МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М.В. ЛОМОНОСОВА

УДК 519.712.2

На правах рукописи

Поцелуевская Евгения Александровна

Алгоритмы поиска решения задачи об F-выполнимости, основанные на приближении булевых функций к классам Шефера

Специальность 01.01.09 - Дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва - 2012

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

Научный руководитель:	кандидат физико-математических наук Носов Валентин Александрович
Официальные оппоненты:	Кузюрин Николай Николаевич, доктор физико-математических наук Институт системного программирования РАН заведующий отделом, профессор
	Тарасов Алексей Вячеславович кандидат физико-математических наук Институт криптографии, связи и информатики Академии ФСБ России начальник кафедры
Ведущая организация:	Национальный исследовательский университет «МЭИ»

Защита состоится 25 мая 2012 г. в 16-45 на заседании диссертационного совета Д.501.001.84 при Московском государственном университете имени М.В. Ломоносова по адресу: Российская Федерация, 119991, Москва, Ленинские горы, д.1, МГУ имени М.В. Ломоносова, Механико-математический факультет, аудитория 14-08.

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

Автореферат разослан 25 апреля 2012 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 выполнимости булевых формул является одной из классических задач дискретной математики и формулируется следующим образом. Дана формула над булевыми переменными $x_1, \ldots, x_n$, имеющая вид:

$$(x_{i_1}^{\alpha_1} \vee \cdots \vee x_{i_k}^{\alpha_k})(x_{j_1}^{\beta_1} \vee \cdots \vee x_{j_l}^{\beta_l}) \ldots (x_{t_1}^{\gamma_1} \vee \cdots \vee x_{t_p}^{\gamma_p}),$$

где ($\alpha_i, \beta_i, \ldots, \gamma_i$ - булевы константы). Необходимо определить, существует ли набор значений переменных $x_1 = \sigma_1, \ldots, x_n = \sigma_n$, обращающий формулу в единицу.

В 1971 году Стивеном Куком был доказан фундаментальный для теории сложности вычислительных систем результат[1], заключающийся в том, что задача о выполнимости является NP-полной. Тем самым был поднят вопрос о равенстве классов сложности P и NP, который остаётся открытым до сих пор.

Вскоре было установлено, что для некоторых классов функций существуют алгоритмы, позволяющие решить задачу за полиномиальное время, к таким классам, в частности, относятся функции, где в записи в конъюнктивной нормальной форме (КНФ) в каждой дизъюнкции задействовано не более 2 переменных (2-КНФ)[2], класс функций, КНФ которых состоит из дизъюнктов Хорна[3], а также ряд других классов[4].

Алгоритмы для поиска решения задачи о выполнимости появлялись начиная с 60-х годов прошлого века и продолжают активно исследоваться вплоть до сегодняшнего дня. Обзор наиболее заметных результатов в этой области можно найти в монографиях *Handbook of Satisfiability*[5],

---

[1] Cook S.A. The Complexity of Theorem Proving Procedures // Proc. 3rd Ann. ACM Symp. on Theory of Computing (STOC 71). – 1971. – P. 151-158

[2] Even S., Itai A., Shamir A. On the complexity of timetable and multi-commodity flow problems // SIAM Journal of Computing. – No. 5(4). – 1976

Aspvall B., Plass M.F., Tarjan R.E. A linear-time algorithm for testing the truth of certain quantified boolean formulas // Information Processing Letters. – No. 8(3). – March 1979. – P. 121-123

[3] Dowling W.F., Gallier J.H. Linear-time algorithms for testing the satisfiability of propositional Horn formulas // Journal of Logic Programming. – No. 1(3). – 1984. –P. 267-284

[4] Franco J., Gelder A.V. A perspective on certain polynomial-time solvable classes of satisfiability // Discrete Applied Mathematics. – Vol. 125. – Issues 2-3. –2003. – P. 177-214

Алексеев В.Б., Носов В.А. NP-полные задачи и их полиномиальные варианты. Обзор // Обозрение прикладной и промышленной математики. – 1997. – Т. 4. – Вып. 2. – С. 165-193

[5] Biere A., Heule M., van Maaren H., Walsh T., eds. Handbook of Satisfiability. // Vol. 185 of Frontiers in Artificial Intelligence and Applications. – IOS Press, 2009. – 981 pp.

Introduction to mathematics of satisfiability[6], в работе Всемирнова М.А., Гирша Э.А., Данцина Е.Я. и Иванова С.В. «Алгоритмы для пропозициональной выполнимости и верхние оценки их сложности»[7], в сборнике Дингжу, Гу и Пардалоса *Satisfiability problem: theory and applications*[8].

К наиболее распространенным техникам решения задачи относятся: детерминированные алгоритмы класса DPLL, основанные на на процедурах, описанных в работах Дэвиса и Патнема[9] и Дэвиса, Лоджмана и Лавлэнда[10]; вероятностные алгоритмы класса PPSZ[11]; вероятностные алгоритмы, основанные на случайных блужданиях, и, в частности, алгоритм Шонинга[12]; детерминированные алгоритмы, полученные дерандомизацией вероятностных алгоритмов[13].

