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

ДИССЕРТАЦИЯ

на соискание ученой степени

доктора физико-математических наук

Москва — 2021

Содержание

Введение **5**

1 Предварительные сведения **28**

1.1 Булевы функции и булевы схемы 28

1.2 Мин-плюс алгебра 36

2 Веса пороговых функций большой степени **43**

2.1 Построение функции 43

2.2 Нижняя оценка $2^{\Omega(2^{n/4})}$ 46

2.2.1 Доказательство теоремы 2.1 48

2.3 Улучшенная нижняя оценка 56

3 Булевы схемы с небольшим числом пороговых элементов . . . **67**

3.1 Предварительные результаты 67

3.2 Нижняя оценка 69

4 Булевы схемы из точных пороговых элементов **75**

4.1 Точные пороговые функции 75

4.1.1 Базовые свойства 76

4.2 Включения между классами 78

4.3 Разделение классов 84

5 Пороговые элементы над {1,2} **87**

5.1 Предварительные сведения 87

5.2 Описание полиномиальных пороговых функций через через пороговые схемы 89
5.3 Нижние оценки для полиномиальных пороговых функций 95
5.4 Макс-плюс полиномиальные пороговые функции 98
5.5 Соотношения между областями определения 103
5.6 Пороговые схемы с монотонными элементами 105

6 Вычисление функции голосования с помощью функций голосования меньшего числа переменных 107
6.1 Обозначения и вспомогательные результаты 107
6.2 Верхняя оценка для случая глубины 3 109
6.3 Нижние оценки 111

7 Базы данных, снабженные логическими теориями 124
7.1 Теории, запросы и их преобразования 124
7.2 Нижние оценки размера преобразований: общий подход 136
7.3 Гиперграфовые програмы: связь с преобразованиями запросов . . 138
7.4 Гиперграфовые программы: сложность 143
7.4.1 Произвольные гиперграфовые программы HGP 144
7.4.2 Гиперграфовые программы степени 2 146
7.4.3 Линейные HGP 149
7.4.4 Древесные HGP 151
7.4.5 Древесные HGP степени 2 162

8 Корни макс-плюс многочленов 166
8.1 Макс-плюс аналог комбинаторной теоремы о нулях 166
8.2 Макс-плюс аналог леммы Шварца-Зиппеля 172
8.3 Универсальные тестирующие множества 174
8.3.1 Тестирующие множества над $\mathbb{R}$ 174
8.3.2 Тестирующее множество над $\mathbb{Q}$ 176

9 Мин-плюс линейные системы 188
9.1 Циклические игры 188
9.2 Мин-плюс многочлены и мин-плюс уравнения 190
9.3 Комбинаторное описание размерности множества корней 198
9.4 Задача о подсчете размерности множества решений мин-плюс систем NP-полна 205
9.5 Линейная двойственность в мин-плюс алгебре 212
9.5.1 Формулировки результатов 212
9.5.2 Линейная двойственность для систем неравенств 216
9.5.3 Линейная двойственность для систем многочленов 219

10 Мин-плюс аналоги теоремы Гильберта о нулях 223
10.1 Формулировки результатов 224
10.2 Теоремы о нулях в двойственной форме 230
10.2.1 Предварительные понятия и результаты 231
10.2.2 Объемлющий многогранник 238
10.2.3 Сингулярность грани P_0 242
10.2.4 Примеры 245
10.2.5 Теоремы о нулях в двойственной форме над $\mathbb{R}_\infty$ 247
10.2.6 Нижние оценки 260
10.3 Теоремы о нулях в прямой форме 264

Список работ, в которых опубликованы основные результаты диссертации 268

Список литературы 270

Введение

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 Шеннона [116]. 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 [116] 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 [133].

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 [38,134]. 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 [115]. 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 методов. 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 [137], 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, например, в [129, 6] (см. также обзор [132]).

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 [1, 49], 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 была доведена до экспоненциальной в [71]. 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 класса AC^0. Например, в качестве таких функций можно добавить функции PARITY и MAJ. Тогда для получившегося класса схем добавленные функции уже являются просты-

ми. Соответственно, класс становится сильнее по сравнению с AC^0, и для него нижние оценки нужно доказывать отдельно. Для случая добавления функции PARITY сверхполиномиальные нижние оценки были получены в [138, 121]. 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 [102].

В случае же, если мы в качестве элементов в AC^0-схемы добавляем функцию MAJ, ситуация оказывается более сложной. Этот класс принято обозначать через TC^0. Известно, что функция PARITY, как и все функции MOD_m, оказываются простыми и вычисляются 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 (см., напр., [128]). Из верхних оценок вычислительных способностей этого класса, известно, что всякая функция, вычислимая такой схемой полиномиального размера, вычислима также схемой логарифмической 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 [111]. 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 $\mathcal{C}_1$ и $\mathcal{C}_2$ обозначим через $\mathcal{C}_1 \circ \mathcal{C}_2$ класс схем, состоящих из схем из класса $\mathcal{C}_1$, в которые подставлены выхо-

ды схем из класса $\mathcal{C}_2$. Обозначим через ANY класс всех булевых функций. Этот класс мы будем использовать только с нижним индексом. Также отметим, что размер бывает полезно измерять как числом элементов схемы, так и числом ребер. В большинстве случаев эти меры эквивалентны 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 равны ± 1.

Нетрудно видеть, что $\cup_{d\geqslant 1}\widehat{\mathsf{LT}}_d = \mathsf{TC}^0$. Соотношение с классами LT_d не очевидно, однако в серии работ [34, 106, 120, 51] было показано, что $\cup_{d\geqslant 1}\mathsf{LT}_d = \mathsf{TC}^0$, и более точно, для всякого $d \geqslant 1$ выполняется $\mathsf{LT}_d \subseteq \widehat{\mathsf{LT}}_{d+1}$ [51]. 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 [66]. 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 $\mathsf{MAJ}\circ\mathsf{THR} = \mathsf{MAJ}\circ\mathsf{MAJ}$ [52]. Для второго также известны сильные нижние оценки [46, 112, 36] и известны отделения от классов $\mathsf{MAJ} \circ \mathsf{MAJ}$ [52] и $\mathsf{THR} \circ \mathsf{THR}$ [36]. 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, и доказаны в работе [83].

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 [98]. С тех пор полиномиальные пороговые элементы нашли массу применений в сложности булевых схем, структурной теории сложности, теории обучения и коммуникационной сложности (см., напр., [110, 88, 16, 117]).

