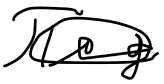
Федеральное государственное бюджетное учреждение науки
Математический институт им. В. А. Стеклова
Российской академии наук

На правах рукописи
УДК 510.5



Подольский Владимир Владимирович

Вопросы теории сложности вычислений в алгебраических и логических структурах

01.01.06 – математическая логика,
алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

Москва — 2021

Работа выполнена в отделе математической логики Федерального государственного бюджетного учреждения науки Математический институт им. В.А. Стеклова Российской академии наук.

Официальные оппоненты:

Аблаев Фарид Мансурович — доктор физико-математических наук, профессор, заведующий кафедрой теоретической кибернетики Института вычислительной математики и информационных технологий ФГАОУ ВО «Казанский (Приволжский) федеральный университет» (специальность 01.01.09);

Волков Михаил Владимирович — доктор физико-математических наук, главный научный сотрудник, заведующий кафедрой алгебры и дискретной математики ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина» (специальность 01.01.06);

Гирш Эдуард Алексеевич — доктор физико-математических наук, профессор РАН, ведущий научный сотрудник лаборатория математической логики ФГБУН Санкт-Петербургское отделение Математического института им. В.А. Стеклова РАН (специальность 01.01.06).

Ведущая организация:

Федеральное государственное образовательное учреждение высшего профессионального образования «Московский государственный университет имени М.В. Ломоносова».

Защита диссертации состоится 17 июня 2021 г. в 14 часов 00 минут на заседании диссертационного совета Д 002.022.03 при Федеральном государственном бюджетном учреждением науки Математический институт им. В.А. Стеклова Российской академии наук по адресу: 119991, г. Москва, ул. Губкина, д. 8, 9-й этаж, конференц-зал.

С диссертацией можно ознакомиться в библиотеке Математического института им. В. А. Стеклова РАН и на сайте
`http://mi-ras.ru/dis/ref21/podolskii/dis.pdf`

Автореферат разослан «____» марта 2021 г.

Ученый секретарь диссертационного совета
Д 002.022.03 при МИАН,
д. ф.-м. н. М. А. Королев

Актуальность темы

Работа посвящена исследованию вопросов сложности вычислений в алгебраических и логических структурах.

Вопросы сложности вычислений начали исследоваться с 1940-х годов, в первую очередь, в связи с задачами, происходящими из электротехники. Одной из основополагающих работ в этой области является работа К. Шеннона[1]. В связи с мотивацией этих исследований актуальными моделями вычислений в работах того времени были булевы схемы и ветвящиеся программы. В частности, в той же работе К. Шеннона были доказаны сильные неконструктивные нижние оценки на сложность булевых функций в этих моделях (с использованием мощностного метода). Подробнее о результатах того времени можно прочитать в обзоре А.Д. Коршунова[2].

Следующий важный этап развития теории сложности вычислений был связан с уже другой моделью — машинами Тьюринга. Около 1960-х годов в связи с распространением компьютеров все большую важность стала приобретать эффективность вычислений. Первые сложностные классы начали изучаться примерно в это время. Бурное развитие эта область получила в 1970-х годах, когда была разработана теория NP-полноты[3,4]. К этому времени относится формулировка текущего главного вопроса теории сложности вычислений — проблемы о сложностных классах P и NP.

В связи с формулировкой этой проблемы получила новый виток развития и теория сложности булевых схем. Оказалось, что между вычислениями на машинах Тьюринга и вычислениями с помощью булевых схем есть важные связи[5]. В частности, доказательство сильных нижних оценок на сложность вычисления явно заданных функций булевыми схемами позволило бы показать, что $\mathsf{P} \neq \mathsf{NP}$. Но оказалось, что доказательство таких нижних оценок — задача совсем не простая, и сильные нижние оценки в модели булевых схем общего вида по-прежнему остаются недостижимыми для современных мето-

[1] Shannon C. E. The synthesis of two-terminal switching circuits // Bell Syst. Tech. J. 1949. Vol. 28, N. 1. P. 59–98.

[2] Коршунов, А. Д. Сложность вычислений булевых функций // Успехи математических наук. 2012. Vol. 67, N. 1. P. 97–168.

[3] Cook S. A. The Complexity of Theorem-Proving Procedures // Proceedings of the 3rd Annual ACM Symposium on Theory of Computing, May 3-5, 1971, Shaker Heights, Ohio, USA / Ed. by M. A. Harrison, R. B. Banerji, J. D. Ullman. ACM, 1971. P. 151–158.

[4] Левин, Л. А. Универсальные задачи перебора // Проблемы передачи информации. 1973. Vol. 9, N. 3. P. 115–116.

[5] Savage J. E. Computational Work and Time on Finite Machines // J. ACM. 1972. Vol. 19, N. 4. P. 660–674.

дов. Тем не менее, были получены существенные продвижения для случая схем с дополнительными ограничениями.

Важным случаем здесь являются монотонные схемы, то есть схемы, в которых не используются отрицания. Прорывной результат был получен в работе А.А. Разборова[6], где была доказана сверхполиномиальная оценка сложности функции из NP в модели монотонных булевых схем. В последствии эта оценка была усилена и распространена на другие функции во ряде других работ[7,8] (см. также обзор А.Д. Коршунова[9]).

Еще одним важным видом ограничений, накладываемых на булевы схемы, являются ограничения на глубину схем. Самым слабым естественным, и при этом нетривиальным, классом с такими ограничениями является класс AC^0 булевых схем постоянной глубины, состоящих из конъюнкций и дизъюнкций неограниченной входной степени, а также отрицаний. Получение нижних оценок для таких схем уже оказалось крайне нетривальным. Первые результаты в этом направлении были получены в работах М. Айтаи[10] и М.Л. Ферста и др.[11], где было доказано, что схема из AC^0, вычисляющая функцию PARITY (эта функция равна единице, если во входном наборе нечетное число единиц), должна иметь сверхполиномиальный размер. Эта оценка позже была доведена до экспоненциальной[12]. Из этого результата вытекает также экспоненциальная нижняя оценка сложности функции голосования MAJ (эта функция равна единице, если во входном наборе не меньше половины единиц) в классе схем AC^0.

За этими результатами последовал ряд других продвижений в направлении исследования булевых схем ограниченной глубины. Так, естественной идеей усиления результата было бы расширить класс AC^0, разрешив в схемах в качестве элементов использовать функции, которые трудны для

[6]Разборов, А. А. Нижние оценки монотонной сложности некоторых булевых функций // Доклады Академии наук. 1985. Vol. 281, N. 4. P. 798–801.

[7]Андреев, А. Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций // Доклады Академии наук. 1985. Vol. 282, N. 5. P. 1033–1037.

[8]Alon N., Boppana R. The monotone circuit complexity of Boolean functions // Combinatorica. 1987. Vol. 7, N. 1. P. 1–22.

[9]Коршунов, А. Д. Монотонные булевы функции // Успехи математических наук. 2003. Vol. 58, N. 5. P. 89–162.

[10]Ajtai M. Σ^1_1-Formulae on finite structures // Annals of Pure and Applied Logic. 1983. Vol. 24, N. 1. P. 1 – 48.

[11]Furst M. L., Saxe J. B., Sipser M. Parity, Circuits, and the Polynomial-Time Hierarchy // Math. Syst. Theory. 1984. Vol. 17, N. 1. P. 13–27.

[12]Håstad J. Almost Optimal Lower Bounds for Small Depth Circuits // Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA / Ed. by J. Hartmanis. ACM, 1986. P. 6–20.

класса AC^0. Например, в качестве таких функций можно добавить функции PARITY и MAJ. Тогда для получившегося класса схем добавленные функции уже являются простыми. Соответственно, класс становится сильнее по сравнению с AC^0, и для него нижние оценки нужно доказывать отдельно. Для случая добавления функции PARITY были получены сверхполиномиальные нижние оценки[13,14]. Более того, были получены результаты для следующего более общего семейства классов. Через $\mathsf{ACC}^0[m]$ обозначим класс булевых схем постоянной глубины, состоящий из отрицаний, конъюнкций и дизъюнкций, а также из элементов MOD_m проверяющих, делится ли сумма входных битов элемента на m. Все элементы (кроме, естественно, отрицаний) здесь имеют неограниченную входную степень. В частности, для $m = 2$ функция MOD_2 есть в точности PARITY. Было доказано, что для случая, когда m является степенью простого числа p, некоторые явно заданные функции требуют схем экспоненциального размера в классе $\mathsf{ACC}^0[m]$. В качестве примеров трудных функций можно взять функции MOD_k, где k имеет простые множители, отличные от p, и все ту же функцию голосования MAJ. Вопрос о нахождении функции из класса NP, трудной для классов $\mathsf{ACC}^0[m]$ для произвольных m, остается открытым, хотя недавно были получены серьезные продвижения в этом направлении. Так, было доказано, что такие функции есть в квазиполиномиальном аналоге класса NP[15].

В случае же, если мы в качестве элементов в схемы из AC^0 добавляем функцию MAJ, ситуация оказывается более сложной. Этот класс принято обозначать через TC^0. Известно, что функция PARITY, как и все функции MOD_m, оказывается простой и вычисляется схемами постоянной глубины и полиномиального размера в этом классе. Так что этот класс оказывается не менее сильным, чем классы $\mathsf{ACC}^0[m]$. Также в этом классе эффективно решаются многие естественные задачи, такие как, например, арифметические операции с числами в двоичной записи[16]. Из верхних оценок вычислительных способностей этого класса известно, что всякая функция, вычислимая такой схемой полиномиального размера, вычислима также схемой логариф-

[13]Разборов, А. А. Нижние оценки размера схем ограниченной глубины в полном базисе, содержащем функцию логического сложения // Математические Заметки. 1987. Vol. 41, N. 4. P. 598–607.