Также интерес представляет нахождение классов функций, для которых возможно полиномиальное решение задачи об F-выполнимости, которая является обобщением задачи выполнимости и частным случаем задачи выполнимости систем ограничений (constraint satisfaction problem, CSP). Задача формулируется следующим образом: дано $F = F_1, \ldots, F_s$ - любое конечное множество формул (функциональных символов). F-формула определяется как конъюнкция $F_{i_1}(\cdot)F_{i_2}(\cdot)\ldots F_{i_t}(\cdot)$ с переменными $x_1, \ldots, x_n$, расставленными некоторым образом. Необходимо определить существует ли набор значений переменных, обращающий F-формулу в единицу. Задача об F-выполнимости полиномиально сводится к задаче о выполнимости и основное её отличие от задачи о выполнимости заключается в том, что она имеет другую длину входа.

---

[6]Marek V. W. Introduction to mathematics of satisfiability. – CRC Press, 2009. – 365 p.

[7]Всемирнов М.А., Гирш Э.А., Данцин Е.Я., Иванов С.В. Алгоритмы для пропозициональной выполнимости и верхние оценки их сложности // Теория сложности вычислений. VI, Зап. научн. сем. ПОМИ, 277, ПОМИ, СПб. – 2001

[8]Dingzhu Du, Jun Gu, Panos M. Pardalos. Satisfiability problem: theory and applications // Proceedings of a DIMACS workshop, March 11-13 1996. – 1996

[9]Davis M., Putman H. A computing procedure for quantification theory // Journal of the ACM. – 1960. – No. 7(3). – P. 201-215

[10]Davis M., Logeman G., Loveland D. A machine program for theorem-proving // Communications of the ACM. – 1962. – No. 5(7). – P. 394-397

[11]Paturi R., Pudlák P., Saks M.E., Zane F. An improved exponential-time algorithm for k-SAT // Journal of the ACM. – Vol. 52. – No. 3. – 2005. – P. 337-36

[12]Shöning U. A probabilistic algorithm for k-SAT and constraint satisfaction problems // Proceedings of FOCS'99. – 1999. – P. 410-414

[13]Dantsin E., Goerdt A., Hirsch E. A., Kannan R., Kleinberg J., Papadimitriou C., Raghavan O., Schoning U. A deterministic $(2 - 2/(k + 1))^n$ algorithm for k-SAT based on local search // Theoretical Computer Science. – Vol. 289. – Issue 1. – P. 69–83. – 2002

В работе *The complexity of satisfiability problems*[14] Шефер выделил следующие 6 классов булевых функций, для которых обобщенная проблема F-выполнимости решается за полиномиальное время:

- 0-выполнимые функции (0-ВЫП): все функции f, для которых верно: $f(0,\ldots,0)=1$;
- 1-выполнимые функци (1-ВЫП)и: все функции f, для которых верно $f(1,\ldots,1)=1$;
- слабоотрицательные функции (СЛО): все функции f, для которых существует запись в КНФ, в которой каждый дизъюнкт содержит только переменные с отрицаниями кроме, быть может, одной (также известны как дизъюнкты Хорна), т.е. формула вида:

  $$(x_{i_1}^{\alpha} \vee \bar{x_{i_2}} \vee \cdots \vee \bar{x_{i_k}})(x_{j_1}^{\beta} \vee \bar{x_{j_2}} \vee \cdots \vee \bar{x_{j_l}}) \ldots (x_{t_1}^{\gamma} \vee \bar{x_{t_2}} \vee \cdots \vee \bar{x_{t_k}}),$$

  где $(\alpha,\beta,\ldots,\gamma$ - булевы константы).
- слабоположительные функции (СЛП): все функции f, для которых существует запись в КНФ, в которой каждый дизъюнкт содержит только переменные без отрицаний, кроме, быть может, одной, т.е. формула вида:

  $$(x_{i_1}^{\alpha} \vee x_{i_2} \vee \cdots \vee x_{i_k})(x_{j_1}^{\beta} \vee x_{j_2} \vee \cdots \vee x_{j_l}) \ldots (x_{t_1}^{\gamma} \vee x_{t_2} \vee \cdots \vee x_{t_k}),$$

  где $(\alpha,\beta,\ldots,\gamma$- булевы константы).
- мультиаффинные функции (МАФ): все функции f, которым соответствует формула, представляющая собой конъюнкцию линейных форм, т.е. формула вида:

  $$(a_1x_1 + \ldots a_nx_n + a_0)(b_1x_1 + \ldots b_nx_n + b_0) \ldots (c_1x_1 + \ldots c_nx_n + c_0),$$

  где $(a_i, b_i, \ldots, c_i$ - булевы константы).
- биюнктивные функции (БИН): все функции f, для которых существует запись в КНФ, где каждая скобка содержит ровно две переменные, т.е. формула вида

  $$(x_{i_1}^{\alpha_1} \vee x_{i_2}^{\alpha_2})(x_{j_1}^{\beta_1} \vee x_{j_2}^{\beta_2}) \ldots (x_{t_1}^{\gamma_1} \vee x_{t_2}^{\gamma_2}),$$

[14]Schaefer T.J. The complexity of satisfiability problems // Proceedings of the 10th ACM Symposium on Theory of Computing. – 1978. – P. 216-226

где ($\alpha_i, \beta_i, \ldots, \gamma_i$- булевы константы).