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 эту величину были доказаны для $d = 1$. В [101] (см. также [100] и [73]) было доказано, что для всех f с $\deg_\pm f = 1$ выполняется $W(f,1) = n^{O(n)}$. В [73] было доказано, 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, что $W(f,d) = n^{O(dn^d)}$ (см. [114, 28, 135]). В работе [135] было доказано, 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

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

Лучшая ранее известная оценка этой величины следует из работы [135] и 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 [10] была доказана экспоненциальная нижняя оценка для схем с одним элементом MAJ, вычисляющих PARITY. Этот результат был усилен в работах [18, 17], где была доказана 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 доказана в [10]: оценка в статье сформулирована для схем с элементом MAJ, но доказательство буквально переносится и на случай элемента THR. Результаты работ [18, 17], напротив, не переносятся с элементов MAJ на элементы THR. Что касается сверхполиномиальных оценок, то в работе [35] доказана оценка $n^{\Omega(\log n)}$ для схем с $O(\log^2 n)$ элементами THR. Эта оценка доказана для функции, более сложной, чем PARITY. В работе [55] доказана 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) [127]. Доказательство этого результата

вероятностное, и известные детерминированные конструкции дают существенно худшее значение глубины [2]. Существует также версия этой конструкции, в которой схема состоит из элементов MAJ_3 (см., напр., [54]).

Наряду с пороговыми функциями можно рассматривать точные пороговые функции. Булева функция $f\colon \{0,1\}^n \to \{0,1\}$ называется *точной пороговой*, если существуют целые числа $t, w_1, \ldots, w_n$, такие что

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

Можно рассматривать точные пороговые функции в качестве элементов схемы. Однако, результатов о таких схемах довольно мало и они разрозненны [19, 57, 67, 68].

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

Другое направление связано с приложениями теории сложности булевых схем в 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[1]. 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 [92]). Однако, этот подход вынужден постоянно преодолевать сложности с реализуемостью. Основная проблема состоит в том, что если теория, добавля-

[1]Неформально мы используем слова «база данных» в широком смысле, как структурированный набор данных. Позднее в формальном изложении мы сопоставим базам данных некоторые логические теории первого порядка.

емая 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. 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 [126]. В результате этих усилий возникли несколько направлений, каждое со своими специфическими целями. Среди недавних таких направлений можно выделить область интеграции данных (см. обзор в [95]) и область обмена данных [45, 89].

Другим актуальным направлением является теория баз данных с онтологическим доступом, ее развитие началось примерно с 2005 г. [32, 42, 104, 107]. 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. 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 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 (см., напр., [78, 96, 123, 97, 113, 76, 130]). Важным достоинством мин-плюс алгебры является то, что она делает некоторые свойства классических объектов доступными для вычислений [125, 78, 96, 123]: с одной стороны, мин-плюс аналоги классических объектов отражают некоторые свойства классических объектов, а с другой стороны, мин-плюс объекты

имеют гораздо более 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 у независимости векторов [41,79,3]. 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* (см. определения и основные результаты в работе [41]). 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 [41]. Также для мин-плюс линейных многочленов изучены аналог определителя матрицы и его свойств [3, 41, 60], аналог гауссовской верхне-треугольной формы [60]. 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 [4]. Для мин-плюс систем линейных неравенств известно, что задача о разрешимости полиномиально эквивалентна задача об определении победителя в циклических играх [4].

Для мин-плюс многочленов произвольной степени известно намного меньше. В [119] было дано явное описание радикала мин-плюс идеала. В [113, 122]

была доказана мин-плюс версия теоремы Безу для случая, когда число многочленов равно числу переменных. В [40] теорема Безу была распространена на системы многочленов произвольного размера. В [24] была доказана оценка на число невырожденных корней системы разреженных мин-плюс многочленов. В [125] было доказано, что задача разрешимости мин-плюс систем многочленов NP-полна. В [59] была выдвинута гипотеза о мин-плюс аналоге теоремы Гильберта о нулях в двойственной форме.

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

Основные результаты работы кратко можно сформулировать следующим образом.

— 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.

Опишем кратко структуру 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 первом разделе приводится конструкция функции, для которой во втором разделе 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 третьем разделе 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 функций PARITY. В первом разделе приводятся

известные вспомогательные результаты, необходимые именно в этой главе. Во втором разделе 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 $\mathsf{LT}_i \subseteq \mathsf{ELT}_{i+1} \subseteq \mathsf{LT}_{i+1}$. Также 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 [36, 37]. 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 $\operatorname{sgn}(a) = \operatorname{sgn}(b)$. 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 $\mathsf{PTF}_{a,b}(\operatorname{poly}(n), d(n))$ 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 $\mathsf{PTF}_{1,2}(2, \infty) = \mathsf{THR}$, $\mathsf{PTF}_{1,2}(2, \operatorname{poly}(n)) = \mathsf{MAJ}$, $\mathsf{PTF}_{1,2}(O(1), \infty) = \mathsf{ANY}_{O(1)} \circ \mathsf{THR}$, $\mathsf{PTF}_{1,2}(O(1), \operatorname{poly}(n)) = \mathsf{ANY}_{O(1)} \circ \mathsf{MAJ}$, $\mathsf{PTF}_{1,2}(\operatorname{poly}(n)) = \mathsf{THR} \circ \mathsf{MAJ}$. В разделе 3 мы замечаем, что нижние оценки на длину рассматриваемых пороговых элементов следуют из известных методов. Также мы доказываем, что $\mathsf{PTF}_{1,2}(\operatorname{poly}(n)) \subsetneq \mathsf{PTF}_{1,2}(\infty)$ 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. 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 $\mathrm{MAJ} \circ \mathrm{MAJ}$. 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 $O(n^{2/3})$. Отметим, что для глубины 2 текущая лучшая оценка для случая, когда в элементах MAJ разрешаются произвольные пороги, равна $k \leqslant \frac{2n}{3} + O(1)$ [26, 108]. Для случая, если порог обязан равняться $k/2$ известна оценка $k \leqslant n - 2$ [131, 8] 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 последовательно усилена в работах [44, 75] до $k \geqslant n/2 - o(n)$.

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 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: $\mathsf{HGP} = \mathsf{HGP}_3 = \mathsf{NP}/\mathrm{poly}$, $\mathsf{HGP}_2 = \mathsf{coNL}/\mathrm{poly}$, $\mathsf{HGP}_2^{tree} = \mathsf{NL}/\mathrm{poly}$, $\mathsf{HGP}^{tree} = \mathsf{SAC}^1$, $\mathsf{HGP}_2^{tree} = \mathsf{HGP}_2^{path} = \mathsf{AC}^0_{3,\mathrm{AND}}$. 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 меньшего множества [5]. 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 уни-

версальные 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 найти минимальный размер универсального тестового множества для данных n и k. Для классических многочленов вопрос изучался в серии работ [61, 20, 82, 65], где было доказано, что минимальный размер универсального тестового множества равен k. Для макс-плюс многочленов над $\mathbb{K} = \mathbb{R}$ мы доказываем, что также минимальный размер универсального тестового множества равен k. Для макс-плюс многочленов над $\mathbb{K} = \mathbb{Q}$ мы доказываем, что для минимального размера универсального тестового 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 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 известна, 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 [62]. 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 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 [59]. 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 [21, 80]. Доказательства в этих работах основаны на совершенно другом подходе, результаты не дают эффективную версию теоремы и не переносятся на случай мин-плюс многочленов.