[14]Smolensky R. Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity // Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA / Ed. by A. V. Aho. ACM, 1987. P. 77–82.

[15]Murray C. D., Williams R. R. Circuit Lower Bounds for Nondeterministic Quasi-polytime from a New Easy Witness Lemma // SIAM J. Comput. 2020. Vol. 49, N. 5.

[16]Vollmer H. Introduction to Circuit Complexity - A Uniform Approach. Texts in Theoretical Computer Science. An EATCS Series. Springer, 1999.

мической глубины полиномиального размера, состоящей из конъюнкций и дизъюнкций входной степени 2, а также отрицаний. Класс таких схем обозначается через NC^1. Это достаточно сильный класс, имеющий и другие естественные описания. В частности, в нем вычислимы в точности те же функции, которые вычислимы булевыми формулами полиномиального размера (выражениями, состоящими из булевых переменных, стандартных булевых связок и скобок).

На настоящий момент неизвестно сверхполиномиальных нижних оценок для класса TC^0. Более того, исходя из некоторых результатов, есть основания полагать, что получение таких нижних оценок является трудной задачей и требует разработки новых методов[17]. Вопрос о доказательстве нижних оценок для класса TC^0 является одним из центральных для современной теории сложности булевых схем.

Поскольку вопрос о нижних оценках для класса TC^0 остается открытым уже долгое время, естественно рассматривать подклассы этого класса и пытаться доказывать нижние оценки для них. Естественным ограничением была бы фиксация глубины конкретной константой. Но для этого сначала удобно несколько обобщить определение класса и сделать его более однородным.

Введем определение (линейной) пороговой функции. Булева функция $f\colon \{0,1\}^n \to \{0,1\}$ называется *пороговой*, если существуют целые числа $t, w_1, \ldots, w_n$, такие что

$$f(x) = 1 \Leftrightarrow \sum_{i=1}^{n} w_i x_i - t \geqslant 0. \tag{1}$$

Линейная форма в правой части (1) называется *(линейным) пороговым элементом*, число t называется *порогом*, а w_i — *весами*. Легко видеть, что функции $\mathrm{AND}, \mathrm{OR}, \mathrm{NOT}, \mathrm{MAJ}$ являются пороговыми функциями. Класс всех пороговых функцией будем обозначать через THR. Класс всех функций голосования будем обозначать через MAJ.

Для классов булевых функций и отдельных функций мы будем добавлять нижний индекс к этим множествам, чтобы указывать верхнюю границу на число переменных в функциях. Для данных классов схем $\mathcal{C}$ и $\mathcal{D}$ обозначим через $\mathcal{C} \circ \mathcal{D}$ класс схем, состоящих из схем из класса $\mathcal{C}$, в которые подставлены выходы схем из класса $\mathcal{D}$. Обозначим через ANY класс всех булевых функций. Этот класс мы будем использовать только с нижним индексом. Также отметим, что размер схем бывает полезно измерять как числом элементов схемы, так и числом ребер. В большинстве случаев эти меры эквивалентны

[17] Razborov A. A., Rudich S. Natural Proofs // J. Comput. Syst. Sci. 1997. Vol. 55, N. 1. P. 24–35.

с точностью до полинома. Мы будем указывать, в чем измеряется размер, всюду, где это существенно.

Для произвольного $d \geqslant 1$ обозначим через LT_d класс булевых схем глубины d, состоящих из пороговых функций в качестве элементов схемы. Будем называть схемы такого вида *пороговыми схемами*. Через $\widehat{\mathsf{LT}}_d$ обозначим класс схем глубины d, состоящих из таких пороговых функций, что для всех них есть такие представления (1), что все коэффициенты w_i ограничены по абсолютному значению полиномом от числа переменных.

Нетрудно видеть, что $\cup_{d\geqslant 1}\widehat{\mathsf{LT}}_d = \mathsf{TC}^0$. Соотношение с классами LT_d не очевидно, однако в результате серии работ[18,19,20,21] было показано, что $\cup_{d\geqslant 1}\mathsf{LT}_d = \mathsf{TC}^0$, и более точно, для всякого $d \geqslant 1$ выполняется $\mathsf{LT}_d \subseteq \widehat{\mathsf{LT}}_{d+1}$[21]. Таким образом, классы $\widehat{\mathsf{LT}}_d$ и LT_d образуют вложенную систему классов:

$$\widehat{\mathsf{LT}}_1 \subseteq \mathsf{LT}_1 \subseteq \widehat{\mathsf{LT}}_2 \subseteq \mathsf{LT}_2 \subseteq \ldots \subseteq \widehat{\mathsf{LT}}_d \subseteq \mathsf{LT}_d \subseteq \ldots \subseteq \mathsf{TC}^0.$$

Первые классы в этой цепочке $\widehat{\mathsf{LT}}_1$ и LT_1 слабые и могут вычислить только пороговые функции. Класс $\widehat{\mathsf{LT}}_2$, однако, уже весьма содержательный, в нем (в случае отсутствия ограничения на размер схемы) можно вычислить уже всякую булеву функцию. Вопрос о предъявлении явной функции, трудной для этого класса схем, является крайне нетривиальным, ответ на него был получен в работе А. Хайнала и др.[22] Вопрос о сверхполиномиальных нижних оценках для класса LT_2 по-прежнему открыт. В терминах композиции схем мы можем написать $\widehat{\mathsf{LT}}_2 = \mathsf{MAJ} \circ \mathsf{MAJ}$ и $\mathsf{LT}_2 = \mathsf{THR} \circ \mathsf{THR}$. Естественно рассмотреть два промежуточных подкласса $\mathsf{MAJ} \circ \mathsf{THR}$ и $\mathsf{THR} \circ \mathsf{MAJ}$. Про первый из них известно, что $\mathsf{MAJ} \circ \mathsf{THR} = \mathsf{MAJ} \circ \mathsf{MAJ}$[21]. Для второго также известны сильные нижние оценки[23,24] и известны отделения от классов

[18]Chandra A. K., Stockmeyer L., Vishkin U. Constant depth reducibility // SIAM Journal on Computing. 1984. Vol. 13, N. 2. P. 423–439.

[19]Pippenger N. The Complexity of Computations by Networks // IBM Journal of Research and Development. 1987. Vol. 31, N. 2. P. 235–243.

[20]Siu K., Bruck J. On the Power of Threshold Circuits with Small Weights // SIAM J. Discrete Math. 1991. Vol. 4, N. 3. P. 423–435.

[21]Goldmann M., Håstad J., Razborov A. A. Majority Gates VS. General Weighted Threshold Gates // Computational Complexity. 1992. Vol. 2. P. 277–300.

[22]Hajnal A., Maass W., Pudlák P., Szegedy M., Turán G. Threshold Circuits of Bounded Depth // Journal of Computer and System Sciences. 1993. Vol. 46, N. 2. P. 129–154.

[23]Forster J. A linear lower bound on the unbounded error probabilistic communication complexity // Journal of Computer and System Sciences. 2002. Vol. 65, N. 4. P. 612–625.

[24]Razborov A. A., Sherstov A. A. The Sign-Rank of AC^0 // SIAM Journal on Computing. 2010. Vol. 39, N. 5. P. 1833–1855.

$\mathsf{MAJ} \circ \mathsf{MAJ}$[25] и $\mathsf{THR} \circ \mathsf{THR}$[26]. Лучшие известные для LT_2 оценки составляют $\Omega(n^{3/2}/\log^3 n)$ для числа элементов и $\Omega(n^{5/2}/\log^{7/2} n)$ для числа ребер[27].

Другим направлением исследований, связанных с пороговыми элементами, является их обобщение до полиномиальных пороговых элементов. Полиномиальным пороговым элементом для функции $f\colon \{0,1\}^n \to \{0,1\}$ называется целочисленный многочлен $p(x)$ от n переменных, такой что для всех $x \in \{0,1\}^n$ верно, что $f(x) = 1$ тогда и только тогда, когда $p(x) \geqslant 0$.

Таким образом, полиномиальные пороговые элементы — это просто многочлены, представляющие булевы функции своим знаком. Их формальное изучение началось еще в 1968 году с классической книги М.Л. Минского и С.А. Паперта[28]. С тех пор полиномиальные пороговые элементы нашли массу применений в сложности булевых схем, структурной теории сложности, теории обучения и коммуникационной сложности[29,30,31,32].

Двумя ключевыми мерами сложности полиномиальных пороговых элементов являются их степень и вес. Степень — это просто степень $\deg(p)$ многочлена p. Весом $W(p)$ называется сумма абсолютных значений коэффициентов p. Соответствующими мерами сложности булевых функций являются пороговая степень $\deg_\pm f$, равная минимальной степени порогового элемента для f, и минимальный вес порогового элемента для f. Оба эти параметра играют ключевую роль в приложениях этой модели вычислений. Интерес представляет также вопрос о связи этих мер сложности. Обозначим через $W(f,d)$ минимально возможный вес порогового элемента для функции f в случае, когда степень порогового элемента ограничена d. Первые оценки на

[25]Goldmann M., Håstad J., Razborov A. A. Majority Gates vs. General Weighted Threshold Gates // Computational Complexity. 1992. Vol. 2, N. 4. P. 277–300.

