемому направлению расшифровки функций, можно выделить теорию тестового распознавания[31,32].

Цель работы. Рассматривается задача расшифровки дискретных функций из различных классов при помощи запросов на значение функции. Независимо рассматривается задача определения существенных переменных. Целью работы является исследование обычной и параллельной сложности расшифровки функций из различных классов и определения существенных переменных, а также построение оптимальных, оптимальных параметро-эффективных и оптимальных параллельных алгоритмов расшифровки функций и оптимальных алгоритмов определения существенных переменных.

Научная новизна. Исследования, проведенные в данной диссертации, направлены на изучение обычной, параметро-эффективной и параллельной сложности алгоритмов расшифровки булевских монотонных функций, псевдо-булевских монотонных функций, интервально-постоянных функций, разбивающих функций, полных разбивающих функций, симметрических интервально-постоянных функций, пороговых функций и дизъюнкций переменных. Также исследована связь между сложностью расшифровки функций и сложностью определения их существенных переменных.

Впервые предложены аналоги шенноновской функции для сложности параметро-эффективной и параллельной расшифровки, позволяющие строить оптимальные алгоритмы расшифровки.

В работе получены следующие результаты.

1. Для классов монотонных, разбивающих и интервально-постоянных функций получены порядки сложности определения существенных переменных. Для разбивающих функций построен алгоритм отве-

[26] J.Arpe, B.Reischuk *Learning Juntas in the Presence of Noise*, Theoret. Comput. Sci. 384(1): 2-21, 2007

[27] M.Kolountzakis, E.Markakis, A.Mehta *Learning Symmetric Juntas in Time* $n^{o(k)}$, In the proceedings of "Interface between Harmonic Analysis and Number Theory 2005"

[28] E.Mossel, R.O'Donnell, R.Servedio *Learning juntas*, In Proceedings of the 35th Annual ACM Symposium on Theory of Computing, 2003

[29] J.L.Balcazar, J.Diaz, R.Gavalda, O.Watanabe *An optimal parallel algorithm for learning DFA*, Proceedings of the seventh annual conference on Computational learning theory, 208-217, 1994

[30] J.S.Vitter, J.Lin *Learning in Parallel*, Inf. Comput. 96(2): 179-202, 1992

[31] В.Б.Кудрявцев, А.Е.Андреев, Э.Э.Гасанов *Теория тестового распознавания*, ФИЗМАТЛИТ, М., 2007

[32] В.Б.Кудрявцев, Э.Э.Гасанов, О.А.Долотова, Г.Р.Погосян *Теория тестирования логических устройств*, ФИЗМАТЛИТ, М., 2006

тов на запросы на значение функции, позволивший в случае малого числа существенных переменных получить асимптотику сложности определения существенных переменных. Для полных разбивающих функций при малом и большом числе существенных переменных получены асимптотики сложности определения существенных переменных, отличные от оценок в общем случае. Для получения оценок сложности параллельной расшифровки введено понятие 2-разделяемых функций и показано, что классы разбивающих функций, монотонных функций, псевдо-булевских монотонных функций и интервально-постоянных функций являются 2-разделяемыми (т.е. содержат 2-разделяемые функции). Для 2-разделяемых классов функций построен алгоритм ответов на запросы на значение функции, позволивший получить порядок параллельной сложности определения существенных переменных таких функций.

2. Для различных классов интервально-постоянных функций, в частности, для классов монотонных и разбивающих функций, получены мощностные нижние оценки сложности параметро-эффективной расшифровки таких классов. Предложен универсальный алгоритм параметро-эффективной расшифровки интервально-постоянных функций, оптимальный по порядку на различных подклассах класса интервально-постоянных функций. Упомянутые нижние оценки и алгоритм расшифровки позволили получить асимптотические оценки сложности параметро-эффективной расшифровки для многих подклассов интервально-постоянных функций.

3. Предложен параметро-эффективный алгоритм расшифровки интервально-постоянных функций с небольшой параллельной сложностью и показано, что для некоторых подклассов класса интервально-постоянных функций этот алгоритм имеет как оптимальную сложность, так и оптимальную параллельную сложность. В частности, при некоторых ограничениях это относится к классам булевских монотонных функций, псевдо-булевских монотонных функций, разбивающих функций и интервально-постоянных функций в целом. Для данных классов получен порядок сложности параллельной расшифровки для оптимальных по порядку в смысле обычной сложности параметро-эффективных алгоритмов расшифровки.