Глава 1

Предварительные сведения

1.1 Булевы функции и булевы схемы

Мы будем использовать обозначение $[n] = \{1, \ldots, n\}$.

В большинстве глав работы мы будем исследовать булевы функции, то есть функции, аргументы и значения которых принимают значения в двухэлементном множестве. Стандартным для нас будет соглашение, что это двухэлементное множество есть просто $\{0, 1\}$, то есть булевой функцией будет называться функция вида

$$f\colon \{0,1\}^n \to \{0,1\}.$$

Кроме представления булевых функций в виде $f\colon \{0,1\}^n \to \{0,1\}$, мы также будем рассматривать булевы функции в форме $f\colon \{-1,+1\}^n \to \{-1,+1\}$, это оказывается полезным в некоторых ситуациях. В этом представлении -1 соответствует булевому значению «истина», а 1 соответствует значению «ложь».

Можно также рассматривать и другие двухэлементные множества в качестве области определения и области значений булевой функции. Мы каждый раз будем указывать, какое множество рассматривается в данный момент.

Для нас будет важно понятие линейных пороговых функций, задаваемых линейными неравенствами над действительными числами. Пусть $x_1, \ldots, x_n \in \{0, 1\}$ — булевы переменные. Для $w = (w_1, \ldots, w_n) \in \mathbb{R}^n$ и $t \in \mathbb{R}$ мы определяем *пороговый элемент* как линейную форму $\sum_{i=1}^n w_i x_i - t$. Пороговый элемент задает булеву функцию $\mathrm{THR}_{w,t}$ следующим образом: $\mathrm{THR}_{w,t}(x) = 1$ тогда и только тогда, когда $\sum_{i=1}^n w_i x_i - t \geqslant 0$. Мы называем w вектором весов порого-

вого элемента, а его координаты — *весами*. Мы называем t *порогом* порогового элемента. Отдельно важен частный случай, в котором веса равны 1, а порог равен $n/2$. В этом случае мы обозначаем введенную функцию через MAJ и называем функцией голосования, то есть $\mathrm{MAJ}(x) = 1$ тогда и только тогда, когда $\sum_{i=1}^{n} x_i \geqslant n/2$.

Оказывается, что любую линейную пороговую функцию можно представить пороговым элементом с целыми весами ограниченной величины.

Утверждение 1.1 ([101]). *Всякую пороговую функцию от n переменных можно вычислить пороговым элементом с целыми весами, по модулю не превосходящими $(n+1)^{(n+1)/2}/2^n$.*

В дальнейшем, если не сказано обратное, мы всегда предполагаем, что веса в пороговых элементах целые.

Мы также будем рассматривать другие стандартные функции, например, AND, OR и XOR от произвольного числа переменных n. Для функции XOR мы также будем использовать другое обозначение PARITY. С помощью нижнего индекса мы будем обозначать количество переменных в этих функциях тогда, когда это требуется, например AND_k — это конъюнкция k булевых переменных. Мы будем обозначать функцию взятия отрицания через NOT.

Линейные пороговые функции можно обобщить на случай многочленов большей степени. *(Полиномиальным) пороговым элементом* для булевой функции $f\colon \{0,1\}^n \to \{0,1\}$ называется целочисленный многочлен $p(x)$ от n переменных $x = (x_1, \ldots, x_n)$, такой что для всякого $x \in \{0,1\}^n$ верно $f(x) = 1$ тогда и только тогда, когда $p(x) \geqslant 0$. Можно сказать это иначе: для всех $x \in \{0,1\}^n$ верно $f(x) = \operatorname{sgn} p(x)$, где мы принимаем следующее определение знаковой функции: $\operatorname{sgn}(t) = 1$, если $t \geqslant 0$, и $\operatorname{sgn}(t) = 0$ иначе. Таким образом, полиномиальный пороговый элемент — это просто представление булевой функции знаком многочлена. Функцию, соответствующую данному пороговому элементу мы иногда будем называть его *знаковой функцией*. Заметим, что как и в

случае линейных пороговых элементов, мы можем здесь рассматривать целочисленный многочлен без ограничения общности: если функция представляется знаком многочлена с действительными коэффициентами, то она представляется и знаком целочисленного многочлена.

Двумя ключевыми мерами сложности пороговых функций является их степень и вес. *Степенью* $\deg p$ порогового элемента p называется просто степень многочлена. *Весом* $W(p)$ порогового элемента p называется сумма абсолютных значений его коэффициентов.

С этими мерами сложности пороговых элементов связаны следующие меры сложности булевых функций. Пороговой степенью функции f называется минимальная степень порогового элемента для f. Мы обозначаем ее через $\deg_{\pm} f$. Нас также будет интересовать минимальный вес порогового элемента заданной степени не больше d для функции f. Мы будем обозначать эту величину через $W(f, d)$. Заметим, что она определена, только если $d \geqslant \deg_{\pm} f$. Также нетрудно видеть, что для всех f верно $\deg_{\pm} f \leqslant n$ и $W(f, n) \leqslant 2^{O(n)}$ (просто рассмотрим многочлен p, такой что $p(x) = f(x)$ для всех x).

Мы можем определить полиномиальные пороговые элементы также для функций над переменными $\{-1, +1\}$. Заметим, что переход между переменными $\{0, 1\}$ и $\{-1, +1\}$ можно выполнить с помощью простой линейной замены. Так что пороговая степень функции не зависит от того, над какими переменными мы ее рассматриваем, а вес может измениться не более чем на множитель 2^n (см. [93] для более подробного обсуждения связи весов в этих двух постановках).