Вопрос о размерах и свойствах классов Шефера глубоко изучался начиная с момента описания этих классов самим Шефером. В частности, значительный вклад в изучение данного вопроса внесли работы Алексеева В.Б.,Горшкова С.П, Гизунова С.А, Носова В.А и Тарасова А.В.[15]. Среди зарубежных авторов наиболее весомый вклад в эту область внесли работы Нади Крейгноу, Стефана Рейта, Эльмара Бёлера, и других соавторов [16].

---

[15]Алексеев В.Б. О числе семейств подмножеств, замкнутых относительно пересечения // Дискретная математика. – 1989. – Т. 1. – Вып. 2. – С. 129-136.

Алексеев В.Б., Носов В.А. NP-полные задачи и их полиномиальные варианты. Обзор // Обозрение прикладной и промышленной математики. – 1997. – Т. 4. – Вып. 2. – С. 165-193.

Гизунов С.А., Носов В.А. Сложность распознавания классов Шефера // Вестник МГУ. – 1995. – Сер. 1.

Гизунов С.А., Носов В.А. О классификации всех булевых функций 4-х переменных по классам Шефера // Обозрение прикладной и промышленной математики. – 1995. – Т. 1. – Вып. 3. – С. 440-467

Горшков С.П. Применение теории NP-полных задач для оценки сложности решения систем булевых уравнений // Обозрение прикладной и промышленной математики. – 1995. – Т. 1. – Вып. 3. – С. 325-398

Горшков С. П. О сложности распознавания мультиаффинности, биюнктивности, слабой положительности и слабой отрицательности булевых функций // Обозрение прикладной и промышленной математики. Серия «Дискретная математика». – 1997. – Т. 4. – Вып. 2. – С. 216–237

Горшков С.П. О сложности задачи нахождения числа решений систем булевых уравнений // Дискретная математика. – 1996. – Т. 8. – Вып. 1. – С. 72–85

Горшков С.П. О пересечении классов мультиаффинных, биюнктивных, слабо положительных и слабо отрицательных булевых функций // Обозрение прикладной и промышленной математики. Серия «Дискретная математика». ТВП. – 1997. – Т. 4. – Вып. 2. – С. 238-259

Горшков С.П., Тарасов А.В. О максимальных группах инвариантных преобразований мультиаффинных, биюнктивных, слабо положительных и слабо отрицательных булевых функций // Дискретная математика. – 2009. – Т. 21. – Вып. 2. – С. 94-101

[16]Böhler E., Creignou N., Reith S., Vollmer H. Playing with Boolean blocks, part I: Post's lattice with applications to complexity theory // SIGACT News, Complexity Theory. – 2003. – Column 42, 34(4). – P. 38-52

Böhler E., Creignou N., Reith S., Vollmer H. Playing with Boolean blocks, part II: Constraint satisfaction problems // SIGACT News, Complexity Theory. – 2004. – Column 43, 35(1). – P. 22-35

Creignou N., Hermann J. Complexity of generalized satisfiability counting problems // Information and Computation. – 1996. - V. 125 – No. 1. – P. 1-12

Creignou N., Hebrard J. On generating all satisfying truth assignments of a generalized CNF-formula // Theoretical Informatics and Applications. – 1997. – V. 31. – No. 6. - P. 499-511

Creignou N., Hermann M. Complexity of constraint satisfaction problems// Survey Document for CP 2001 Tutorial. - 2001. - 33 pp

Creignou N., Khanna S., Sudan M. Complexity classifications of Boolean constraint satisfaction problems // SIAM Monographs on Discrete Mathematics and Applications/ SIAM, Philadelphia. – 2001. – 106 pp

Поиск случаев, когда задачи выполнимости и F-выполнимости решаются за полиномиальное время, важен и для многих прикладных задач. В частности, тесты, основанные на проблеме выполнимости сегодня широко применяются для автоматизации проектирования, а также для проверки разрабатываемых программ. К прикладным задачам, для решения которых применяется данная проблема, также относятся: определение перекрестных помех в интегральных схемах[17], верификация моделей для параллельных систем с конечным числом состояний[18], вывод гаплотипа в биоинформатике[19], а также многие другие задачи[20]. С другой стороны, выявление сложных случаев задачи о выполнимости, представляет интерес для построения эффективных систем защиты информации.

В диссертации рассматривается вопрос изучения некоторых частных свойств классов Шефера, которые могли бы быть полезными для быстрого решения задачи об F-выполнимости или, напротив, для формирования задач, сложных для решения, а также вопрос построения алгоритмов поиска решения задачи об F-выполнимости, основанных на свойствах классов Шефера.

Актуальность диссертационной работы определяется теоретической значимостью задачи о выполнимости для области дискретной математики, а также широким практическим применением задачи о выполнимости, что делает востребованными алгоритмы, позволяющие для некоторых классов функций решать данную задачу за полиномиальное время.

Цель работы и задачи исследования. Цель диссертации состоит в разработке новых алгоритмов решения задачи о выполнимости, основанных на классах Шефера, и в изучении свойств классов Шефера.