Основные методы исследования. В работе используются методы дискретного анализа и теории сложности.

Теоретическая и практическая ценность работы. Работа имеет теоретический характер и может быть полезна специалистам по расшифровке функций, специалистам по теории алгоритмического обучения, по теории автоматов и их приложений.

Апробация работы. Результаты настоящей работы докладывались

- на IX Международной конференции «Интеллектуальные системы и компьютерные науки» (2006г.),
- на IX Международном семинаре «Дискретная математика и ее приложения» (2007г.),
- на Международной конференции «Современные проблемы математики, механики и их приложений», посвященной 70-летию ректора МГУ академика В.А.Садовничего (2009г.),
- на Международной конференции студентов, аспирантов и молодых ученых «Ломоносов-2009», «Ломоносов-2010», «Ломоносов-2011» (2009, 2010, 2011гг.). На конференции «Ломоносов-2011» награжден дипломом за лучший доклад на секции «Математика и Механика».
- на Международном семинаре «Дискретная математика» (2010г.)
- на семинаре «Вопросы сложности алгоритмов поиска» под руководством профессора Э. Э. Гасанова, 2005–2010 гг. (неоднократно);
- на научно-исследовательском семинаре кафедры Математической теории интеллектуальных систем «Теория автоматов», 2008–2010 гг. (неоднократно);
- на семинаре «Кибернетика и информатика» под руководством профессора В. Б. Кудрявцева, МГУ им. М.В. Ломоносова, 2010–2011 гг. (неоднократно);

Публикации по теме диссертации. Основные результаты диссертации опубликованы в восьми статьях [1]−[8] и материалах конференций [9]−[14], список которых приведен в конце автореферата.

Структура и объем диссертации. Диссертация состоит из введения и трех глав. Объем диссертации 117 стр. Список литературы содержит 37 наименований.

Краткое содержание работы

В диссертации мы используем следующие обозначения для классов функций. Пусть Φ — некоторый класс функций. Тогда $\Phi^n \subseteq \Phi$ есть подкласс, состоящий из функций от n переменных $x_1, \ldots, x_n$; $\Phi^{k,n} \subseteq \Phi^n$ есть подкласс, состоящий из функций от n переменных $x_1, \ldots, x_n$, существенно зависящих не более чем от k переменных; $\Phi^{=n} \subseteq \Phi^n$ есть подкласс, состоящий из функций от n переменных $x_1, \ldots, x_n$, существенно зависящих от всех n своих переменных.

Пусть $f : \{0,1\}^{V_n} \to \mathbb{N}$ — псевдо-булевская функция. Если для любых фиксаций $\alpha, \beta, \gamma \in \{0,1\}^{V_n}$, таких что $\alpha > \gamma > \beta$ из $f(\alpha) = f(\beta)$ следует, что $f(\alpha) = f(\gamma)$, то будем называть f *интервально-постоянной*. Другими словами, если такая функция присваивает одно и то же значение двум сравнимым наборам, то она присваивает то же значение любому набору из грани, задаваемой этими двумя наборами. Класс всех таких функций будем обозначать через ICF (*interval constant functions*).

Рассмотрим такую псевдо-булевскую функцию, что если она присваивает одно и то же значение двум произвольным фиксациями, то она присваивает то же значение любой фиксации из грани, задаваемой этими двумя фиксациями. Такие функции будем называть *разбивающими функциями* и обозначать соответствующий класс как SPL (*splitting functions*). Очевидно, что класс интервально-постоянных функций содержит класс разбивающих функций, т.е. SPL $\subset$ ICF. Если разбивающая функция, существенно зависящая от k переменных, принимает 2^k значений, то будем называть ее *полной разбивающей функцией*. Класс полных разбивающих функций будем обозначать через CSPL (*complete splitting functions*).