Пусть $\mathcal{G}$ — некоторое семейство булевых функций. *Булевой схемой* C над базисом $\mathcal{G}$ называется ациклический ориентированный граф. Каждая его вершина входной степени 0 помечена либо константой 0 или 1, либо переменной, либо ее отрицанием. Такие вершины называются *входными элементами* схемы. Каждая из остальных вершин помечена одной из функций из $\mathcal{G}$. При этом входная степень вершин равна числу переменных соответствующей ей функ-

ции, и установлено взаимно однозначное соответствие входящих ребер вершины с переменными функции. Вершины схемы вместе с сопоставленными им функциями называются *элементами* схемы. Для всякого не входного элемента g его *входами* называются элементы, из которых выходят ребра в g. Один из элементов схемы выделяется как *выходной элемент* схемы. При данном $\vec{x} \in \{0,1\}^n$ мы можем последовательно по индукции сопоставить с каждым элементом схемы его значение. Значение входного элемента равно значению соответствующей ему функции (константы, переменной или ее отрицания). Значения остальных элементов вычисляются применением функции, соответствующей этому элементу, к его входам. Значение схемы C на входе $\vec{x} \in \{0,1\}^n$ обозначается через $C(\vec{x})$ и определяется как значение выходного элемента схемы на $\vec{x}$. Схема C *вычисляет* функцию $f\colon \{0,1\}^n \to \{0,1\}$ тогда и только тогда, когда $C(\vec{x}) = f(\vec{x})$ для всех $\vec{x} \in \{0,1\}^n$. *Размером* схемы обычно называется число элементов или число ребер в ней. В случаях, когда в схеме нет кратных ребрах, эти величины квадратично связаны. Там, где это существенно, мы будем уточнять, что в данном случае понимается под размером схемы.

Число n входных переменных функции является параметром. Так что мы обычно рассматриваем не индивидуальную функцию, а последовательность функций $f = \{f_n\}_{n\in\mathbb{N}}$, где $f_n\colon \{0,1\}^n \to \{0,1\}$. Аналогично мы рассматриваем последовательность схем, и мы говорим, что $C = \{C_n\}_{n\in\mathbb{N}}$ *вычисляет* f тогда и только тогда, когда C_n вычисляет f_n для всех n.

Схема C имеет *полиномиальный размер*, если существует многочлен $p \in \mathbb{Z}[t]$, такой что размер C_n не больше $p(n)$.

Формулой называется булева схема, в которой из каждого элемента выходит не более одного ребра. Схема называется *монотонной* тогда и только тогда, когда в ней не используются отрицания переменных и все функции в элементах схемы монотонны. Легко видеть, что монотонные схемы могут вычислять только монотонные булевы функции.

В качестве элементов схемы мы можем рассматривать стандартные функции, такие как, AND, OR, XOR. Но мы также можем рассматривать в качестве элементов схемы и другие функции, например, пороговые функции. Мы также можем рассматривать элементы NOT в схемах, но в большинстве рассматриваемых нами классов схем отрицания можно пронести вниз к переменным, и тем самым, избавиться от них.

Обозначим через THR семейство всех функций вида $\mathrm{THR}_{w,t}$ для произвольных w и t. Обозначим через MAJ, AND, OR, XOR семейства всех функций вида MAJ, AND, OR и XOR соответственно. Аналогично функциям, мы можем добавлять нижний индекс к этим множествам, чтобы указывать верхнюю границу на число переменных в функции. Обозначим через SYM класс симметричных булевых функций (то есть, функций, не меняющихся при произвольной перестановке переменных). Обозначим через ANY класс всех булевых функций. Этот последний класс мы будем использовать только с нижним индексом, указывающим верхнюю границу на число переменных в функциях. Иногда нам нужно будет рассматривать булевы схемы, состоящие лишь из одного элемента, лежащего в каком-то семействе. Для таких классов схем мы будем использовать те же обозначения THR, MAJ и другими. Отличие класса функций от класса схем состоит лишь в том, что в схемах допускается применение отрицания к переменным. Там где это может вызывать путаницу, мы будем уточнять, разрешаются ли в данном случае применения отрицаний к переменным.

С помощью этих семейств мы можем определить различные классы булевых функций. AC^0 определяется как класс всех схем, глубина которых ограничена константой, и которые состоят из функций $\mathsf{AND} \cup \mathsf{OR}$ (произвольной входной степени). Мы заводим также варианты этого класса конкретной глубины, полагая AC^0_d равным классу всех таких схем глубины i для $i \geqslant 1$. Мы также обозначаем через $\mathsf{AC}^0_{d,\mathsf{AND}}$ и $\mathsf{AC}^0_{d,\mathsf{OR}}$ подклассы этого класса схем, в которых выходной элемент лежит в классе AND и OR соответственно. Нетрудно заметить, что в та-

ких схемах можно предполагать, что уровни элементов AND и OR чередуются. Например, можно считать, что схемы из $\mathsf{AC}^0_{3,\mathsf{AND}}$ имеют вид $\mathsf{AND} \circ \mathsf{OR} \circ \mathsf{AND}$.

Отметим, что во всех вводимых классах нас также интересует оценка размера схемы. Если не сказано обратное, мы всюду предполагаем, что речь идет только о схемах полиномиального размера. Мы также будем отождествлять (там, где это не вызывает путаницу) класс схем с классом функций, которые можно вычислить такими схемами.

Определим TC^0 как класс схем, глубина которых ограничена константой, и которые состоят из функций MAJ. Мы заводим также варианты этого класса конкретной глубины, полагая TC^0_i равным классу всех таких схем глубины i для $i \geqslant 1$. Таким образом, $\mathsf{TC}^0 = \cup_{i=1}^{\infty} \mathsf{TC}^0_i$. Для этих классов размер мы измеряем числом ребер.

Для $i \geqslant 1$ положим LT_i равным классу схем глубины i, состоящих из функций THR. Мы также определяем версию этого класса с «маленькими весами»: определим $\widehat{\mathsf{LT}}_i$ как подкласс LT_i, в котором все веса во всех элементах ограничены полиномом от n.

Заметим, что полиномиальные веса можно промоделировать кратными ребрами, а отрицательные веса можно промоделировать допонительными отрицаниями (которые затем можно пронести ко входам). Так что верен следующий несложный факт.

Утверждение 1.2. *Для всех $i \geqslant 1$ верно $\widehat{\mathsf{LT}}_i = \mathsf{TC}^0_i$.*

Из имеющихся классов схем мы можем получать новые с помощью операции композиции. Для данных классов $\mathcal{C}_1$ и $\mathcal{C}_2$ обозначим через $\mathcal{C}_1 \circ \mathcal{C}_2$ класс схем, состоящих из схем из класса $\mathcal{C}_1$, в которые подставлены выходы схем из класса $\mathcal{C}_2$.

Мы определяем класс $\mathsf{P/poly}$ как класс всех функций, вычислимых схемами полиномиального размера с элементами из AND_2 и OR_2. Классом NC^1 мы называем класс всех функций, вычислимых формулами полиномиального размера с

элементами из AND_2 и OR_2. Мы говорим, что булева функция f лежит в классе $\mathsf{NP}/\mathrm{poly}$ тогда и только тогда, когда существует многочлен $p(n)$ и схема C из класса P/poly полиномиального размера, такие что для всех n и всех $\vec{x} \in \{0,1\}^n$

$$f(\vec{x}) = 1 \;\Leftrightarrow\; \exists \vec{y} \in \{0,1\}^{p(n)} \;\; C_{n+p(n)}(\vec{x}, \vec{y}) = 1. \tag{1.1}$$

Отметим особенность монотонного аналога класса $\mathsf{NP}/\mathrm{poly}$: разрешается использовать отрицания в схеме C при переменных из $\vec{y}$.