[26]Chattopadhyay A., Mande N. S. A Short List of Equalities Induces Large Sign Rank // 59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018 / Ed. by M. Thorup. IEEE Computer Society, 2018. P. 47–58.

[27]Kane D. M., Williams R. Super-linear gate and super-quadratic wire lower bounds for depth-two and depth-three threshold circuits // Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016 / Ed. by D. Wichs, Y. Mansour. ACM, 2016. P. 633–643.

[28]Minsky M. L., Papert S. A. Perceptrons: Expanded edition. Cambridge, Mass.: MIT Press, 1988.

[29]Razborov A. A. On Small Depth Threshold Circuits // Proceedings of the Third Scandinavian Workshop on Algorithm Theory. London, UK: Springer-Verlag, 1992. P. 42–52.

[30]Klivans A. R., Servedio R. A. Learning DNF in time $2^{\tilde{O}(n^{1/3})}$ // J. Comput. Syst. Sci. 2004. Vol. 68, N. 2. P. 303–318.

[31]Beigel R. Perceptrons, PP, and the Polynomial Hierarchy // Computational Complexity. 1994. Vol. 4. P. 339–349.

[32]Sherstov A. A. Communication Lower Bounds Using Dual Polynomials // Bulletin of the EATCS. 2008. Vol. 95. P. 59–93.

эту величину были доказаны для $d = 1$. Известно[33,34,35], что для всех f с $\deg_\pm f = 1$ выполняется $W(f,1) = n^{O(n)}$. Известно также[35], что эта оценка точна, то есть существует f с $\deg_\pm f = 1$, для которой $W(f,1) = n^{\Omega(n)}$.

Что касается большей степени d, верхняя оценка несложно выводится из случая $d = 1$. А именно, для всех f с $\deg_\pm f \leqslant d$ верно[36,37,38], что $W(f,d) = n^{O(dn^d)}$. Также известно[38], что эта оценка точна для постоянного d. То есть, для любого d существует функция f пороговой степени d, такая что $W(f,d) = n^{\Omega(n^d)}$ (константа в Ω зависит от d).

Таким образом, оказывается, что требуемый вес растет с ростом степени d. Естественный вопрос — насколько большим он может стать (заметим, что при $d = n$ вес снова становится маленьким: $W(f,n) = 2^{O(n)}$). Более конкретно, нас интересует величина

$$W = \max_d \max_{f:\ \deg_\pm(f) \leqslant d} W(f,d). \tag{2}$$

Лучшая ранее известная оценка[38] этой величины составляет $2^{\Omega(2^{n/8})}$.

Поскольку не удается доказать нижние оценки на размер схем постоянного размера с MAJ и THR элементами, естественно исследовать вопрос нижних оценок для схем постоянной глубины с небольшим количеством пороговых элементов (и с произвольным количеством конъюнкций, дизъюнкций и отрицаний). В работе Дж. Аспнеса и др.[39] была доказана экспоненциальная нижняя оценка для схем с одним элементом MAJ, вычисляющих PARITY. Позже этот результат был усилен, и была доказана[40,41] аналогичная оценка для схем с $n^{o(1)}$ элементами MAJ. Что касается схем с элементами THR, то экспоненциальная оценка для одного элемента THR по существу доказа-

[33]Muroga S., Toda I., Takasu S. Theory of majority decision elements // Journal of the Franklin Institute. 1961. Vol. 271, N. 5. P. 376 – 418.

[34]Muroga S. Threshold Logic and its Applications. John Wiley & Sons, Inc., 1971.

[35]Håstad J. On the Size of Weights for Threshold Gates // SIAM J. Discret. Math. 1994. Vol. 7, N. 3. P. 484–492.

[36]Saks M. E. Slicing the hypercube // Surveys in Combinatorics. 1993. P. 211–255.

[37]Buhrman H., Vereshchagin N. K., de Wolf R. On Computation and Communication with Small Bias // IEEE Conference on Computational Complexity. 2007. P. 24–32.

[38]Подольский, В. В. Перцептроны с большим весом // Проблемы передачи информации. 2009. Vol. 45. P. 51–59.

[39]Aspnes J., Beigel R., Furst M., Rudich S. The expressive power of voting polynomials // Combinatorica. 1994. Vol. 14. P. 135–148. 10.1007/BF01215346.

[40]Beigel R., Reingold N., Spielman D. A. PP Is Closed under Intersection // J. Comput. Syst. Sci. 1995. Vol. 50, N. 2. P. 191–202.

[41]Beigel R. When do extra majority gates help? Polylog (N) majority gates are equivalent to one // Computational Complexity. 1994. Vol. 4. P. 314–324. 10.1007/BF01263420.

на в той же работе Дж. Аспнеса и др.[42]: оценка в статье сформулирована для схем с элементом MAJ, но доказательство буквально переносится и на случай элемента THR. Результаты[43,44] для схем с $n^{o(1)}$ элементами MAJ, напротив, не переносятся с элементов MAJ на элементы THR. Что касается сверхполиномиальных оценок, то известна[45] оценка $n^{\Omega(\log n)}$ для схем с $O(\log^2 n)$ элементами THR. Эта оценка доказана для функции, более сложной, чем PARITY. Также известна[46] сверхполиномиальная оценка для схем с $O(\log n)$ пороговыми элементами, вычисляющими PARITY.

Вместе с изучением булевых схем, состоящих из функций голосования, интересно также исследование сложности самой функции голосования. Классическим результатом в этом направлении является доказательство того, что функцию MAJ_n можно вычислить монотонной схемой глубины $5.3 \log n$ (то есть, элементами схемы являются AND_2 и OR_2)[47]. Доказательство этого результата вероятностное, и известные детерминированные конструкции дают существенно худшее значение глубины[48]. Существует также версия[49] этой конструкции, в которой схема состоит из элементов MAJ_3.

Наряду с пороговыми функциями можно рассматривать точные пороговые функции. Булева функция $f\colon \{0,1\}^n \to \{0,1\}$ называется *точной поро-*

[42]Aspnes J., Beigel R., Furst M., Rudich S. The expressive power of voting polynomials // Combinatorica. 1994. Vol. 14. P. 135–148. 10.1007/BF01215346.

[43]Beigel R., Reingold N., Spielman D. A. PP Is Closed under Intersection // J. Comput. Syst. Sci. 1995. Vol. 50, N. 2. P. 191–202.

[44]Beigel R. When do extra majority gates help? Polylog (N) majority gates are equivalent to one // Computational Complexity. 1994. Vol. 4. P. 314–324. 10.1007/BF01263420.

[45]Chattopadhyay A., Hansen K. A. Lower Bounds for Circuits with Few Modular and Symmetric Gates // Automata, Languages and Programming / Ed. by L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, M. Yung. Springer Berlin / Heidelberg, 2005. Vol. 3580 of *Lecture Notes in Computer Science*. P. 994–1005. 10.1007/11523468_80.

[46]Gopalan P., Servedio R. A. Learning and lower bounds for AC0 with threshold gates // Proceedings of the 13th international conference on Approximation, and 14 the International conference on Randomization, and combinatorial optimization: algorithms and techniques. APPROX/RANDOM'10. Berlin, Heidelberg: Springer-Verlag, 2010. P. 588–601.

[47]Valiant L. G. Short Monotone Formulae for the Majority Function // J. Algorithms. 1984. Vol. 5, N. 3. P. 363–366.

[48]Ajtai M., Komlós J., Szemerédi E. An 0 (n log n) sorting network // Proceedings of the fifteenth annual ACM symposium on Theory of computing. 1983. P. 1–9.

[49]Cohen G., Damgård I. B., Ishai Y., Kölker J., Miltersen P. B., Raz R., Rothblum R. D. Efficient Multiparty Protocols via Log-Depth Threshold Formulae - (Extended Abstract) // Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II / Ed. by R. Canetti, J. A. Garay. Vol. 8043 of *Lecture Notes in Computer Science*. Springer, 2013. P. 185–202.

говой, если существуют целые числа $t, w_1, \ldots, w_n$, такие что

$$f(x) = 1 \Leftrightarrow \sum_{i=1}^{n} w_i x_i = t.$$

Можно рассматривать точные пороговые функции в качестве элементов схемы. Однако, результатов о таких схемах довольно мало и они разрозненны[50,51,52,53].

Дальнейшее исследование пороговых булевых схем является одним из направлений данной работы.

Другое направление связано с приложениями теории сложности булевых схем к математической логике, а именно, к исследованиям баз данных с онтологическим доступом. Базы данных с онтологическим доступом представляют собой подход к хранению и организации доступа к базам данных[54]. В этом подходе база данных снабжается логической теорией первого порядка, то есть данные рассматриваются как множество предикатов на элементах (объектах) базы данных, и теория содержит некоторые универсальные утверждения об этих предикатах.

Идея дополнения данных логической теорией рассматривается как минимум с 1970-х годов (например, язык программирования Пролог основан на подобных идеях[55]). Однако, этот подход вынужден постоянно преодолевать сложности с реализуемостью. Основная проблема состоит в том, что если теория, добавляемая к данным, слишком сильна, то даже самые стандартные алгоритмические задачи становятся неразрешимыми.

Нас будет интересовать как раз одна из таких базовых алгоритмических задач, а именно, задача поиска ответа на запрос. Цель запроса к базе данных — найти все элементы в базе, удовлетворяющие определенным условиям.