Рассмотрим такую псевдо-булевскую функцию, что для любых двух фиксаций α и β из того, что $\alpha \leq \beta$ следует, что $f(\alpha) \leq f(\beta)$. Такие функции будем называть *псевдо-булевскими монотонными функциями* и обозначать соответствующий класс через PM. Очевидно, что класс ICF содержит класс псевдо-булевских монотонных функций, т.е. PM $\subset$ ICF. Класс булевских монотонных функций обозначим через M, M $\subset$ PM. Фиксацию $\alpha \in \{0,1\}^{V_n}$ будем называть *верхним нулем* функции $f \in \mathrm{M}^n$, если $f(\alpha) = 0$ и $f(\beta) = 1$ для любой фиксации $\beta > \alpha$. Аналогично α является *нижней единицей*, если $f(\alpha) = 1$ и $f(\beta) = 0$ для любой фиксации $\beta < \alpha$.

Симметрическая функция, зависящая от всех своих переменных — это функция, присваивающая одно и то же значение любым перестановкам произвольной фиксации. Функция с несущественными переменными является симметрической, если ее проекция, задаваемая фиксацией, фиксирующей в точности ее существенные переменные, является симметрической

функцией. Класс всех симметрических интервально-постоянных функций будем обозначать через SICF. Класс симметрических интервально-постоянных функций с не более чем $c+1$ различными значениями обозначим через SICF_c. Подмножество SICF, состоящее из булевских монотонных функций, назовем множеством пороговых функций и обозначим через THR. Рассмотрим булевскую функцию, являющуюся дизъюнкцией некоторых своих переменных. Класс таких функций будем обозначать через OR. Очевидно, $\mathrm{OR} \subset \mathrm{THR}$.

Очевидно, пересечение классов псевдо-булевских монотонных функций и псевдо-булевских разбивающих функций не пусто и не совпадает ни с одним из этих классов. В некотором смысле ICF (наряду с псевдо-булевскими монотонными функциями) может пониматься как естественное псевдо-булевское обобщение класса булевских монотонных функций.

Псевдо-булевская функция над $\{0,1\}^{V_n}$, $V_n = \{x_1, \ldots, x_n\}$ называется *2-разделяемой*, если существует такая перестановка $(i_1, \ldots, i_n)$, что для переменных $y_1 = x_{i_1}, \ldots, y_n = x_{i_n}$ выполнено: a) если y_i не является существенной, то y_j не является существенной при $j > i$; b) если переменная y_{2i-1} является существенной и β — частичная фиксация, фиксирующая $\beta(y_{2i-1}) = 1$, то проекция f_β не зависит от переменной y_j при $j > 2i-1$; c) если переменная y_{2i} является существенной и β — частичная фиксация, фиксирующая $\beta(y_{2i-1}) = \beta(y_{2i}) = 0$, то проекция f_β не зависит от переменной y_j при $j > 2i$. Класс Φ функций будем называть *2-разделяемым*, если для любых $n, k \in \mathbb{N}$ класс $\Phi^{k,n}$ содержит 2-разделяемую функцию с k существенными переменными. Далее показано, что классы булевских монотонных функций и разбивающих функций являются 2-разделяемыми.

Описываемое исследование проведено в рамках *модели точной расшифровки при помощи запросов на значение функции*. В этой модели функция f от n переменных задана при помощи черного ящика и задача ученика (алгоритма расшифровки) состоит в том, чтобы расшифровать f, т.е. полностью восстановить ее таблицу значений. Чтобы расшифровать загаданную функцию, алгоритм расшифровки может делать *запросы на значение функции*, т.е. подавать произвольные наборы из $\{0,1\}^{V_n}$ черному ящику. Алгоритм расшифровки подает запросы блоками, учитель одновременно отвечает на все вопросы из одного блока. В *стандартной постановке* алгоритм расшифровки должен расшифровать загаданную функцию, использовав но возможности наименьшее число запросов на значение функции. В *параллельной постановке* алгоритм расшифровки должен минимизировать число блоков, требуемых для расшифровки.

В работе исследуется *сложность расшифровки* в худшем случае. Будем говорить, что алгоритм расшифровки класса Φ является *эффективным*

на Φ, если его сложность на Φ^n не более чем полиномиальна по n. Алгоритм является *параметро-эффективным на* Φ, если сложность алгоритма на $\Phi^{k,n}$ как функция от k и n слабо зависит от n.