Отметим, что классы P/poly и $\mathsf{NP}/\mathrm{poly}$ являются неоднородными аналогами классов P и NP (неоднородность означает, что для различных размеров входа схемы могут быть существенно различны, чего не происходит, например, для машин Тьюринга).

Через SAC^1 обозначим класс схем глубины $O(\log n)$, состоящих из функций OR и AND_2 (про такие схемы обычно говорят, что входная степень в них *полуограничена*).

Наконец, нам помимо булевых схем потребуется еще одна модель вычислений. *Недетерминированной ветвящейся программой* B называется ориентированный граф $G = (V, E)$, ребра которого помечены константами 0 и 1, переменными $x_1, \ldots, x_n$ или их отрицаниями. В графе выделены две вершины s и t. На входе $\vec{x} \in \{0,1\}^n$ ветвящаяся программа B выдает $B(\vec{x}) = 1$ тогда и только тогда, когда существует путь из s в t, проходящий только по ребрам, значения меток которых равны 1. Недетерминированная ветвящаяся программа B *вычисляет* функцию $f\colon \{0,1\}^n \to \{0,1\}$ тогда и только тогда, когда для любого $\vec{x} \in \{0,1\}^n$ верно $B(\vec{x}) = f(\vec{x})$. *Размером* ветвящейся программы называется сумма числа ее вершин и числа ребер $|V| + |E|$. Ветвящаяся программа *монотонна*, если в ней не используются отрицания переменных.

Так же как и для функций и схем, под ветвящейся программой мы будем понимать последовательность ветвящихся программ B_n от n переменных для всех $n \in \mathbb{N}$.

Ветвящаяся программа B является программой *полиномиального размера*, если существует многочлен $p \in \mathbb{Z}[x]$, такой что размер B_n не превышает $p(n)$.

Булева функция f лежит в классе NBP тогда и только тогда, когда существует ветвящаяся программа полиномиального размера B, вычисляющая f. Известно, что NBP является неоднородным аналогом класса NL функций, вычислимых недетерминированными машинами Тьюринга на логарифмической памяти, то есть $\mathsf{NBP} = \mathsf{NL}/\mathrm{poly}$ [81, 109].

Для введенных классов выполняется следующая цепочка вложений [81]:

$$\mathsf{AC}^0 \subset \mathsf{NC}^1 \subseteq \mathsf{NBP} \subseteq \mathsf{SAC}^1 \subseteq \mathsf{P}/\mathrm{poly} \subseteq \mathsf{NP}/\mathrm{poly}. \tag{1.2}$$

Известно, что первое включение в этой цепочке строгое [48,1,71]. Вопрос о строгости каждого из остальных включений является крупной открытой проблемой в теории сложности вычислений.

Нам будет удобно для каждого из введенных выше классов K обозначать его монотонную версию через mK.

Похожая цепочка выполняется и для монотонных классов:

$$\mathsf{mAC}^0 \subset \mathsf{mNC}^1 \subset \mathsf{mNBP} \subseteq \mathsf{mSAC}^1 \subset \mathsf{mP}/\mathrm{poly} \subset \mathsf{mNP}/\mathrm{poly}. \tag{1.3}$$

Известно, что все включения в этой цепочке, кроме среднего, строгие (см. [81]). Нам потребуются неравенства классов $\mathsf{mP}/\mathrm{poly} \neq \mathsf{mNP}/\mathrm{poly}$ [137, 6] и $\mathsf{mNBP} \neq \mathsf{mNC}^1$ [84].

Для класса NBP определим класс coNBP как класс всех булевых функций f, таких что $\neg f \in \mathsf{NBP}$. В монотонном случае мы определяем монотонную версию coNBP как класс всех булевых функций f, таких что $f^* \in \mathsf{mNBP}$, где f^* — двойственная к f функция, то есть $f^*(x) = \neg f(\neg x)$ для всех x.

Нам также потребуются определения еще нескольких конкретных функций.

Определение 1.1. *Для булевых векторов $x, y \in \{0,1\}^n$ положим* $\mathrm{GT}(x, y) = 1$ *тогда и только тогда, когда $x \geqslant y$, где $x = (x_1, \ldots, x_n)$ и $y = (y_1, \ldots, y_n)$*

рассматриваются как двоичные записи целых чисел, в которых x_n и y_n — старшие биты.

Определение 1.2. *Для булевых векторов $x, y \in \{0,1\}^n$ функция непересечения* DISJ *определяется как* $\mathrm{DISJ}(x,y) = 1$ *тогда и только тогда, когда для всех i, $(x_i = 0 \vee y_i = 0)$. То есть, если мы рассмотрим x и y как характеристические векторы подмножеств $\{1,\ldots,n\}$, то* $\mathrm{DISJ}(x,y) = 1$ *тогда и только тогда, когда $x \cap y = \emptyset$.*

Определение 1.3. *Для булевых векторов $x, y \in \{0,1\}^n$ функция скалярное произведение* $\mathrm{IP}_2(x,y)$ *определяется как* $\mathrm{IP}_2(x,y) = \bigoplus_{i=1}^{n}(x_i \wedge y_i)$. *То есть, функция* IP_2 *вычисляет скалярное произведение двух поданных на вход векторов.*

Определение 1.4. *Для вектора $x \in \{0,1\}^n$ функция ODD-MAX-BIT (сокращенно* OMB*) определяется как* $\mathrm{OMB}(x_1,\ldots,x_n) = 1$ *тогда и только тогда, когда* $(\max\{i \mid x_i = 1\} \mod 2) = 1$. *То есть, функция равна единице, если самая правая единица среди входных битов встречается на нечетной позиции. Если в x нет единиц, то значение функции равна нулю.*

1.2 Мин-плюс алгебра

Мин-плюс или *тропическое* полукольцо определяется как 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:

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

Существенное различие полуколец с ∞ и без нее состоит в наличии нейтрального элемента по мин-плюс сложению.

Заметим, что аналогично мы можем рассмотреть макс-плюс полукольцо, где в качестве операции $\oplus$ используется операция взятия максимума. В этом случае, элемент $+\infty$ в полукольце (если он присутствует) заменяется на $-\infty$. В остальном все результаты без труда переносятся между макс-плюс и мин-плюс случаями. В разных разделах работы мы будем переходить между макс-плюс и мин-плюс полукольцом в зависимости от удобства.