Creignou N. Boolean CSP. – Universite de la Mediterranee, 2006. – 82 pp

Reith S., Wagner K.W. The Complexity of Problems Defined by Subclasses of Boolean Functions // Technical Report 218, Lehrstuhl für Theoretische Informatik. – Universität Würzburg. – January 1999

[17]Chen P., Keutzer K. Towards true crosstalk noise analysis // International Conference on Computer-Aided Design. – November 2009. – P. 132-138

[18]Biere A., Cimatti A., Clarke E., Zhu Y. Symbolic model checking without BDDs // Tools and Algorithms for the Construction and Analysis of Systems. – May 2009. – P. 193-207

Sheeran M., Singh S., Stalmarck G. Checking safety properties using induction and a SAT solver // Formal Methods in Computer-Aided Disign. – 2000. –P. 108-125

Mcmillan K.L. Interpolation and SAT-based model checking // Computer-Aided Verification. – 2003. – P. 1-13

[19]Lynce I., Marques-Silva J. Efficient haplotype inference with Boolean satisfiability // National Conference on Artificial Intelligence. – July 2006

[20]Marques-Silva, J. Practical Applications of Boolean Satisfiability // Workshop on Discrete Event Systems (WODES'08), Goteborg, Sweden. – May 2008

К задачам, подлежащим исследованию в рамках диссертации, относятся:

1. Анализ существующих результатов (как теоретических, так и практических) в области решения задачи о выполнимости булевых формул.

2. Исследование свойств классов Шефера с точки зрения возможности использования этих свойств для решения задачи об F-выполни -мости.

3. Разработка алгоритмов решения задачи об F-выполнимости с использованием свойств классов Шефера.

4. Практическая реализация алгоритмов решения задачи об F-выполнимости и сбор статистической информации о времени работы программ для различных входных данных с целью проверки быстродействия разработанных алгоритмов.

Методы исследования. В работе используются методы теории булевых функций, теории графов, теории вероятностей и теории сложности. Разработанные алгоритмы основаны на сочетании перебора значений для определенного подмножества S переменных x_i, задействованных в F-формуле, и решении при каждом фиксированном наборе из S полиномиальной подзадачи для соответствующего класса Шефера. Также для одного из алгоритомов для ускорения работы была рассмотрена модификация классического метода «разделяй и властвуй» для решения сложных задач путем разбиения на простые подзадачи.

Научная новизна. Результаты работы являются новыми. В диссертации получены следующие основные результаты:

1. Установлены свойства классов Шефера, которые могу быть использованы для решения задачи об F-выполнимости. В частности, определена классификация по принадлежности функций к различным классам Шефера для функций из классов, получаемых путем расширения классов слабоотрицательных, слабоположительных, мультиаффинных и биюнктивных функций. Расширение осуществлялось путем добавления к классу Шефера произвольной функции и замыкания полученного множества. Данный результат

предоставляет метод для построения сложных случаев задачи об F-выполнимости.

2. Разработаны алгоритмы решения задачи об F-выполнимости булевых формул, основанные на приближении функций к классам БИН, СЛО, СЛП и МАФ (в зависимости от способа задания исходной формулы), а также алгоритм решения задачи об F-выполнимости, основанный на применении метода «разделяй и властвуй». Для всех алгоритмов разработаны программы, результаты работы которых свидетельствуют об эффективности алгоритмов.

Теоретическая и практическая ценность результатов. Работа имеет теоретический характер. Её результаты работы могут найти применение в теории булевых функций в вопросе дальнейшего исследования свойств классов Шефера. Практические результаты диссертации также могут найти применение в областях, где имеет значение быстрое решение задачи о выполнимости (в частности, для автоматизации проектирования и проверки программ), а также в области защиты информации (предложена криптосистема с открытым ключом на базе задачи об F-выполнимости). Конкретные программные реализации алгоритмов не претендуют на место универсальных решателей задач о выполнимости, так как их быстродействие основано только на близости функций к классам Шефера. Однако в сочетании с другими алгоритмами, которые быстро работают для других классов задач, использованные подходы могут быть задействованы в программных решателях задачи о выполнимости, которые широко применяются на практике.

Апробация и внедрение результатов. Результаты диссертации докладывались на следующих конференциях и семинарах:

- Международная конференция студентов, аспирантов и молодых ученых «Ломоносов 2011» (апрель 2011);
- Международный семинар «Дискретная математика-2010» (февраль 2010);
- Международная конференция студентов, аспирантов и молодых ученых «Ломоносов 2009» (апрель 2009);

- Международная конференция «Современные проблемы математики, механики и их приложения», посвященная 70-летию ректора МГУ академика В.А. Садовничего (апрель 2009);

- Международная конференция студентов, аспирантов и молодых ученых «Ломоносов 2008» (апрель 2008);

- Научно-исследовательский семинар кафедры Математической теории интеллектуальных систем «Теория автоматов» (2008-2012, неоднократно).

Кроме того, разработка алгоритма решения задачи об F-выполнимости функций, заданных в КНФ и зависящих не более, чем от трех переменных, осуществлялась в рамках исследовательского проекта по государственному контракту. Работа была успешно принята заказчиком с целью дальнейшего практического применения.