Пусть Φ — некоторый класс псевдо-булевских функций. Будем говорить, что алгоритм *расшифровывает* класс Φ, если для любого $n \in \mathbb{N}$ он расшифровывает любую функцию из Φ^n при условии, что он получает n в виде входного параметра. Обозначим множество алгоритмов расшифровки класса Φ через $\mathcal{A}(\Phi)$. Любой элемент множества $\mathcal{A}(\Phi)$ можно понимать и как единичный алгоритм, получающий n на вход, и как последовательность алгоритмов, такую что n-й алгоритм последовательности расшифровывает функции из Φ^n. Такое определение удобно при рассмотрении асимптотического поведения сложности алгоритмов расшифровки.

Пусть $\varphi(A, f)$ — это число запросов на значение функции, требуемое алгоритму A для расшифровки функции f. Будем называть $\varphi(A, f)$ *сложностью алгоритма* A *на функции* f. Положим

$$\varphi(\Phi, n) = \min_{A \in \mathcal{A}(\Phi)} \max_{f \in \Phi^n} \varphi(A, f).$$

Заметим, что здесь используется min, а не inf, поскольку число алгоритмов расшифровки функций из Φ^n конечно. Будем называть величину $\max_{f \in \Phi} \varphi(A, f)$ сложностью алгоритма на классе Φ. Функцию $\varphi(\Phi, n)$ назовем *сложностью расшифровки* Φ. Если сложность алгоритма на Φ^n по порядку равна сложности расшифровки Φ при $n \to \infty$, будем говорить, что алгоритм A *оптимальный на* Φ.

Положим, что

$$\varphi(\Phi, n, k) = \min_{A \in \mathcal{A}(\Phi)} \max_{f \in \Phi^{k,n}} \varphi(A, f).$$

Заметим, что $\varphi(\Phi, n) = \varphi(\Phi, n, n)$. Функцию $\varphi(\Phi, n, k)$ будем называть *сложностью параметро-эффективной расшифровки класса* Φ. Если сложность алгоритма A на $\Phi^{k,n}$ по порядку равна сложности параметро-эффективной расшифровки Φ при $n, k \to \infty$, будем говорить, что алгоритм A является *оптимальным параметро-эффективным на* Φ.

Пусть $\varphi_p(A, f)$ — это число блоков запросов на значение функции, требуемых алгоритму A для расшифровки функции f. Величину $\varphi_p(A, f)$ будем называть *параллельной сложностью алгоритма* A *на функции* f. Величину $\max_{f \in \Phi} \varphi_p(A, f)$ назовем *параллельной сложностью алгоритма* A *на классе* Φ.

Обозначим $\mathcal{A}_q(\Phi, n, k) = \{A \in \mathcal{A}(\Phi) : \varphi(A, \Phi^{k,n}) \leq q\}$.

Положим

$$\varphi_p(\Phi, n, k, q) = \min_{A \in \mathcal{A}_q(\Phi, n, k)} \max_{f \in \Phi^{k,n}} \varphi_p(F, f).$$

Пусть Φ — некоторый класс псевдо-булевских функций. Будем говорить, что алгоритм *определяет существенные переменные* функций класса Φ, если для любого $n \in \mathbb{N}$ он находит существенные переменные любой функции из Φ^n при условии, что он получает n в виде входного параметра. Обозначим множество алгоритмов определения существенных переменных функций класса Φ через $\mathcal{B}(\Phi)$. Как и в случае расшифровки функций, любой элемент множества $\mathcal{B}(\Phi)$ можно понимать и как единичный алгоритм, получающий n на вход, и как последовательность алгоритмов, такую что n-й алгоритм последовательности расшифровывает функции из Φ^n.

Пусть $\psi(B, f)$ — это число запросов на значение функции, требуемое алгоритму B для определения существенных переменных функции f. Будем называть $\psi(B, f)$ *сложностью алгоритма B на функции f*. Положим

$$\psi(\Phi, n) = \min_{B \in \mathcal{B}(\Phi)} \max_{f \in \Phi^n} \psi(B, f).$$

Мы снова используем min, а не inf, поскольку число соответствующих алгоритмов для Φ^n конечно. Будем называть величину $\max_{f \in \Phi} \psi(B, f)$ сложностью алгоритма B на Φ. Функцию $\psi(\Phi, n)$ назовем *сложностью определения существенных переменных функций в* Φ. Если сложность алгоритма B на Φ^n по порядку равна сложности определения существенных переменных функций в Φ при $n \to \infty$, будем говорить, что алгоритм B *оптимальный на* Φ.