Мин-плюс моном от переменных $\vec{x} = (x_1, \ldots, x_n)$ определяется как

$$m(\vec{x}) = c \odot x_1^{\odot i_1} \odot \ldots \odot x_n^{\odot i_n}, \tag{1.4}$$

где c — элемент полукольца $\mathbb{K}$, а $i_1, \ldots, i_n$ — неотрицательные целые числа. В классических обозначениях моном соответствует линейной функции

$$m(\vec{x}) = c + i_1 x_1 + \ldots + i_n x_n.$$

Для $\vec{x} = (x_1, \ldots, x_n)$ и $I = (i_1, \ldots, i_n)$ мы вводим обозначение

$$\vec{x}^I = x_1^{\odot i_1} \odot \ldots \odot x_n^{\odot i_n} = i_1 x_1 + \ldots + i_n x_n = \langle \vec{x}, I \rangle.$$

Здесь для векторов $\vec{a}, \vec{b} \in \mathbb{K}^n$ через $\langle \vec{a}, \vec{b} \rangle$ мы обозначаем их скалярное произведение. Степенью монома m называется сумма $i_1 + \ldots + i_n$. Мы обозначаем эту сумму через $|I|$.

Мин-плюс многочленом называется мин-плюс сумма мин-плюс мономов

$$p(\vec{x}) = \bigoplus_i m_i(\vec{x})$$

или в классических обозначениях $p(\vec{x}) = \max_i m_i(\vec{x})$. *Степенью* мин-плюс многочлена p, обозначаемой через $\deg(p)$, называется максимальная степень его мономов. Точка $\vec{a} \in \mathbb{K}^n$ называется *корнем* мин-плюс многочлена p, если максимум $\max_i \{m_i(\vec{a})\}$ достигается на не менее чем двух мономах среди m_i, либо равен ∞.

Геометрически на конечных точках мин-плюс многочлен $p(\vec{x})$ — это кусочно-линейная вогнутая функция (а макс-плюс многочлен, соответственно, выпуклая

функция), а корни p — это точки негладкости этой функции, то есть точки, в которых сходятся несколько линейных частей.

На мин-плюс многочленах можно естественным образом рассматривать операции сложения и умножения. В частности, *произведением* двух мин-плюс многочленов $p(\vec{x}) = \bigoplus_i m_i(\vec{x})$ и $q(\vec{x}) = \bigoplus_j m'_j(\vec{x})$ мы называем мин-плюс многочлен $p \odot q$, мономами которого являются произведения $m_i(\vec{x}) \odot m'_j(\vec{x})$ для всех i, j. Нам потребуется следующее наблюдение.

Лемма 1.1. *Точка $\vec{a} \in \mathbb{K}^n$ является корнем $p \odot q$ тогда и только тогда, когда она является корнем $p(\vec{x})$ или $q(\vec{x})$.*

Доказательство. Пусть $\vec{a}$ — корень p. Если $p(\vec{a}) = \infty$, то легко видеть, что и значение $p \odot q$ бесконечно в этой точке. Иначе, пусть $m_{i_1}(\vec{x}), m_{i_2}(\vec{x})$ — различные мономы p, для которых $m_{i_1}(\vec{a}) = m_{i_2}(\vec{a}) = \min_i m_i(\vec{a})$. Пусть $m'_{j_1}(\vec{x})$ моном q, такой что $m'_{j_1}(\vec{a}) = \min_j m'_j(\vec{a})$. Тогда $m_{i_1} \odot m'_{j_1}$ и $m_{i_2} \odot m'_{j_1}$ — два различных монома $p \odot q$ с минимальным значением на $\vec{a}$ среди всех мономов $p \odot q$. Симметричное рассуждение показывает, что всякий корень q является корнем $p \odot q$.

Если $\vec{a}$ не является корнем ни p, ни q, то существуют единственные i_1 и j_1, такие что $m_{i_1}(\vec{a}) = \min_i m_i(\vec{a})$ и $m'_{j_1}(\vec{a}) = \min_j m'_j(\vec{a})$. Тогда минимальное значение на $\vec{a}$ среди всех мономов $p \odot q$ достигается на единственном мономе $m_{i_1} \odot m'_{j_1}$, а следовательно, $\vec{a}$ не является корнем $p \odot q$. ■

Мы говорим, что $\vec{a}$ является корнем системы мин-плюс многочленов $F = \{f_1, \ldots, f_k\}$ от переменных $\vec{x}$, если $\vec{a}$ является корнем каждого многочлена $f_i \in F$.

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

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

Степенью мин-плюс уравнения называется максимум степеней f и g. Точка $\vec{a} \in \mathbb{K}^n$ является *решением* мин-плюс уравнения (f, g), если выполняется равенство $f(\vec{a}) = g(\vec{a})$. Аналогично мин-плюс уравнениям мы также можем рассматривать мин-плюс неравенства.

Линейные многочлены и уравнения. Важный частный случай мин-плюс многочленов и мин-плюс уравнений — линейные мин-плюс многочлены и линейные мин-плюс уравнения, которые являются просто многочленами и уравнениями степени 1. Если в многочлене (или уравнении) нет монома степени 0 (то есть, свободного члена), то мы говорим, что этот многочлен (или уравнение) *однородно*.

Удобно записывать однородные линейные многочлены f в форме

$$\min_{1 \leqslant j \leqslant n} \{a_j + x_j\}.$$

В частности, если некоторая переменная x_j не встречается в многочлене, для удобства обозначений мы все равно можем использовать то же обозначение и просто положить соответствующий коэффициент a_j равным ∞ (даже если мы работаем над полукольцом без ∞).

Мин-плюс однородной линейной системе

$$\min_{1 \leqslant j \leqslant n} \{a_{ij} + x_j\},\ 1 \leqslant i \leqslant m, \tag{1.5}$$

тогда можно естественным образом сопоставить ее матрицу A. Мы также будем использовать обозначение $A \odot \vec{x}$ для таких систем. Заметим, однако, что мы будем предполагать, что в матрице A нет строк и столбцов, состоящих только из элементов ∞. Такую строку всегда можно удалить, поскольку всякий вектор является ее корнем. Также можно удалить и бесконечный столбец, поскольку он не влияет на разрешимость системы.

Заметим также, что часто для полукольца без бесконечности системы $A \odot \vec{x}$ рассматриваются тоже с матрицами A без использования бесконечности. На-

пример, такой подход стандартен при исследовании свойств линейных систем как таковых.

Аналогично мин-плюс однородной системе линейных уравнений

$$\left(\min_{1 \leqslant j \leqslant n} \{a_{ij} + x_j\},\ \min_{1 \leqslant j \leqslant n} \{b_{ij} + x_j\} \right),\ 1 \leqslant i \leqslant m,$$

можно сопоставить пару матриц A и B, соответствующих левой и правой части уравнения. Мы также будем записывать такие системы в форме $A \odot \vec{x} = B \odot \vec{x}$. Аналогично мы можем рассматривать системы линейных неравенств $A \odot \vec{x} \leqslant B \odot \vec{x}$.