Публикации. Результаты диссертации опубликованы в 5 работах автора, перечень которых приведен в конце автореферета [1-5].

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения и списка литературы из 70 наименований (включая работы автора). Общий объем диссертации – 135 страниц. В работе содержится 8 рисунков и 12 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во **Введении** приводится общая постановка задачи, а также краткое описание результатов диссертации.

В **Главе 1** приведен обзор различных формулировок задачи о выполнимости, а также известных алгоритмов её решения, включая результаты последних лет. Обзор основан на результатах работы Алексеева В.Б. и Носова В.А «NP-полные задачи и их полиномиальные варианты» по проблеме NP-полноты, обзоре дискретных алгоритмов решения задачи Всемирнова М.А., Гирша Э.А., Данцина Е.Я. и Иванова С.В «Алгоритмы для пропозициональной выполнимости и верхние оценки их сложности», на статьях из сборника Дингжу, Гу и Пардалоса *Satisfiability problem: theory and applications*, монографиях *Handbook of Satisfiability*, *Introduction to mathematics of satisfiability* и других работах. Из обзора следует, что несмотря на то, что основные методы решения задачи

пропозициональной выполнимости были заложены ещё в 60-70х годах прошлого века, эта тема имеет активное развитие и сегодня, в частности ежегодно проводятся соревнования для программных решателей задачи[21]. Статистические данные о практической работе этих программ показывают, что для значительной части формул задача всё же может быть решена за полиномиальное время.

В **Главе 2** исследуются некоторые частные свойства классов Шефера, которые могли бы быть полезными для быстрого решения задачи об F-выполнимости или, напротив, для формирования задач, сложных для решения, а также раскрывается вопрос сведения произвольных булевых функций к классам Шефера путем фиксации переменных.

Если рассмотреть оператор замыкания относительно операций, используемых для составления F-формул $[\cdot]$ (переименование переменных, склеивание переменных, конъюнкция), то классы Шефера будут замкнуты относительно этого оператора. Для этого оператора приводится доказательство следующей теоремы:

Теорема 2.1 *Пусть C - один из классов Шефера (0-ВЫП, 1-ВЫП, СЛП, СЛО, МАФ, БИН), $g \notin C$. Тогда существует $h \in [C \cup \{g\}]$, $h \neq 0$, такая что $h \notin \{0\text{-ВЫП} \cup 1\text{-ВЫП} \cup \text{СЛП} \cup \text{СЛО} \cup \text{МАФ} \cup \text{БИН}\}$.*

Далее в главе рассматривается вопрос классификации булевых функций, получаемых из классов Шефера путем добавления к соответствующему классу произвольной функции и замыкания данного множества относительно оператора [.]. Каждой булевой функции f сопоставляется вектор распределения этой функции по четырем классам Шефера $\delta^f = (\delta_1^f, \delta_2^f, \delta_3^f, \delta_4^f)$, где:

- $\delta_1^f = 1$ при $f \in$ СЛО, $\delta_1^f = 0$ при $f \notin$ СЛО;
- $\delta_2^f = 1$ при $f \in$ СЛП, $\delta_2^f = 0$ при $f \notin$ СЛП;
- $\delta_3^f = 1$ при $f \in$ МАФ, $\delta_3^f = 0$ при $f \notin$ МАФ;
- $\delta_4^f = 1$ при $f \in$ БИН, $\delta_4^f = 0$ при $f \notin$ БИН.

Теорема 2.2 *Пусть для ненулевых функций f и g известны векторы распределения по классам Шефера δ^f и δ^g соответственно. Тогда:*

[21] http://www.satcompetition.org

1. *Если* $(\delta_i^g, \delta_i^f) \in \{(0,0),(0,1),(1,0)\}$, *то существует* $h \in [\{f,g\}]\backslash([\{f\}]\bigcup[\{g\}])$, *такую что* $\delta_i^h = 0$.

2. *Если* $(\delta_i^g, \delta_i^f) = (1,1)$, *то для всех* $h \in [\{f,g\}]$: $\delta_i^h = 1$.

Следствие 2.1 *Пусть* C *- класс Шефера (один из классов СЛО, СЛП, МАФ, БИН). Для ненулевой функции* g *известен вектор ее распределения по классам Шефера* δ^g. *Тогда:*

1. *Если существует* $f \in C$, *такая что* $(\delta_i^g, \delta_i^f) \in \{(0,0),(0,1),(1,0)\}$, *то существует* $h \in [C\bigcup\{g\}]\backslash[\{g\}]$: $\delta_i^h = 0$, *то есть* h *не принадлежит классу, соответствующему номеру* i.

2. *Если существует* $f \in M$, *такая что* $(\delta_i^g, \delta_i^f) = (1,1)$, *то существует* $h \in [C\bigcup\{g\}]\backslash[\{g\}]$: $\delta_i^h = 1$, *то есть* h *принадлежит классу, соответствующему номеру* i.

Исходя из этого, а также из результатов, изложенных в работе «Сложность распознавания классов Шефера» С.А. Гизунова и В.А. Носова, была проведена классификация функций h, получаемых путем расширения классов Шефера.