[50]Beigel R., Tarui J., Toda S. On Probabilistic ACC Circuits with an Exact-Threshold Output Gate // Proceedings of the Third International Symposium on Algorithms and Computation. Vol. 650 of *Lecture Notes in Computer Science*. Springer, 1992. P. 420–429.

[51]Green F. A complex-number Fourier technique for lower bounds on the Mod-m degree // Computational Complexity. 2000. Vol. 9, N. 1. P. 16–38.

[52]Hansen K. A. Computing Symmetric Boolean Functions by Circuits with Few Exact Threshold Gates // Proceedings of the 13th Annual International Conference on Computing and Combinatorics. Vol. 4598 of *Lecture Notes in Computer Science*. Springer, 2007. P. 448–458.

[53]Hansen K. A. Depth Reduction for Circuits with a Single Layer of Modular Counting Gates // Proceedings of the 4th International Computer Science Symposium in Russia. Vol. 5675 of *Lecture Notes in Computer Science*. Springer, 2009. P. 117–128.

[54]Неформально мы используем слова «база данных» в широком смысле, как структурированный набор данных. Формальном изложении в тексте диссертационной работы мы сопоставим базам данных некоторые логические теории первого порядка.

[55]Kowalski R. A. The Early Years of Logic Programming // Commun. ACM. 1988. Vol. 31, N. 1. P. 38–43.

В случае, когда данные снабжены логической теорией, задача поиска ответа на запрос не может быть решена обычными методами, пригодными для работы со стандартными базами данных, и требуются новые методы.

Так что, с одной стороны, мы хотели бы добавить к базе логическую теорию, чтобы помочь работать с базой, а с другой стороны, нам нужно избежать возникающих вычислительных проблем.

С 1970-х годов исследования в этой области пытались преодолеть эти сложности. Ранние продвижения в этом направлении описаны в книге Дж.Д. Ульмана[56]. В результате этих усилий возникли несколько направлений, каждое со своими специфическими целями. Среди недавних таких направлений можно выделить область интеграции данных[57] и область обмена данными[58,59].

Другим актуальным направлением является теория баз данных с онтологическим доступом, ее развитие началось примерно с 2005 года[60,61,62,63]. Основной целью этого направления является разработка подхода, помогающего поддерживать большие и распределенные базы данных, и делать работу с данными более доступной для пользователя. Логическая теория помогает в достижении этой цели, позволяя создавать удобный язык для запросов, прятать технические детали структуры данных, поддерживать запросы к распределенным и разнородным источникам данных. Еще одной важной особенностью является то, что данные в базе не обязаны быть полными.

[56]Ullman J. D. Principles of Database and Knowledge-base Systems, Vol. I. New York, NY, USA: Computer Science Press, Inc., 1988.

[57]Lenzerini M. Data Integration: A Theoretical Perspective // Proceedings of the Twenty-first ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems. PODS '02. New York, NY, USA: ACM, 2002. P. 233–246.

[58]Fagin R., Kolaitis P. G., Miller R. J., Popa L. Data exchange: semantics and query answering // Theoretical Computer Science. 2005. Vol. 336, N. 1. P. 89 – 124. Database Theory.

[59]Kolaitis P. G. Schema Mappings, Data Exchange, and Metadata Management // Proceedings of the Twenty-fourth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems. PODS '05. New York, NY, USA: ACM, 2005. P. 61–75.

[60]Calvanese D., De Giacomo G., Lembo D., Lenzerini M., Rosati R. *DL-Lite*: Tractable Description Logics for Ontologies // Proc. of the 20th Nat. Conf. on Artificial Intelligence (AAAI 2005). AAAI Press, 2005. P. 602–607.

[61]Dolby J., Fokoue A., Kalyanpur A., Ma L., Schonberg E., Srinivas K., Sun X. Scalable Grounded Conjunctive Query Evaluation over Large and Expressive Knowledge Bases // Proc. of the 7th Int. Semantic Web Conf. (ISWC 2008). Vol. 5318 of *Lecture Notes in Computer Science*. Springer, 2008. P. 403–418.

[62]Ontology Reasoning with Large Data Repositories / S. Heymans, L. Ma, D. Anicic, Z. Ma, N. Steinmetz, Y. Pan, J. Mei et al. // Ontology Management, Semantic Web, Semantic Web Services, and Business Applications. Springer, 2008. Vol. 7 of *Semantic Web and Beyond*. P. 89–128.

[63]Poggi A., Lembo D., Calvanese D., De Giacomo G., Lenzerini M., Rosati R. Linking Data to Ontologies // Journal on Data Semantics. 2008. Vol. X. P. 133–173.

Какая-то информация может отсутствовать в базе в явном виде, но тем не менее, логически выводиться из теории, сопутствующей базе данных.

Важной особенностью баз данных с онтологическим доступом является то, что для достижения перечисленных целей часто достаточно снабдить данные слабыми и простыми теориями. Это важно с точки зрения задачи поиска ответа на запрос: идея этого направления с алгоритмической точки зрения состоит в том, чтобы для использования подхода не требовалось разрабатывать новую алгоритмическую технику, а можно было вместо этого сводить задачу поиска ответа на запрос к аналогичной задаче для стандартных баз данных, а затем уже использовать существующие алгоритмические методы.

Самым стандартным подходом здесь является идея с переформулировкой данного запроса в таком виде, чтобы ответ на новый переформулированный запрос не требовал обращения к теории. Такую переформулировку мы будем называть *преобразованием* запроса. Преобразование запроса не должно зависеть от конкретных данных в базе и может зависеть только от самого запроса и от теории, сопровождающей базу. Как только преобразование построено, мы можем использовать стандартные методы теории баз данных для поиска ответа на него. Однако, возникает естественная проблема, что длина преобразования запроса может быть сильно больше длины самого запроса, что может сделать этот подход (по крайней мере, теоретически) неэффективным. Другими словами, преодолев трудности с алгоритмической разрешимостью, это направление естественным образом сталкивается с вопросами алгоритмической сложности.

Нас будет интересовать вопрос о длинах преобразований запросов для различных вариантов ограничений на запросы и теории. Оказывается, что в исследованиях по этому направлению помогают ранее известные результаты из теории сложности булевых схем.

Еще одно направление исследований данной работы посвящено вопросам сложности в мин-плюс алгебре, называемой также тропической алгеброй. *Мин-плюс* или *тропическим* полукольцом называется множество $\mathbb{K}$, которое может быть равно $\mathbb{R}$, $\mathbb{R}_\infty = \mathbb{R} \cup \{+\infty\}$, $\mathbb{Q}$, $\mathbb{Q}_\infty = \mathbb{Q} \cup \{+\infty\}$, $\mathbb{Z}$ или $\mathbb{Z}_\infty = \mathbb{Z} \cup \{+\infty\}$, снабженное двумя операциями, *мин-плюс сложением* $\oplus$ и *мин-плюс умножением* $\odot$, определенными следующим образом:

$$x \oplus y = \min\{x, y\}, \qquad x \odot y = x + y.$$

Отметим, что в силу симметрии совершенно аналогично можно рассматривать и макс-плюс полукольцо.

Мин-плюс многочлены являются естественным аналогом классических многочленов. В классических терминах мин-плюс многочлены являются выражениями вида $f(\vec{x}) = \min_i M_i(\vec{x})$, где каждое $M_i(\vec{x})$ является линейной формой (мин-плюс мономом) от переменных $\vec{x} = (x_1, \ldots, x_n)$, и все коэффициенты всех M_i — неотрицательные целые числа, кроме, возможно, свободных членов, которые могут быть произвольными элементами $\mathbb{K}$ (свободный коэффициент соответствует коэффициенту мин-плюс монома, а остальные коэффициенты — это степени переменных).

Степенью мин-плюс монома M называется сумма его коэффициентов (кроме свободного коэффициента), степень мин-плюс многочлена f, обозначаемая через $\deg(f)$, — это просто максимальная степень его мономов. Точка $\vec{a} \in \mathbb{K}^n$ называется корнем многочлена f, если максимум $\max_i\{M_i(\vec{a})\}$ достигается как минимум для двух различных мономов M_i.

Наряду с мин-плюс многочленами мы также рассматриваем мин-плюс уравнения. *Мин-плюс уравнением* называется пара мин-плюс многочленов

$$(f(\vec{x}), g(\vec{x}))\,.$$

Точка $\vec{a} \in \mathbb{K}^n$ является *решением* мин-плюс уравнения (f, g), если выполняется равенство $f(\vec{a}) = g(\vec{a})$.

Мин-плюс многочлены возникают в различных разделах математики и находят многочисленные приложения[64,65,66,67,68,69,70]. Важным достоинством мин-плюс алгебры является то, что она делает некоторые свойства классических объектов доступными для вычислений[64,65,66,71]: с одной стороны, мин-плюс аналоги классических объектов отражают некоторые свойства классических объектов, а с другой стороны, мин-плюс объекты имеют гораздо более

[64]Itenberg I., Mikhalkin G., Shustin E. Tropical Algebraic Geometry. Oberwolfach Seminars. Birkhäuser, 2009.

[65]Maclagan D., Sturmfels B. Introduction to Tropical Geometry. Graduate Studies in Mathematics. American Mathematical Society, 2015.

[66]Sturmfels B. Solving Systems of Polynomial Equations. American Mathematical Society, 2002. Vol. 97 of *CBMS Regional Conference in Math.*

[67]Mikhalkin G. Amoebas of Algebraic Varieties and Tropical Geometry // Different Faces of Geometry / edited byS. Donaldson, Y. Eliashberg, M. Gromov. Springer US, 2004. Vol. 3 of *International Mathematical Series*. P. 257–300.