Есть еще одно важное соглашение для полуколец с бесконечностью. Для удобства обозначений будем считать, что $\mathbb{K} = \mathbb{R}_\infty$. Для других полуколец с бесконечностью мы используем аналогичное соглашение. Для матриц $A, B \in \mathbb{R}_\infty^{m \times n}$ мы говорим, что система $A \odot \vec{x} < B \odot \vec{x}$ имеет решение, если существует $\vec{x} \in \mathbb{R}_\infty^n$, такой что для всякой строки системы либо одна из сторон конечна, и тогда должно выполняться строгое равенство, либо обе стороны равенства равны бесконечности (неформально, мы считаем, что $\infty < \infty$). Это соглашение будет удобно для результатов о линейной двойственности.

Чаще всего мы будем рассматривать именно однородные линейные системы, так что мы будем опускать слово «однородный», считая, что система однородна по умолчанию.

Мы будем рассматривать множества корней мин-плюс систем многочленов и множества решений мин-плюс систем уравнения. Нетрудно видеть (см., напр., [113]), что эти множества являются объединением нескольких (возможно неограниченных) многогранников, возможно различной размерности (в случае $\mathbb{Z}$ корни — целые точки объединения многогранников). *Размерностью* множества решений мы будем называть максимальную размерность его многогранников.

Рассмотрим произвольную мин-плюс линейную систему многочленов. Заметим, что множество ее решений S замкнуто относительно мин-плюс умножения

на число, или, другими словами, $S = S + \mathbb{R}\vec{1}$, где $\vec{1}$ — вектор из единиц. Таким образом, мы можем рассматривать множество решений как множество в мин-плюс проективном пространстве $\mathbb{TP}^{n-1} = \mathbb{K}^n/\langle\vec{1}\rangle_{\mathbb{R}}$. Мы будем рассматривать это множество как в пространстве $\mathbb{R}^n$, так и в пространстве $\mathbb{TR}^{n-1}$, в зависимости от контекста. Каждый раз мы будем уточнять, в каком пространстве рассматривается множество решений. Ясно, что размерность множества решений в проективном пространстве всегда на 1 меньше, чем размерность в $\mathbb{R}^n$.

Рассмотрим матрицу $A \in \mathbb{K}^{m\times n}$. Заметим, что прибавление некоторого числа ко всем ячейкам некоторой строки A не меняет множества решений системы (1.5). Таким образом, в наших рассуждениях мы будем свободно добавлять и вычитать числа из строк матриц. То же самое можно сказать и об умножении строки матрицы на положительное число.

Все эти наблюдения переносятся также и на системы линейных мин-плюс уравнений.

Для матрицы $A \in \mathbb{K}^{m\times n}$ и вектора $\vec{x} \in \{K\}^n$ удобно определить матрицу $A_{\vec{x}} \in \mathbb{K}^{m\times n}$, у которой в ячейке (i, j) записано $a_{ij} + x_j$.

Рассмотрим мин-плюс линейную систему многочленов с матрицей $A \in \mathbb{K}^{m\times n}$, предположим, что $a_{ij} \geqslant 0$ для всех $i \in [m],\ j \in [n]$, для которых a_{ij} конечно (мы можем привести всякую матрицу к такой форме, прибавив векторы $c \cdot \vec{1}$ к строкам). Предположим, что все конечные ячейки матрицы ограничены константой M, то есть $a_{ij} \leqslant M$.

Нетрудно видеть, что верна следующая лемма (см., напр., [60]).

Лемма 1.2 ([60]). *Если описанная система имеет корень $\vec{x} = (x_1, \ldots, x_n)$, то у нее есть также корень $(x'_1, \ldots, x'_n)$, удовлетворяющий неравенствам $0 \leqslant x'_j \leqslant M$ для всех конечных координат $\vec{x}$.*

Иногда мы также будем рассматривать и неоднородные системы

$$\min_{1\leqslant j\leqslant n} \{a_{ij} + x_j\} \cup \{a_i\},\ 1 \leqslant i \leqslant m. \tag{1.6}$$

В таких случаях мы будем явно указывать, что речь идет о неоднородной системе. Такой системе можно естественным образом сопоставить матрицу $A \in \mathbb{K}^{m\times(n+1)}$ и записать ее в матричной форме как $A \odot (\vec{x}, 0)$. Аналогично мы можем рассматривать и неоднородные системы уравнений $A\odot(\vec{x}, 0) = B\odot(\vec{x}, 0)$. Заметим, что над полукольцом без бесконечности система $A \odot (\vec{x}, 0)$ имеет корень тогда и только тогда, когда однородная система $A \odot \vec{x}'$ имеет корень, где $\vec{x}' = (\vec{x}, x_{n+1})$. Действительно, если есть решение $\vec{x}'$ для последней системы, то мы можем прибавить одно и то же число ко всем координатам $\vec{x}'$, чтобы сделать $x_{n+1} = 0$ и получить решение неоднородной системы. То же самое верно и для систем уравнений. Но это не верно для полуколец с бесконечностью: однородная система всегда имеет корень (просто положим $\vec{x} = (\infty, \ldots, \infty)$), но неоднородная система может не иметь корня. Однако, над полукольцом с бесконечностью система $A \odot (\vec{x}, 0)$ имеет корень тогда и только тогда, когда существует корень для $A \odot \vec{x}'$ с $x_{n+1} \neq \infty$.

Глава 2

Веса пороговых функций большой степени

В этой главе мы докажем нижние оценки весов полиномиальных пороговых элементов заданной степени, вычисляющих заданные функции.

2.1 Построение функции

В этом разделе мы построим функцию, для которой докажем более слабый вариант нашей оценки. Эта функция является обобщением функции GT.

Наша функция будет зависеть от $n = 2m$ переменных

$$(x, y) = (x_1, \ldots, x_m, y_1, \ldots, y_m) \in \{0,1\}^n.$$

Зафиксируем некоторые числа $k_1, \ldots, k_d$, такие что $\sum_{i=1}^{d} k_i = m$, и разобъем входные переменные x и y на d групп размеров $k_1, \ldots, k_d$, так что

$$(x, y) = (x^1, x^2, \ldots, x^d, y^1, y^2, \ldots, y^d),$$

где $x^i, y^i \in \{0,1\}^{k_i}$ для всех i.

Напомним, что через $[k]$ мы обозначаем множество $\{1, \ldots, k\}$. Обозначим через $<_1$ следующее самое естественное упорядочивание множества $[k]$: $1, 2, 3, \ldots, k-1, k$, а через $<_0$ — обратное упорядочивание: $k, k-1, k-2, \ldots, 2, 1$. Мы будем использовать эти упорядочивания на множествах $[k_1], \ldots, [k_d]$. Из контекста всегда будет ясно, о каком из множеств идёт речь.