Положим, что

$$\psi(\Phi, n, k) = \min_{B \in \mathcal{B}(\Phi)} \max_{f \in \Phi^{k,n}} \psi(B, f).$$

Заметим, что $\psi(\Phi, n) = \psi(\Phi, n, n)$. Функцию $\psi(\Phi, n, k)$ будем называть *сложностью параметро-эффективного определения существенных переменных функций класса* Φ. Если сложность алгоритма B на $\Phi^{k,n}$ по порядку равна сложности параметро-эффективного определения существенных переменных функций из Φ при $n, k \to \infty$, будем говорить, что алгоритм B является *оптимальным параметро-эффективным на* Φ.

Пусть $\psi_p(B, f)$ — это число блоков запросов на значение функции, требуемых алгоритму B для определения существенных переменных функции f. Величину $\psi_p(B, f)$ будем называть *параллельной сложностью алгоритма B на функции f*. Величину $\max_{f \in \Phi} \psi_p(B, f)$ назовем *параллельной сложностью алгоритма B на классе* Φ.

Обозначим $\mathcal{B}_q(\Phi, n, k) = \{B \in \mathcal{B}(\Phi) : \psi(B, \Phi^{k,n}) \leq q\}$.

Положим

$$\psi_p(\Phi, n, k, q) = \min_{B \in \mathcal{B}_q(\Phi, n, k)} \max_{f \in \Phi^{k,n}} \psi_p(F, f).$$

В главе 1 исследуется сложность определения существенных переменных различных классов псевдо-булевских функций. Для классов монотонных, разбивающих и интервально-постоянных функций получены порядки сложности определения существенных переменных.

Теорема 1. *Имеет место асимптотическое равенство* $\psi(\Psi, n, k) \asymp k \log n$ *при* $n, k \to \infty$ *и* $2^k = O(k \log n)$, *где* $\Psi \in \{\mathrm{PM}, \mathrm{M}, \mathrm{SPL}, \mathrm{ICF}\}$.

Для разбивающих функций построен алгоритм ответов на запросы на значение функции, позволивший в случае малого числа существенных переменных получить асимптотику сложности определения существенных переменных.

Теорема 2. *Имеет место асимптотическое равенство*

$$\psi(\mathrm{SPL}, n, k) \sim k \log n$$

при $n, k \to \infty$ *и* $2^k = o(k \log n)$.

Для полных разбивающих функций при малом и большом числе существенных переменных получены асимптотики сложности определения существенных переменных, отличные от оценок в общем случае.

Теорема 3. *Пусть* $k = \log_2 \log n + \beta(n)$, $2^{\beta(n)} \to 0$ *при* $n \to \infty$. *Тогда*

$$\psi(\mathrm{CSPL}, n, k) \sim \log n.$$

Теорема 4. *При* $k \sim n$, $n \to \infty$ *выполнено*

$$\psi(\mathrm{CSPL}, n, k) \sim n.$$

Для получения оценок сложности параллельной расшифровки введено понятие 2-разделяемых функций и показано, что как класс разбивающих функций, так и класс монотонных функций являются 2-разделяемыми (т.е. содержат 2-разделяемые функции), откуда классы псевдо-булевских монотонных функций и интервально-постоянных функций также являются 2-разделяемыми. Для 2-разделяемых классов функций построен алгоритм ответов на запросы на значение функции, позволивший получить порядок параллельной сложности определения существенных переменных таких функций, т.е. доказать следующую теорему.

Теорема 5. *Для $k, n \in \mathbb{N}$ и произвольной константы $c > 2$, такой что $2^k < (\frac{c}{2} - 1)k \log n$, выполнено*

$$\psi_p(\Psi, n, k, c \cdot k \log n) \asymp k$$

при $k, n \to \infty$, где $\Psi \in \{\mathrm{PM}, \mathrm{M}, \mathrm{SPL}, \mathrm{ICF}\}$.

В главе 2 исследуется сложность параметро-эффективной расшифровки классов псевдо-булевских функций. Для различных классов интервально-постоянных функций, в частности, для классов монотонных и разбивающих функций, получены мощностные нижние оценки сложности параметро-эффективной расшифровки таких классов. Предложен универсальный алгоритм параметро-эффективной расшифровки интервально-постоянных функций, оптимальный по порядку на различных подклассах класса интервально-постоянных функций.