[68]Richter-Gebert J., Sturmfels B., Theobald T. First steps in tropical geometry // Idempotent Mathematics and Mathematical Physics, Contemporary Mathematics. 2003. Vol. 377. P. 289–317.

[69]Huber B., Sturmfels B. A polyhedral method for solving sparse polynomial systems // Mathematics of Computation. 1995. Vol. 64. P. 1541–1555.

[70]Воробьев, Н. Н. Экстремальная алгебра положительных матриц // Elektronische Informationsverarbeitung und Kybernetik. 1967. Vol. 3, N. 1. P. 39–71.

[71]Theobald T. On the frontiers of polynomial computations in tropical geometry // J. Symb. Comput. 2006. Vol. 41, N. 12. P. 1360–1375.

простую и дискретную структуру и, как результат, становятся более доступными для алгоритмических подходов. Одна из основных целей мин-плюс алгебры состоит в построении теории мин-плюс многочленов, которая поможет работать с ними и потенциально приведет к продвижениям в смежных областях. При этом, с точки зрения вычислительных приложений, важными являются вопросы об алгоритмических задачах в возникающей теории.

В настоящий момент лучше всего изучены вопросы о мин-плюс линейных многочленах и системах, состоящих из них. Для них построен аналог значительной части классической теории линейных уравнений. Это включает исследования по мин-плюс аналогу ранга матриц и независимости векторов[72,73,74]. В классическом случае существует множество различных определений ранга, которые оказываются эквивалентными. В мин-плюс случае ситуация оказывается сложнее, и существует множество неэквивалентных определений ранга. Три самых распространенных понятия ранга в мин-плюс алгебре: *ранг Барвинока*, *ранг Капранова* и *тропический ранг* (определения и основные результаты можно найти в работе М. Девелина и др.[72]). Между этими рангами выполняется соотношение

$$tropical\ rank(A) \leqslant Kapranov\ rank(A) \leqslant Barvinok\ rank(A) \qquad (3)$$

для всякой матрицы A. Все неравенства в (3) могут быть строгими[72]. Также для мин-плюс линейных многочленов изучены аналог определителя матрицы и его свойств[72,74,75], аналог гауссовской верхне-треугольной формы[75]. Известно, что задача разрешимости мин-плюс систем линейных многочленов лежит в классе $\mathsf{NP} \cap \mathsf{coNP}$ и полиномиально сводится к известной задаче об определении победителя в циклических играх[76]. Для мин-плюс систем линейных неравенств известно, что задача о разрешимости полиномиально эквивалентна задаче об определении победителя в циклических играх[76].

Для мин-плюс многочленов произвольной степени известно намного меньше. Построено[77] явное описание радикала мин-плюс идеала. Была доказа-

[72]Develin M., Santos F., Sturmfels B. On the rank of a tropical matrix // Combinatorial and computational geometry. 2005. Vol. 52. P. 213–242.

[73]Izhakian Z., Rowen L. The Tropical Rank of a Tropical Matrix // Communications in Algebra. 2009. Vol. 37, N. 11. P. 3912–3927.

[74]Akian M., Gaubert S., Guterman A. Linear independence over tropical semirings and beyond // Contemporary Mathematics. 2009. Vol. 495. P. 1–33.

[75]Grigoriev D. Complexity of Solving Tropical Linear Systems // Computational Complexity. 2013. Vol. 22, N. 1. P. 71–88.

[76]Akian M., Gaubert S., Guterman A. Tropical polyhedra are equivalent to mean payoff games // International Journal of Algebra and Computation. 2012. Vol. 22, N. 1.

[77]Shustin E., Izhakian Z. A tropical Nullstellensatz // Proceedings of the American Mathematical Society. 2007. Vol. 135, N. 12. P. 3815–3821.

на[78,79] мин-плюс версия теоремы Безу для случая, когда число многочленов равно числу переменных. Позже[80] теорема Безу была распространена на системы многочленов произвольного размера. Также известна[81] оценка на число невырожденных корней системы разреженных мин-плюс многочленов. Было доказано[82], что задача разрешимости мин-плюс систем многочленов NP-полна. Была выдвинута[83] гипотеза о мин-плюс аналоге теоремы Гильберта о нулях в двойственной форме.

Цель работы

Получение сильных нижних оценок на веса полиномиальных пороговых элементов заданной степени, вычисляющих заданные булевы функции. Доказательство нижних оценок сложности вычисления функции четности схемами постоянной глубины, содержащими небольшое число пороговых элементов. Исследование схем, состоящих из точных пороговых функций, и их связи с пороговыми схемами. Исследование реализации булевых функций многочленами над переменными, принимающими значения $\{a, b\}$ для произвольной пары чисел a и b, установление связи этой модели с пороговыми схемами. Исследование монотонных булевых схем постоянной глубины d, состоящих из функций MAJ_k от k переменных и вычисляющих функцию MAJ_n от n переменных. Доказательство верхних и нижних оценок на минимальное значение k, для которого такие схемы глубины d существуют. Исследование выразительной способности новой модели вычислений, гиперграфовых программ, в связи с вопросами о размере преобразований запросов к базам данных с онтологическим доступом для различных вариантов ограничений на запросы и теории, дополняющие базы данных. Доказательство аналогов комбинаторной теоремы о нулях и леммы Шварца-Зиппеля для мин-плюс многочленов. Получение оценок на размер минимального тестового множества для мин-плюс многочленов с заданным ограничением на число мономов.

[78]Richter-Gebert J., Sturmfels B., Theobald T. First steps in tropical geometry // Idempotent Mathematics and Mathematical Physics, Contemporary Mathematics. 2003. Vol. 377. P. 289–317.

[79]Steffens R., Theobald T. Combinatorics and Genus of Tropical Intersections and Ehrhart Theory // SIAM Journal on Discrete Mathematics. 2010. Vol. 24, N. 1. P. 17–32.

[80]Davydow A., Grigoriev D. Bounds on the Number of Connected Components for Tropical Prevarieties // Discrete & Computational Geometry. 2017. Vol. 57, N. 2. P. 470–493.

[81]Bihan F. Irrational Mixed Decomposition and Sharp Fewnomial Bounds for Tropical Polynomial Systems // Discrete & Computational Geometry. 2016. Vol. 55, N. 4. P. 907–933.

[82]Theobald T. On the frontiers of polynomial computations in tropical geometry // J. Symb. Comput. 2006. Vol. 41, N. 12. P. 1360–1375.

[83]Grigoriev D. On a tropical dual Nullstellensatz // Advances in Applied Mathematics. 2012. Vol. 48, N. 2. P. 457 – 464.

Исследование алгоритмической сложности задачи разрешимости мин-плюс линейных систем многочленов. Доказательство аналогов теоремы Гильберта о нулях для мин-плюс многочленов и мин-плюс уравнений, в том числе эффективных версий этих теорем.

Научная новизна

Все результаты диссертации являются новыми. Основные из них состоят в следующем.

— Получены дважды экспоненциальные нижние оценки на веса полиномиальных пороговых элементов заданной степени, вычисляющих заданные булевы функции.

— Доказана экспоненциальная нижняя оценка сложности вычисления функции четности схемами постоянной глубины, содержащими логарифмическое число пороговых элементов.

— Построена иерархия точных пороговых схем и доказано, что она тесно переплетается с иерархией пороговых схем. Доказаны разделения некоторых классов в нижних уровнях этих иерархий.

— Исследованы вопросы реализации булевых функций многочленами над переменными, принимающими значения $\{a, b\}$ для произвольной пары чисел a и b. Установлены связи этой модели с пороговыми схемами.

— Исследованы монотонные булевы схемы постоянной глубины d, состоящие из функций MAJ_k и вычисляющие функцию MAJ_n. Доказаны верхние и нижние оценки на минимальное значение k, для которого такие схемы глубины d существуют.

— В связи с приложениями к исследованиям размера преобразований запросов к базам данных с онтологическим доступом исследована сложность булевых функций в модели гиперграфовых программ. Для различных классов таких программ установлена их выразительная способность в терминах известных сложностных классов.

— Получены аналоги комбинаторной теоремы о нулях и леммы Шварца-Зиппеля для мин-плюс многочленов.

— Доказаны оценки на размер минимального тестового множества для мин-плюс многочленов с заданным ограничением на число мономов.

— Доказано, что задача о разрешимости мин-плюс линейных систем многочленов полиномиально эквивалентна задаче об определении победителя в циклических играх.

— Доказан аналог теоремы Гильберта о нулях для мин-плюс многочленов. В том числе, доказана эффективная версия этой теоремы с близкими к точным оценками на степени возникающих в теореме многочленов.

Методы исследования

В работе используются методы теории сложности вычислений, комбинаторные и вероятностные методы, методы комбинаторной геометрии. Для получения результатов о преобразованиях запросов к базам данных с онтологическим доступом была исследована новая модель вычислений — гиперграфовые программы.

Теоретическая и практическая ценность

Работа носит теоретический характер. Результаты диссертации могут найти применение в теории сложности вычислений, мин-плюс алгебре и ее приложениях, в исследованиях баз данных с онтологическим доступом. Результаты о базах данных с онтологическим доступом могут иметь значение для прикладных задач работы с такими базами данных.