Далее пусть для булевой функции $f(x_1,\ldots,x_n)$ известно, к каким классам Шефера она принадлежит. Выясним, к каким классам Шефера будет принадлежать функция g, полученная из f фиксацией переменных. Без потери общности, будем считать, что зафиксированы переменные $x_1 = \sigma_1, \ldots, x_k = \sigma_k$.

Теорема 2.3 *Если* $f \in$ *0-ВЫП, то:*

- *при* $(\sigma_1,\ldots,\sigma_k) = (0,\ldots,0)$, *функция* $g \in$*0-ВЫП;*
- *при* $(\sigma_1,\ldots,\sigma_k) \neq (0,\ldots,0)$ *функция* $g \in$ *0-ВЫП тогда и только тогда, когда* $f(\sigma_1,\ldots,\sigma_k,0,\ldots,0) = 1$;
- *В случае, если известен набор фиксируемых переменных и их значения:* $(x_{i_1},\ldots,x_{i_k}) = (\sigma_1,\ldots,\sigma_k)$, *вероятность того, из произвольной функции* $f \in$*0-ВЫП указанной фиксацией переменных можно получить* $g \in$*0-ВЫП равна*

$$P_0 = \frac{2^{2^{n-k}-1}}{2^{2^n-1}}.$$

- *Вероятность получить из 0-выполнимой функции веса* $\|f\| = N$ *0-выполнимую функцию* g *произвольной фиксацией переменных составляет*

$$P_{0,N} = \frac{2^k \sum_{i=0}^{N-2} C_{2^{n-k}-1}^{i} + C_{2^{n-k}-1}^{N-1}}{\sum_{i=0}^{N-1} C_{2^{n-k}-1}^{i} \frac{2^n - i}{2^{n-k}-i}}.$$

Для класса 1-ВЫП верна аналогичная теорема.

Теорема 2.5 *Пусть* $f \in C$*, где* C *- это один из классов, СЛО, СЛП, МАФ или БИН. Тогда при любой фиксации переменных полученная функция* $g \in C$*.*

Теорема 2.6 *Пусть про функцию* f *известно, что* $f \notin C$*, где* C *- это один из классов, СЛО, СЛП, МАФ или БИН. Пусть* g *получена из* f *фиксацией переменных* $(x_1, \ldots, x_k) = (\sigma_1, \ldots, \sigma_k)$*. Тогда верно следующее:*

- *Если среди всевозможных наборов* α,β,γ*, на которых для функции* f *нарушается условие принадлежности классу Шефера* C*:*

  СЛО: $\forall \alpha, \beta \in \{0,1\}^n : \overline{f}(\alpha \wedge \beta) f(\alpha) f(\beta) = 0;$
  СЛП: $\forall \alpha, \beta \in \{0,1\}^n : \overline{f}(\alpha \vee \beta) f(\alpha) f(\beta) = 0;$
  МАФ: $\forall \alpha, \beta, \gamma \in \{0,1\}^n : \overline{f}(\alpha \oplus \beta \oplus \gamma) f(\alpha) f(\beta) f(\gamma) = 0;$
  БИН: $\forall \alpha, \beta, \gamma \in \{0,1\}^n : \overline{f}(\alpha\beta \oplus \beta\gamma \oplus \alpha\gamma) f(\alpha) f(\beta) f(\gamma) = 0;$

  есть такие наборы α',β',γ'*, что*

$$\begin{cases} \alpha'_1 = \beta'_1 = \gamma'_1 = \sigma_1; \\ \ldots \\ \alpha'_k = \beta'_k = \gamma'_k = \sigma_k; \end{cases}$$

  то $g \notin C$*.*

- *В противном случае* $g \in C$*.*

В заключение приводится алгоритм, который по функции, не принадлежащей классу Шефера, и по наборам значений переменных, где нарушаются условия принадлежности этому классу, позволяет найти переменные, которые необходимо зафиксировать, чтобы перевести функцию в класс Шефера, и фиксируемый набор. При этом количество фиксируемых переменных минимально.

Теорема 2.10 *Пусть функция f задана таблицей истинности, l - длина входа алгоритма. Тогда алгоритм заканчивает работу менее чем за $l^2 + l\log_2^2(l)$ шагов.*

В **Главе 3** приводятся три алгоритма решения задачи о выполнимости, основанные на сведений функций к классам Шефера (БИН, СЛО или СЛП, МАФ), и алгоритм решения задачи о выполнимости, основанный на методе «разделяй и властвуй». Задача о выполнимости рассматривается в следующих модификациях:

1. Все функции заданы таблицами истинности или КНФ. Для данного варианта задания функций рассматриваются два случая:
   (a) Все функции зависят не более, чем от трех переменных. В этом случае задача решается приближением к классу БИН.
   (b) Нет ограничений на число переменных. В этом случае задача будет решается приближением к классу СЛО или СЛП (выбор класса осуществляется в ходе работы алгоритма).
2. Все функции заданы в форме полиномов Жегалкина. Тогда задача решается приближением к классу МАФ.