Теорема 6. *Пусть $\Phi \subseteq \mathrm{ICF}$, $A \in \mathcal{A}(\Phi)$ и для некоторой функции $\xi(n)$ выполнено $\varphi(A, \Phi^n) = O(\xi(n))$ при $n \to \infty$. Тогда существует такой алгоритм расшифровки $A' \in \mathcal{A}(\Phi)$, что $\varphi(A', \Phi^{k,n}) = O(k \log n + \sum_{i=1}^{k} \xi(i))$ при $n, k \to \infty$.*

Упомянутые нижние оценки и алгоритм расшифровки позволили получить асимптотические оценки сложности параметро-эффективной расшифровки для многих подклассов интервально-постоянных функций.

Теорема 7. *Имеют место следующие асимптотические равенства*

- $\varphi(\mathrm{ICF}, n, k) \asymp \varphi(\mathrm{PM}, n, k) \asymp \varphi(\mathrm{SPL}, n, k) \asymp k \log n + 2^k$ *при* $n, k \to \infty$,
- $\varphi(\mathrm{M}, n, k) \asymp k \log n + \frac{2^k}{\sqrt{k}}$ *при* $n, k \to \infty$,
- $\forall c = const \;\; \varphi(\mathrm{SICF}_c, n, k) \asymp \varphi(\mathrm{THR}, n, k) \asymp \varphi(\mathrm{OR}, n, k) \asymp k \log n$ *при* $n \to \infty$ *и* $\log k = o(\log n)$.

В главе 3 исследуется параллельная сложность параметро-эффективных алгоритмов расшифровки псевдо-булевских функций. Предложен параметро-эффективный алгоритм расшифровки интервально-постоянных функций с небольшой параллельной сложностью и показано, что для некоторых подклассов класса интервально-постоянных функций этот алгоритм имеет как оптимальную сложность, так и оптимальную параллельную сложность.

Теорема 8. *Пусть* $\Phi \subseteq \mathrm{ICF}$. *Существует такой алгоритм* $A \in \mathcal{A}(\Phi)$, *что* $\varphi(A, \Phi^{k,n}) = O(k \log n + 2^k)$ *при* $n, k \to \infty$ *и* $\varphi_p(A, \Phi^{k,n}) = O(k)$ *при* $n, k \to \infty$.

В частности, при некоторых ограничениях это относится к классам булевских монотонных функций, псевдо-булевских монотонных функций, разбивающих функций и интервально-постоянных функций в целом.

Теорема 9. *Пусть* $\Phi \subseteq \mathrm{ICF}$. *Тогда для любого* $A \in \mathcal{A}(\Phi)$ *выполнено* $k \log n = O(\varphi(A, \Phi^{k,n}))$ *при* $n, k \to \infty$. *Если для некоторого* $A \in \mathcal{A}(\Phi)$ *выполнено* $\varphi(A, \Phi^{k,n}) = O(k \log n)$, *то* $k = O(\varphi_p(A, \Phi^{k,n}))$ *при* $k \to \infty$, *где* $\Phi \in \mathrm{ICF}, \mathrm{PM}, \mathrm{SPL}, \mathrm{M}$.

Другими словами, любой оптимальный на $\Phi^{k,n}$ алгоритм расшифровки из $\mathcal{A}(\Phi)$ имеет параллельную сложность на $\Phi^{k,n}$, большую или равную k по порядку при $n \to \infty$ и $2^k = O(k \log n)$, где $\Phi \in \mathrm{ICF}, \mathrm{PM}, \mathrm{SPL}, \mathrm{M}$.

Для данных классов получен порядок сложности параллельной расшифровки для оптимальных по порядку в смысле обычной сложности параметро-эффективных алгоритмов расшифровки.

Теорема 10. *Для* $k, n \in \mathbb{N}$ *и произвольной константы* $c > 2$, *такой что* $2^k < (\frac{c}{2} - 1) k \log n$, *выполнено*

$$\varphi_p(\Phi, n, k, c \cdot k \log n) \asymp k$$

при $k, n \to \infty$, *где* $\Phi \in \mathrm{ICF}, \mathrm{PM}, \mathrm{SPL}, \mathrm{M}$.