Апробация работы

Результаты диссертации докладывались автором на семинаре по алгоритмическим вопросам алгебры и логики (МГУ, МИАН), колмогоровском семинаре по сложности вычислений и сложности определений (МГУ), общеинститутском семинаре «Математика и ее приложения» (МИАН), коллоквиуме факультета компьютерных наук (НИУ ВШЭ), семинаре лаборатории теоретической информатики (НИУ ВШЭ), семинаре по сложности вычислений (ВЦ РАН, МИАН), семинаре по алгоритмам и теории сложности университета Орхуса, семинаре теоретической группы на факультете Computer Science университета Чикаго, семинаре факультета Computer Science университета UCLA, семинаре по комбинаторике и сложности университета UCLA, а также на следующих международных конференциях:

— международная конференция “Conference on Computational Complexity”, Кембридж, США, 09.06–11.06.2010;

— международная конференция “Turing Centenary Conference and 8th Conference on Computability in Europe”, Кембридж, Великобритания, 18.06–23.06.2012;

— международная конференция «Рождественские математические встречи победителей конкурса фонда Династия», Москва, Россия, 08.01–11.01.2013;

— международная конференция “International Symposium on Mathematical Foundations of Computer Science”, Клостернойбург, Австрия, 26.08–30.08.2013;

— международная конференция “Tropical aspects in Geometry and Topology”, Бонн, Германия, 02.09–06.09.2013;

— международная конференция “International Conference on Computability, Complexity and Randomness”, Москва, Россия, 23.09–27.09.2013;

— международная конференция “Symposium on Theoretical Aspects of Computer Science”, Мюнхен, Германия, 04.03–07.03.2015;

— международная конференция “Complexity of Symbolic and Numerical Problems”, Дагштуль, Германия, 07.06–12.06.2015;

— международная конференция “International Computer Science Symposium in Russia”, Листвянка, Россия, 13.07–17.07.2015;

— международная конференция “Workshop on Low-Depth Complexity”, Санкт-Петербург, Россия, 23.05–25.05.2016;

— международная конференция «Математическая логика, алгебра и вычислимость: двухдневная конференция, посвященная 85-летию С.И. Адяна», Москва, Россия, 18.07–19.07.2016;

— международная конференция “Algorithms and Effectivity in Tropical Mathematics and Beyond”, Дагштуль, Германия, 27.11–02.12.2016;

— международная конференция “Symposium on Theoretical Aspects of Computer Science”, Ганновер, Германия, 08.03–11.03.2017;

— международная конференция “International Symposium on Fundamentals of Computation Theory”, Бордо, Франция, 11.09–13.09.2017;

— международная конференция “Традиционная зимняя сессия МИАН–ПОМИ, посвященная теме «Математическая логика»”, Москва, Россия, 24.12–25.12.2018;

— международная конференция «Алгебра и математическая логика: теория и приложения», Казань, Россия, 24.06–28.06.2019.

Публикации

Основные результаты диссертации опубликованы в 11 работах автора, список которых приведен к конце автореферата. Все относящиеся к диссертации результаты в совместных работах принадлежат автору.

Структура диссертации

Диссертация состоит из введения, десяти глав, разбитых на разделы, и списка литературы.

Содержание работы

Во введении мы обосновываем актуальность темы исследования, кратко описываем историю задач и их современное состояние, формулируем основные результаты и описываем содержание работы.

В первой главе мы даем основные определения, связанные с булевыми функциями, булевыми схемами и мин-плюс алгеброй, а также приводим базовые свойства вводимых понятий.

Во второй главе мы приводим результаты о весах полиномиальных пороговых функций. В разделе 1 приводится конструкция функции, для которой в разделе 2 доказывается нижняя оценка $2^{\Omega(2^{n/4})}$ на величину $W = \max_d \max_{f\colon \deg_\pm(f)\leqslant d} W(f,d)$, характеризующую, насколько большими могут быть веса полиномиальных пороговых элементов для конкретной функции, при заданном ограничении на степень. В разделе 3 мы усиливаем эту оценку до $2^{\Omega(2^{2n/5})}$. Предварительное доказательство более слабой оценки приводится для того, чтобы показать основные идеи, стоящие за конструкцией, по возможности избегая технических осложнений.

В третьей главе мы доказываем экспоненциальную нижнюю оценку на размер схем постоянной глубины, содержащих логарифмическое число пороговых элементов, и вычисляющих функцию PARITY. В разделе 1 приводятся известные вспомогательные результаты, необходимые именно в этой главе. В разделе 2 мы доказываем результат этой главы: для всякого $\epsilon > 0$ всякая схема неограниченной входной степени, глубины h, вычисляющая PARITY, и, помимо элементов AND, OR и NOT содержащая не больше $t \leqslant \left(\frac{1}{4} - \epsilon\right)\log n$ пороговых элементов, имеет размер

$$S \geqslant 2^{\frac{1}{14}\left(\frac{n}{g(t)}\right)^{\frac{1}{h+1}}}$$

для достаточно больших n, где $g(t) = (t+1)^2 2^{4t}$.

В четвертой главе мы приводим систематическое исследование схем, состоящих из точных пороговых элементов. В разделе 1 мы вводим основные определения, связанные с точными пороговыми функциями, и приводим базовые свойства вводимых понятий. В разделе 2 мы доказываем результаты о включениях между различными классами функций, вычислимых пороговыми и точными пороговыми схемами. Мы рассматриваем две иерархии точных пороговых схем: одну с весами всех элементов, ограниченными полиномом, и другую с произвольными весами, то есть по аналогии с пороговыми схемами мы вводим классы $\widehat{\mathsf{ELT}}_i$ и ELT_i. Мы показываем, что использование точных пороговых элементов на всех уровнях схемы, кроме самого верхнего, эквивалентно использованию пороговых элементов на этих уровнях. Мы показываем, что эти иерархии вкладываются одна в другую аналогично иерархии для пороговых функций, то есть для всех $i \geqslant 1$ верно $\widehat{\mathsf{ELT}}_i \subseteq \mathsf{ELT}_i \subseteq \widehat{\mathsf{ELT}}_{i+1}$. Более того, мы показываем, что иерархии для пороговых схем и для точных пороговых схем тесно переплетаются, а именно, для всех $i \geqslant 1$ верно $\widehat{\mathsf{LT}}_i \subseteq \widehat{\mathsf{ELT}}_{i+1} \subseteq \widehat{\mathsf{LT}}_{i+1}$ и $\mathsf{LT}_i \subseteq \mathsf{ELT}_{i+1} \subseteq \mathsf{LT}_{i+1}$. В разделе 3 мы доказываем некоторые разделения между классами этой иерархии, а именно, мы доказываем, что $\mathsf{THR} \circ \mathsf{MAJ} \neq \mathsf{ETHR} \circ \mathsf{ETHR}$, $\mathsf{MAJ} \circ \mathsf{MAJ} \neq \mathsf{ETHR} \circ \mathsf{ETHR}$, $\mathsf{THR} \circ \mathsf{MAJ} \neq \widehat{\mathsf{ELT}}_3$ и $\mathsf{MAJ} \circ \mathsf{MAJ} \not\subseteq \mathsf{EMAJ} \circ \mathsf{ETHR}$. Неформально, полученные результаты в целом означают, что точные пороговые схемы следует исследовать наравне с пороговыми схемами, и в тесной связи с последними. Это подтверждается недавними продвижениям в исследованиях пороговых схем[84,85]. В частности, как следствие наших результатов, мы выделяем $\mathsf{ETHR} \circ \mathsf{ETHR}$ как минимальный класс пороговых схем, для которого неизвестны сверхполиномиальные нижние оценки для явно заданных функций.

В пятой главе мы изучаем пороговые функции, в которых булевы переменные принимают значения $\{a, b\}$ для произвольных a и b. Мы в первую очередь сосредотачиваемся на случае $\{1, 2\}$, поскольку этот случай является самым естественным, существенно отличным от хорошо изученных случаев $\{0, 1\}$ и $\{-1, 1\}$. Отметим, однако, что для большинства результатов конкретные значения $\{a, b\}$, существенно отличные от $\{0, 1\}$ и $\{-1, 1\}$, не важны, и все наши результаты верны в случаях, для которых $\operatorname{sgn}(a) = \operatorname{sgn}(b)$.

[84]Chattopadhyay A., Mande N. S. A Short List of Equalities Induces Large Sign Rank // 59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018 / Ed. by M. Thorup. IEEE Computer Society, 2018. P. 47–58.

[85]Chen L., Williams R. R. Stronger Connections Between Circuit Analysis and Circuit Lower Bounds, via PCPs of Proximity // 34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA / Ed. by A. Shpilka. Vol. 137 of *LIPIcs*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. P. 19:1–19:43.