Первые три алгоритма имеют схожую структуру. Для исходной F-формулы рассматриваются следующие множества элементов, входящих в F-формулу:

- для БИН: D - множество дизъюнкций, зависящих от 3 переменных;
- для СЛО/СЛП: D - множество дизъюнкции, где число переменных без отрицаний/с отрицаниями больше 1;
- для МАФ: P - множество нелинейных полиномов и Q - множество нелинейных мономов с учетом кратности.

Будем говорить, что множество переменных M *покрывает* множество D (Q), если фиксация переменных из M приводит соответствующие элементы к виду, который требуется классом Шефера (для БИН - не более 2 переменных в дизъюнктах, для СЛО/СЛП - не более одного литерала с без отрицания/с отрицанием, для МАФ - линейность). Алгоритмы основаны на поиске наименьшего по мощности множества S переменных, покрывающего все элементы F-формулы. Общий порядок действий алгоритмов следующий:

1. Для БИН и СЛО/СЛП: Упрощение путем удаления единичных дизъюнктов и чистых литералов.

2. По КНФ функции F', полученной в результате упрощения F, строится множество D (P и Q).

3. Для СЛО/СЛП вычисляется число переменных в дизъюнктах, где нарушается условие для соответствующего класса. Далее приближаем формулу к классу, которому соответствует меньшее количество переменных.

4. Определяется множество M переменных, покрывающих дизъюнкты/мономы, которые не соответствуют требованиям класса Шефера.

5. Множество M, фиксация переменных из которого позволяет перевести D (P) в класс Шефера, не обязательно является наименьшим по мощности. По этому множеству строится минимальное множество S.

6. S разбивается на непересекающиеся по дизъюнкциям/полиномам подмножества S_i.

7. В соответствии с разбиением множества S на S_i множество D (P) оказывается разбито на D^i (P^i), такие что каждое D^i (P^i) зависит от своего набора переменных, которые не встречаются в других множествах разбиения. Далее проверка выполнимости формулы осуществляется независимо для каждого такого подмножества D^i (P^i). Для каждого S_i осуществляется перебор значений переменных, входящих в S_i.

8. При фиксированных значениях переменных из S_i решается полиномиальная подзадача об F-выполнимости для соответствующего класса Шефера.

9. Если для какого-то S_i была установлена невыполнимость, то искомая формула невыполнима. Если же для каждого S_i соответствующие формулы выполнимы, то искомая формула выполнима.

Сложность алгоритма решения задачи об F-выполнимости булевых формул приближением к классам Шефера не превосходит $\sum_{i=1}^{k} 2^{|S_i|} poly(|F|)$, где $|F|$ - длина F-формулы.

Однако приведенные алгоритмы по сути являются решением задачи о выполнимости для F-формулы. Они позволяют искать решение задачи для F-выполнимости, но относительно исходной длины входных данных для задачи об F-выполнимости они могут иметь большую сложность, чем относительно длины F-формулы. В связи с этим далее в главе приводится модификация данных алгоритмов, которая ориентирована на работу с исходной постановкой задачи об F-выполнимости. Данная модификация не всегда обеспечит более быстрое решение задачи об F-выполнимости, однако в случае, когда длина входа задачи об F-выполнимости существенно меньше длины F-формулы, она позволит решать задачу эффективнее. Например, если множество $F = \{F(x, y, z)\}$ включает одну функцию, зависящую от трех переменных и не принадлежащую классам Шефера, запись которой состоит из m дизъюнкций, при этом каждая из переменных входит в запись одинаковое количество раз. F-формула имеет вид $F(x_1, x_2, x_3)F(x_4, x_1, x_5)\ldots F(x_1, x_{p-1}, x_p)$ - в каждое из t вхождений функции F входит переменная x_1, которая находится на первом или втором месте, остальные переменные различны для всех вхождений F. Тогда общая сложность исходного алгоритма приближения к классу БИН не превосходит $poly(mt)$. При этом, в частности, при каждом фиксированном значении x_1 метод резолюций потребует $O(m^3t^3)$ операций. Тогда как для модифицированного алгоритма сложность можно оценить как $poly(t) + poly(m) + t \cdot poly(m)$. При этом метод резолюций при каждом фиксированном x_1 потребует $O(m^3t)$ операций, что меньше, чем без модификации.

Далее в главе приведено описание алгоритма приближения к классу БИН с использованием метода «разделяй и властвуй». В основе алгоритма лежит поиск множества переменных F-формулы, после фиксации которых формула окажется разбита на непересекающиеся подмножества дизъюнкций, после чего задача решается рекурсивно для каждого из получившихся непересекающихся подмножеств. Для поиска подмножества переменных для фиксации используется модифицированный алгоритм

Штор-Вагнера[22] нахождения глобального минимального разреза в графе (для этого в ходе работы алгоритма F-формуле сопоставляется неориентированный граф). Для модифицированного таким образом алгоритма приближения к классу БИН верны следующие утверждения:

Утверждение 3.6 *Пусть $T(БИН)$ - сложность решения задачи об F-выполнимости приближением к классу БИН, $T(DC)$ - сложность решения той же задачи приближением к классу БИН с использованием метода «разделяй и властвуй». Тогда $T(DC) \leq T(БИН) + poly(|F|)$, где $|F|$ - длина F-формулы.*

Следствие 3.4 *В случае если для всех $i = 1..k$ $|S_i| \leq \log_2(poly(|x|))$ сложность алгоритма будет полиномиальной величиной относительно длины F-формулы.*

Утверждение 3.7 *В лучшем случае на соответствующем шаге рекурсии сложность работы алгоритма не превышает $2^{\frac{S_i+3}{2}} poly(|F|)$, где $|F|$ - длина F-формулы.*

В **Главе 4** рассматриваются результаты практического применения алгоритмов, а также приводится описание криптографической системы с открытым ключом, которая может быть построена на базе задачи об F-выполнимости.