Последняя теорема есть следствие теорем 8 и 9 и утверждает, что алгоритм из теоремы 8 имеет минимальную по порядку параллельную сложность на $\Phi^{k,n}$ среди всех оптимальных на $\Phi^{k,n}$ алгоритмов из $\mathcal{A}(\Phi)$ при $n \to \infty$ и $2^k = O(k \log n)$, где $\Phi \in \mathrm{ICF}, \mathrm{PM}, \mathrm{SPL}, \mathrm{M}$.

Благодарности

Я выражаю глубокую благодарность своему научному руководителю профессору Гасанову Эльяру Эльдаровичу за постановку задач и помощь в работе. Выражаю благодарность заведующему кафедрой математической теории интеллектуальных систем академику, профессору Валерию Борисовичу Кудрявцеву и всему коллективу кафедры за творческую атмосферу, способствующую исследовательской работе. Благодарю своих родителей, Владимира Викторовича Осокина и Аллу Васильевну Осокину, за поддержку.

Публикации автора по теме диссертации

1. Осокин В.В.: *Асимптотически оптимальный алгоритм расшифровки разбиения булевого куба на подкубы*, Интеллектуальные системы, том 11, вып. 1-4, стр. 635-652 (2007).

2. Осокин В.В.: *О сложности расшифровки разбиения булевого куба на подкубы*, Дискретная математика, том 20, вып. 2, стр. 46-62 (2008).

3. Осокин В.В., Воронин Б.В: *О сложности расшифровки существенных переменных функции, задающей разбиение булевого куба*, Интеллектуальные системы, том 12, вып. 1-4, стр. 159-178 (2008). Осокину В.В. принадлежат доказательства лемм 4.1, 4.2, 5.1, утверждений 6.1 и 6.2 и частично доказательство теорем 2.1, 2.2, 6.1.

4. Осокин В.В.: *О параллельной расшифровке разбиений булевого куба*, Интеллектуальные системы, том 13, вып. 1-4, стр. 427-454 (2009).

5. Осокин В.В.: *Сложность расшифровки монотонных функций с малым числом существенных переменных*, Дискретная математика, том 22, вып. 3, стр. 134-145 (2010).

6. Осокин В.В.: *О параллельной параметро-эффективной расшифровке псевдо-булевских функций*, Интеллектуальные системы, том 14, вып. 1-4, стр. 395-424 (2010).

7. Osokin V.V.: *On the complexity of decoding Boolean cube splitting into cube faces.* Discrete Mathematics and Applications. Volume 18, Issue 3, Pages 155-172, 2008.

8. Osokin V.V.: *On learning monotone Boolean functions with irrelevant variables.* Discrete Mathematics and Applications. Volume 20, Issue 3, Pages 307-320, 2010.

9. Осокин В.В.: *Асимптотика сложности разбиения булевого куба на подкубы.* Материалы IX Международной конференции «Интеллектуальные системы и компьютерные науки» (Москва, 23-27 октября 2006 г.), том 1, часть 1, с. 191-193.

10. Осокин В.В.: *О расшифровке разбиения булевого куба на грани.* Материалы IX Международного семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения академика О.Б.Лупанова (Москва, 18-23 июня 2007 г.), с. 343-346.

11. Осокин В.В.: *Расшифровка k-существенных монотонных функций.* Международная конференция «Современные проблемы математики, механики и их приложений», посвященная 70-летию ректора МГУ академика В.А.Садовничего (30 марта - 2 апреля 2009г., Москва). Материалы конференции. С. 367-368.

12. Осокин В.В.: *О расшифровке одного класса дискретных функций.* Материалы Международного семинара "Дискретная математика"(Москва, 1-5 февраля 2010 г.). 394-396.

13. Осокин В.В.: *О расшифровке существенных переменных дискретных функций.* Сборник тезисов XVI Международной конференции студентов, аспирантов и молодых ученых «Ломоносов-2009», секция «Математика и механика» (Москва, 13-18 апреля 2009). С. 51-52.

14. Осокин В.В.: *Расшифровка обобщенных псевдо-булевских монотонных функций.* Сборник тезисов XVII Международной конференции студентов, аспирантов и молодых ученых «Ломоносов-2010», секция «Вычислительная математика и кибернетика» (Москва, 12-15 апреля 2010). С. 36-37.