Для данных $l(n)$ и $d(n)$ мы обозначаем через $\mathsf{PTF}_{a,b}(l(n), d(n))$ класс функций $f\colon \{a,b\}^n \to \{0,1\}$, таких что существует $p(x) \in \mathbb{Z}[x]$ с не более чем $l(n)$ мономами и степени не больше $d(n)$, такой что для всех $x \in \{a,b\}^n$ верно $f(x) = 1$ тогда и только тогда, когда $p(x) \geqslant 0$. Особенно интересен для нас случай, когда $l(n)$ полиномиально по n. Мы сокращаем обозначение $\mathsf{PTF}_{a,b}(\mathrm{poly}(n), d(n))$ до $\mathsf{PTF}_{a,b}(d(n))$. Если мы не хотим вводить ограничение на степень, то будем писать $\mathsf{PTF}_{a,b}(l(n), \infty)$ и $\mathsf{PTF}_{a,b}(\infty)$ соответственно. В разделе 1 мы даем предварительные определения и сведения, необходимые для этой главы. В разделе 2 — описываем классы таких пороговых функцией в терминах пороговых схем. Мы доказываем равенства $\mathsf{PTF}_{1,2}(2,\infty) = \mathsf{THR}$, $\mathsf{PTF}_{1,2}(2,\mathrm{poly}(n)) = \mathsf{MAJ}$, $\mathsf{PTF}_{1,2}(O(1),\infty) = \mathsf{ANY}_{O(1)} \circ \mathsf{THR}$, $\mathsf{PTF}_{1,2}(O(1),\mathrm{poly}(n)) = \mathsf{ANY}_{O(1)} \circ \mathsf{MAJ}$, $\mathsf{PTF}_{1,2}(\mathrm{poly}(n)) = \mathsf{THR} \circ \mathsf{MAJ}$. В разделе 3 мы замечаем, что нижние оценки на длину рассматриваемых пороговых элементов следуют из известных методов. Также мы доказываем, что $\mathsf{PTF}_{1,2}(\mathrm{poly}(n)) \subsetneq \mathsf{PTF}_{1,2}(\infty)$ при условии $\mathsf{THR} \circ \mathsf{THR} \not\subseteq \mathsf{THR} \circ \mathsf{MAJ} \circ \mathsf{AND}_2$. В разделе 4 мы рассматриваем макс-плюс аналог наших пороговых функций (здесь нам удобно работать в макс-плюс полукольце, а не в мин-плюс полукольце). Мы доказываем, что такие макс-плюс пороговые функции содержат классы $\mathsf{AND} \circ \mathsf{THR}$, $\mathsf{OR} \circ \mathsf{THR}$ и содержатся в классах $\mathsf{AND} \circ \mathsf{OR} \circ \mathsf{THR}$, $\mathsf{OR} \circ \mathsf{AND} \circ \mathsf{THR}$. Мы выделяем этот класс как промежуточный класс в иерархии схем вида $\mathsf{AC}^0 \circ \mathsf{THR}$. Мы доказываем также, что некоторые нетривиальные функции вычисляются такими макс-плюс пороговыми элементами. Как следствие, мы получаем, что этот класс не содержится в классе $\mathsf{MAJ} \circ \mathsf{MAJ}$. В разделе 5 мы устанавливаем результаты о соотношении введенных классов для различных областей определения $\{a,b\}$. Мы доказываем, что $\mathsf{PTF}_{a,b}(\infty) = \mathsf{PTF}_{a^k,b^k}(\infty)$. Наконец, в разделе 6 мы доказываем дополнительный результат о пороговых схемах, полученный в этих исследованиях как побочный результат, но имеющий самостоятельный интерес. А именно, мы доказываем, что пороговая схема глубины 2 с ограниченными весами на нижнем уровне может быть преобразована в эквивалентную схему с ограниченными весами на нижнем уровне, в которой все функции голосования на нижнем уровне монотонны.

В шестой главе мы исследуем вычисление функции MAJ_n монотонными схемами, состоящими из функций MAJ_k для $k < n$. Как упоминалось выше, известно, что для $k = 3$ существует схема логарифмической глубины. Мы исследуем вопрос с противоположной стороны: для каких k существует схема заданной постоянной глубины d? В разделе 1 мы вводим необходимые обозначения и приводим вспомогательные вероятностные неравенства. В разделе

2 мы доказываем, что для глубины $d = 3$ существует схема с $k = O(n^{2/3})$. Отметим, что для глубины 2 текущая лучшая оценка[86] для случая, когда в элементах MAJ разрешаются произвольные пороги, равна $k \leqslant \frac{2n}{3} + O(1)$. Для случая, если порог обязан равняться $k/2$, известна[87,88] оценка $k \leqslant n-2$. В разделе 3 мы доказываем нижние оценки для произвольной глубины d, а именно, мы доказываем оценку

$$k = \Omega\left(\frac{n^{26/(13d+12)}}{(\log n)^{4/(13d+12)}}\right).$$

Для $d = 2$ эта оценка дает $k = \Omega\left(n^{13/19} \cdot (\log n)^{-2/19}\right)$. Для случая, когда на нижнем уровне все веса ограничены единицей, мы получаем оценку

$$k = \Omega\left(\frac{n^{14/(7d+6)}}{(\log n)^{4/(7d+6)}}\right)$$

для произвольного d и $k = \Omega(n^{7/10} \cdot (\log n)^{-1/5})$ для $d = 2$. Отметим, что последняя оценка для $d = 2$ была позже усилена[89,90], и сейчас лучшая известная оценка составляет $k \geqslant n/2 - o(n)$.

В седьмой главе мы вводим модель гиперграфовых программ и исследуем ее выразительную способность. Эти результаты мотивированы приложениями к исследованию преобразований запросов к базам данных с онтологическим доступом. В разделе 1 мы формализуем понятие баз данных с онтологическим доступом, запросов и их преобразований в терминах логики первого порядка и приводим важные для нас понятия и результаты о базах данных с онтологическим доступом. В разделе 2 мы описываем общий подход к доказательству нижних оценок размера преобразований запросов к базам данных с онтологическим доступом. В разделе 3 мы вводим

[86]Posobin G. Computing majority with low-fan-in majority queries // CoRR. 2017. Vol. abs/1711.10176.

[87]Комбаров, Ю. А. Схема глубины два с ограниченным входным ветвлением для функций голосования // Вестник Московского университета. Серия 1: Математика. Механика. N 5. 2018. P. 58–60.

[88]Amano K., Yoshida M. Depth Two (n-2)-Majority Circuits for n-Majority // IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 2018. Vol. 101-A, N. 9. P. 1543–1545.

[89]Engels C., Garg M., Makino K., Rao A. On Expressing Majority as a Majority of Majorities // SIAM J. Discret. Math. 2020. Vol. 34, N. 1. P. 730–741.

[90]Hrubes P., Ramamoorthy S. N., Rao A., Yehudayoff A. Lower Bounds on Balancing Sets and Depth-2 Threshold Circuits // 46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece / Ed. by C. Baier, I. Chatzigiannakis, P. Flocchini, S. Leonardi. Vol. 132 of *LIPIcs*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. P. 72:1–72:14.

понятие гиперграфовой программы и описываем ее связь с преобразованиями запросов к базам данных с онтологическим доступом. *Гиперграфовой программой* P называется гиперграф H, вершины которого помечены переменными $x_1, \ldots, x_n$, их отрицаниями или константами 0 и 1. Гиперграфовая программа P выдает 1 (мы будем писать $P(\vec{x}) = 1$) на входе $\vec{x} \in \{0,1\}^n$ тогда и только тогда, когда существует множество непересекающихся гиперребер (называемое *покрытием*), покрывающее все вершины, метки которых принимают значение 0. Гиперграфовая программа вычисляет булеву функцию f тогда и только тогда, когда для всех $\vec{x} \in \{0,1\}^n$ верно $P(\vec{x}) = f(\vec{x})$. Размером гиперграфовой программы называется сумма числа вершин и числа гиперребер в гиперграфе. Гиперграфовая программа монотонна тогда и только тогда, когда в ней среди меток нет отрицаний переменных. Через HGP мы обозначаем класс всех функций, вычислимых гиперграфовыми программами полиномиального размера. Мы добавляем нижний индекс k, если степени всех вершин в гиперграфе ограничены k. Мы добавляем верхний индекс $tree$, если гиперграф имеет древесную структуру (на вершинах гиперграфа задано дерево и все гиперребра являются поддеревьями), мы добавляем верхний индекс $path$, если гиперграф имеет линейную структуру (аналогично, но на вершинах гиперграфа задан путь). В разделе 4 мы доказываем следующие результаты о выразительной способности гиперграфовых программ: $\mathsf{HGP} = \mathsf{HGP}_3 = \mathsf{NP/poly}$, $\mathsf{HGP}_2 = \mathsf{coNL/poly}$, $\mathsf{HGP}_2^{tree} = \mathsf{NL/poly}$, $\mathsf{HGP}^{tree} = \mathsf{SAC}^1$, $\mathsf{HGP}_2^{tree} = \mathsf{HGP}_2^{path} = \mathsf{AC}^0_{3,\mathrm{AND}}$. Все перечисленные результаты также переносятся на случай монотонных версий этих классов. Эти результаты позволяют дать оценки размеров преобразований запросов для различных классов запросов и теорий, сопровождающих базы данных.