Практические результаты работы алгоритмов проверялись на случайно генерируемых наборах функций, не содержащих единичных дизъюнкций и чистых литералов, то есть рассматривались только случаи, для которых только лишь упрощение F-формулы стандартными методами не приводило к ответу, и для нахождения решения использовались непосредственно соответствующие алгоритмы приближения к классам Шефера. Из полученных статистических данных о работе программ видно, что несмотря на то, что в общем случае алгоритмы приближения к классам Шефера имеют экспоненциальную сложность, степень экспоненты в оценке сложности алгоритма $(\sum_{i=1}^{k} 2^{|S_i|} poly(|F|))$ растет медленнее, чем общее число переменных (соответствующее сложности перебора), что делает алгоритмы эффективными. Так, для решения задачи приближением

[22]Stoer M., Wagner F. A Simple Min-Cut Algorithm // Journal of the ACM, Vol. 44, No. 4. – 1997, P. 585-591

к классу БИН для 100 переменных при ограничении на число функции в F-формуле $s = 10$ и число дизъюнкций для записи каждой функции $k_{max} = 5$, максимальное время работы составило 273 секунды. Кроме того, приведено сравнение результатов использования алгоритма приближения к классу БИН без использования метода «разделяй и властвуй» и с его использованием, которое показывают, что использование метода «разделяй и властвуй» позволяет добиться намного более высокой скорости работы.

Далее в главе рассматривается асимметричная криптосистема с открытым ключом, основанная на алгоритме приближения к классу БИН, для которой можно было бы изучить вопрос использованися в случае распространения квантовых методов криптоанализа. Криптосистема функционирует следующим образом. Основным параметром криптографической системы с открытым ключом на основе задачи об F-выполнимости служит количество различных переменных, задействованных в F-формуле (n). Для формирования ключевой пары выбирается n булевых функций $F_1, \ldots, F_n$, удовлетворяющих условиям критерия Хаффмана, для которых задача о выполнимости решается приближением к классу БИН за полиномиальное время. Далее функции записываются в форме полиномов Жегалкина и осуществляется замена переменных в соответствии с матрицей $P = (A|b)$ (A - невырожденная $n \times n$-матрица) размера $n \times (n+1)$, которая представляет собой закрытый ключ. Функции $F_1, \ldots, F_n$ также преобразовываются с использованием закрытого ключа, так что на выходе имеем функции $h_1, \ldots, h_n$, зависящие от n^2 переменных, которые и служат открытым ключом. Для шифрования данных отправитель подставляет биты сообщения в функции открытого ключа, при этом стойкость системы базируется на сложности нахождения всех имеющихся выполняющих наборов для задачи выполнимости, в то время как получатель сообщения, обладая закрытым ключом, имеет возможность перейти к формулировке задачи, которая решается за полиномиальное время и имеет единственный выполняющий набор (соответствующий исходному тексту).

В **Заключении** отражены общие выводы из проделанной работы.

Автор выражает благодарность своему научному руководителю кандидату физико-математических наук, ведущему научному сотруднику Валентину Александровичу Носову за постановку задач и постоянное внимание к работе. Также благодарю коллектив кафедры Математической теории интеллектуальных систем за внимание к работе и ценные замечания.

СПИСОК ОСНОВНЫХ РАБОТ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

1. Поцелуевская Е.А. Полиномиальные случаи решения задачи об F-выполнимости булевых формул // Интеллектуальные системы. – 2008. – Т. 12. – Вып. 1-4. – С. 351-362.

2. Поцелуевская Е.А. Криптосистема с открытым ключом на основе задачи об F-выполнимости булевых формул // Фундаментальная и прикладная математика. – 2009. Т. 15. – Вып. 5. – С. 199-208. Перевод: Potseluevskaya E. Public-key cryptographic system based on generalized satisfiability problem // Journal of Mathematical Sciences – 2011. – Vol. 172. – No. 5 –P. 751-758, – DOI: 10.1007/s10958-011-0217-x.

3. Поцелуевская Е.А. Алгоритмы решения задачи об F-выполнимости приближением к классам Шефера // Интеллектуальные системы. – 2010. Т. 14. – Вып. 1-4. – С. 471-490.

4. Поцелуевская Е.А. О некоторых свойствах классов Шефера // Интеллектуальные системы. – 2011. – Т. 15. – Вып. 1-4. – С. 265-280.

5. Поцелуевская Е.А. Приближение булевых функций к классам Шефера // Фундаментальная и прикладная математика. – 2010. – Т. 16. – Вып. 7. – С. 197-204.