В восьмой главе мы исследуем свойства корней макс-плюс многочленов (в этой главе нам удобно перейти от мин-плюс полукольца к макс-плюс полукольцу). В разделе 1 мы исследуем вопрос о том, когда макс-плюс многочлен с данным носителем может иметь все точки данного множества своими корнями. Мы доказываем, что для всякого конечного S и для всякого нетривиального макс-плюс многочлена p, такого что $\mathsf{Supp}(p) \subseteq S$, существует $\vec{r} \in S$, не являющийся корнем p (на самом деле, мы доказываем несколько более общий результат). Мы также доказываем, что если $|R| < |S|$, то существует макс-плюс многочлен p с носителем в S, имеющий корни во всех точках R. Это контрастирует со случаем классических многочленов, для которого комбинаторная теорема о нулях дает пример ситуации, когда многочлены с большим носителем не могут иметь корни во всех точках существенного мень-

шего множества[91]. В разделе 2 мы исследуем вопрос о том, сколько корней может иметь макс-плюс многочлен заданной степени в заданном множестве. Мы доказываем следующий аналог классической леммы Шварца-Зиппеля. Пусть $S_1, S_2, \ldots, S_n \subseteq \mathbb{K}$, введем обозначение $|S_i| = k_i$. Тогда для всякого $d \leqslant \min_i k_i$ максимальное число корней, которое невырожденный макс-плюс многочлен p степени d может иметь в $S_1 \times \ldots \times S_n$, равно

$$\prod_{i=1}^{n} k_i - \prod_{i=1}^{n} (k_i - d)\,.$$

В точности такое же утверждение верно для многочленов с индивидуальной степенью по каждой переменной не больше d. В разделе 3 мы исследуем универсальные тестирующие множества для макс-плюс многочленов с заданным числом мономов. *Универсальным тестирующим множеством* для макс-плюс многочленов от n переменных с k мономами называется множество точек $S \subseteq \mathbb{K}^n$, такое что всякий нетривиальный многочлен с не более чем k мономами имеет не корень в одной из точек S. Нашей целью является поиск минимального размера универсального тестирующего множества для данных n и k. Для классических многочленов известно[92,93,94,95], что минимальный размер универсального тестирующего множества равен k. Для макс-плюс многочленов над $\mathbb{K} = \mathbb{R}$ мы доказываем, что также минимальный размер универсального тестирующего множества равен k. Для макс-плюс многочленов над $\mathbb{K} = \mathbb{Q}$ мы доказываем, что для минимального размера универсального тестирующего множества s верно

$$\frac{(k-1)(n+1)+1}{2} \leqslant s \leqslant k(n+1)+1.$$

Для $n = 2$ мы находим точное значение $s = 2k - 1$.

В девятой главе мы исследуем линейные системы мин-плюс многочленов и уравнений. В разделе 1 мы даем основные определения для циклических игр, которые требуются нам в этой главе. В разделе 2 мы доказываем

[91] Alon N. Combinatorial Nullstellensatz // Comb. Probab. Comput. 1999. Vol. 8, N. 1-2. P. 7–29.

[92] Grigoriev D., Karpinski M. The Matching Problem for Bipartite Graphs with Polynomially Bounded Permanents Is in NC (Extended Abstract) // 28th Annual Symposium on Foundations of Computer Science, Los Angeles, California, USA, 27-29 October 1987. 1987. P. 166–172.

[93] Ben-Or M., Tiwari P. A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation // Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing. STOC '88. New York, NY, USA: ACM, 1988. P. 301–309.

[94] Kaltofen E., Yagati L. Improved sparse multivariate polynomial interpolation algorithms // Symbolic and Algebraic Computation: International Symposium ISSAC '88 Rome, Italy, July 4–8, 1988 Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg, 1989. P. 467–474.

[95] Grigoriev D. Y., Karpinski M., Singer M. F. The interpolation problem for k-sparse sums of eigenfunctions of operators // Advances in Applied Mathematics. 1991. Vol. 12, N. 1. P. 76 – 81.

общие утверждения о связи мин-плюс систем многочленов и уравнений (не обязательно линейных). Мы доказываем, что от системы мин-плюс многочленов всегда можно перейти к эквивалентной системе уравнений. Мы доказываем также, что возможен обратный переход (хоть и с дополнительными техническими условиями). Мы переносим эти результаты на случай линейных систем. Как следствие из этих результатов мы доказываем, что задача разрешимости мин-плюс систем линейных многочленов полиномиально эквивалентна известной задаче определения победителя в циклических играх. Про эту задачу известно, что она лежит в $\mathsf{NP} \cap \mathsf{coNP}$, но принадлежность P остается открытым вопросом. В разделе 3 мы переходим к обсуждению размерности множества корней линейной системы мин-плюс многочленов. Заметим, что в этом вопросе не помогает понятие ранга, поскольку оказывается, что для всякой матрицы $A \in \mathbb{R}^{m\times n}$ верно

$$n - tropical\ dimension(A) \leqslant tropical\ rank(A),$$

и неравенство может как обращаться в равенство, так и быть строгим[96]. В этом разделе мы даем комбинаторное описание размерности мин-плюс системы линейных многочленов в терминах существования некоторой блочно-треугольной формы матрицы системы. В разделе 4 мы используем это комбинаторное описание для доказательства NP-полноты задачи, в которой по данной матрице линейной мин-плюс системы и данному k требуется установить, верно ли, что размерность пространства решений системы не меньше k. В разделе 5 мы доказываем результаты о линейной двойственности для мин-плюс линейных систем уравнений и многочленов.

В десятой главе мы доказываем мин-плюс аналог эффективной теоремы Гильберта о нулях, как для систем многочленов, так и для систем уравнений. В разделе 1 мы формулируем доказываемые результаты. Сначала мы вводим понятие двойственной теоремы о нулях, формулируемой в терминах разрешимости линейной системы с матрицей Маколея. Мы формулируем двойственные версии мин-плюс теорем о нулях, отдельно для мин-плюс многочленов и мин-плюс уравнений. После этого мы формулируем и прямые версии этих теорем. В разделе 2 мы доказываем теоремы о нулях для многочленов в двойственной форме. Для этого мы сначала вводим предварительные определения и доказываем предварительные результаты. Затем мы вводим понятие объемлющего многогранника и доказываем, что одна из его граней дает решение системы многочленов для случая полукольца

[96]Grigoriev D., Podolskii V. Complexity of Tropical and Min-plus Linear Prevarieties // Computational Complexity. 2015. Vol. 24, no. 1. P. 31–64.

без бесконечности. Затем мы выводим теорему для полукольца с бесконечностью. Затем мы доказываем точность наших верхних оценок на степень возникающих многочленов в эффективных теоремах о нулях. В частности, результаты этого раздела дают доказательство гипотезы о мин-плюс аналоге теоремы Гильберта о нулях из работы Д.Ю. Григорьева[97]. В разделе 3 мы выводим теоремы о нулях в прямой форме. Отметим, что близкие результаты о прямой теореме Гильберта о нулях для случая мин-плюс уравнений были доказаны независимо в работе А. Бертрама и Р. Истона[98] и в работе Д. Джо и К. Минчевой[99]. Доказательства в этих работах основаны на совершенно другом подходе, результаты не дают эффективную версию теоремы и не переносятся на случай мин-плюс многочленов.

Публикации автора по теме диссертации

1. *Hansen K. A., Podolskii V. V.* Exact Threshold Circuits // Proceedings of the 25th Annual IEEE Conference on Computational Complexity, CCC 2010, Cambridge, Massachusetts, USA, June 9-12, 2010. IEEE Computer Society, 2010. P. 270–279.

2. *Podolskii V. V.* Exponential lower bound for bounded depth circuits with few threshold gates // Inf. Process. Lett. 2012. Vol. 112, N. 7. P. 267–271.

3. *Podolskii V. V.* Lower Bound on Weights of Large Degree Threshold Functions // Log. Methods Comput. Sci. 2013. Vol. 9, N. 2.

4. *Kikot S., Kontchakov R., Podolskii V. V., Zakharyaschev M.* On the succinctness of query rewriting over shallow ontologies // Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), CSL-LICS '14, Vienna, Austria, July 14 - 18, 2014 / Ed. by T. A. Henzinger, D. Miller. ACM, 2014. P. 57:1–57:10.

5. *Bienvenu M., Kikot S., Podolskii V. V.* Tree-like Queries in OWL 2 QL: Succinctness and Complexity Results // 30th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2015, Kyoto, Japan, July 6-10, 2015. IEEE Computer Society, 2015. P. 317–328.

6. *Hansen K. A., Podolskii V. V.* Polynomial threshold functions and Boolean threshold circuits // Inf. Comput. 2015. Vol. 240. P. 56–73.

7. *Grigoriev D., Podolskii V. V.* Complexity of Tropical and Min-plus Linear Prevarieties // Comput. Complex. 2015. Vol. 24, N. 1. P. 31–64.

8. *Grigoriev D., Podolskii V. V.* Tropical Effective Primary and Dual Nullstellensätze // Discret. Comput. Geom. 2018. Vol. 59, N. 3. P. 507–552.

[97]Grigoriev D. On a tropical dual Nullstellensatz // Advances in Applied Mathematics. 2012. Vol. 48, N. 2. P. 457 – 464.

[98]Bertram A., Easton R. The tropical Nullstellensatz for congruences // Advances in Mathematics. 2017. Vol. 308. P. 36 – 82.

[99]Joó D., Mincheva K. Prime congruences of additively idempotent semirings and a Nullstellensatz for tropical polynomials // Selecta Mathematica. 2018. Vol. 24. P. 2207–2233.

9. *Bienvenu M., Kikot S., Kontchakov R., Podolskii V. V., Zakharyaschev M.* Ontology-Mediated Queries: Combined Complexity and Succinctness of Rewritings via Circuit Complexity // J. ACM. 2018. Vol. 65, N. 5. P. 28:1–28:51.

10. *Kulikov A. S., Podolskii V. V.* Computing Majority by Constant Depth Majority Circuits with Low Fan-in Gates // Theory Comput. Syst. 2019. Vol. 63, N. 5. P. 956–986.

11. *Grigoriev D., Podolskii V. V.* Tropical Combinatorial Nullstellensatz and Sparse Polynomials // Found. Comput. Math. 2020. Vol. 20, N. 4. P. 753–781.