Обозначим через $\mathrm{num}_i l$ порядковый номер $l \in [k]$ относительно порядка $<_i$.

Чтобы определить нашу функцию, нам потребуется задать некоторый порядок на множестве $K = [k_1] \times \ldots \times [k_d]$.

По существу, описанная ниже конструкция будет аналогична конструкции в [135].

Порядок, который мы определяем, будет похож на лексикографический, то есть для сравнения двух наборов из K мы будем сравнивать их компоненты одну за другой до тех пор, пока не встретим первое различие. Но в отличие от лексикографического порядка, где каждая компонента наборов сравнивается относительно одного и того же упорядочивания, в нашем порядке компоненты могут сравниваться относительно разных упорядочиваний. Более того, упорядочивание, в котором сравниваются текущие компоненты, зависит не только от порядкового номера этой компоненты, но и от значений предыдущих компонент в наборах.

Перейдем к формальному определению. Предположим, что мы хотим сравнить наборы $\alpha = (\alpha_1, \ldots, \alpha_d) \in K$ и $\beta = (\beta_1, \ldots, \beta_d) \in K$. Сначала мы сравниваем компоненты α_1 и β_1 относительно порядка $<_1$. Если компоненты оказываются не равны, то сравнение наборов закончено: большим является тот набор, у которого первая компонента больше. Если первые компоненты равны, мы переходим к сравнению вторых компонент. Чтобы выбрать порядок для их сравнения, будем использовать следующее рекурсивное правило.

Предположим, что для сравнения l-х компонент наборов уже определен порядок $<_{i_l}$, и оказалось, что $\alpha_l = \beta_l$. Тогда порядок для сравнения $(l+1)$-х компонент определяется порядковым номером α_l (который, по нашему предположению, совпадает с β_l) относительно порядка $<_{i_l}$.

А именно,

$$i_{l+1} = \mathrm{num}_{i_l} \alpha_l \pmod 2. \tag{2.1}$$

Другими словами, мы сравниваем $(l+1)$-е координаты относительно порядка $<_0$, если α_l имеет четный порядковый номер относительно порядка $<_{i_l}$. В

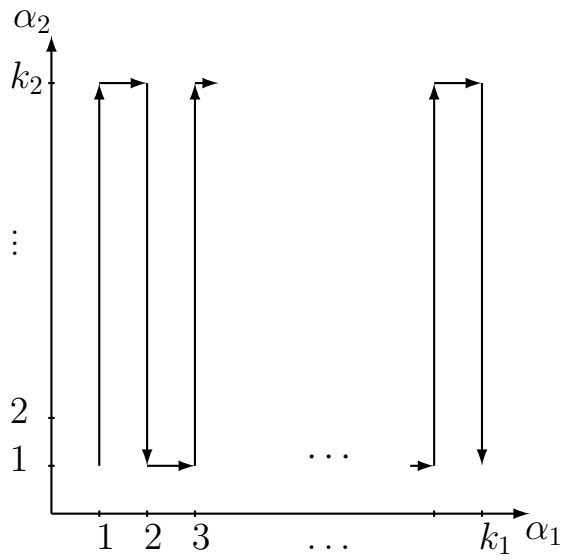


Рисунок 2.1: Порядок в случае $d = 2$.

противном случае сравнение $(l + 1)$-х координат производится относительно порядка $<_1$.

Другими словами, координатам каждого набора $\alpha = (\alpha_1, \ldots, \alpha_d) \in K$ мы сопоставляем порядки $<_{i_1}, \ldots, <_{i_d}$ согласно правилу (2.1). Мы используем эти порядки для сравнения координат набора α с координатами других наборов. Заметим, что для двух наборов $\alpha = (\alpha_1, \ldots, \alpha_d)$ и $\beta = (\beta_1, \ldots, \beta_d)$ порядки, соответствующие их компонентам, совпадают до тех пор, пока не встретится первое различие в координатах. После первой отличной координаты порядки, соответствующие остальным компонентам, могут отличаться для α и β, но дальнейшее сравнение координат нам уже не требуется.

Обозначим через $\mathrm{num}_{\alpha,l}\alpha_l$ порядковый номер l-й компоненты набора α относительно соответствующего порядка.

Несложно описать построенный нами порядок для случая $d = 2$. Изобразим пары (α_1, α_2) точками на плоскости (см. рисунок 2.1).

Первая компонента α_1 соответствует горизонтальной оси, вторая компонента α_2 — вертикальной. Стрелки означают направление от меньших пар к большим.

В случае $d > 2$ построенный порядок описывается уже сложнее. Тем не менее, поскольку доказательство будет вестись индукцией, мы всегда будем рассматривать только две соседние координаты набора. Таким образом, мы будем находиться в ситуации, похожей на случай $d = 2$. Единственное отличие будет в том, что порядок на первой координате может быть не $<_1$.

Теперь мы можем определить нашу функцию.

Определение 2.1. *Пусть для заданной пары* $(x, y) = (x^1, x^2, \ldots, x^d, y^1, y^2, \ldots, y^d)$, *где* $x^i = (x^i_1, \ldots, x^i_{k_i}), y^i = (y^i_1, \ldots, y^i_{k_i}) \in \{0,1\}^{k_i}$, *набор* $\alpha = (\alpha_1, \ldots, \alpha_d) \in K$ *— наибольший набор относительно введенного порядка, такой что* $\prod_{i=1}^{d}(x^i_{\alpha_i} - y^i_{\alpha_i}) \neq 0$.

Тогда положим

$$f(x^1, \ldots, x^d, y^1, \ldots, y^d) = \operatorname{sgn} \prod_{i=1}^{d}(x^i_{\alpha_i} - y^i_{\alpha_i}),$$

где $\operatorname{sgn}(t)$ *равен 1, если* $t \geqslant 0$, *и равен 0 иначе. Если такого набора* α *не существует, то полагаем* $f(x^1, \ldots, x^d, y^1, \ldots, y^d) = 1$.

Заметим, что для $d = 1$ наша функция f — это в точности функция GT.

2.2 Нижняя оценка $2^{\Omega(2^{n/4})}$

Заметим, что определенная нами функция f вычислима пороговым элементом степени d.

Лемма 2.1. $\deg_{\pm}(f) \leqslant d$.

Доказательство. ■

Доказательство. Пусть

$$\alpha^1, \alpha^2, \ldots, \alpha^{|K|},$$

это список всех элементов множества K, записанных по возрастанию во введенном порядке. Для любого $\alpha^j = (\alpha_1^j, \ldots, \alpha_d^j)$ определим t_j как произведение

$$t_j = \prod_{i=1}^{d} (x^i_{\alpha_i^j} - y^i_{\alpha_i^j}).$$

Заметим, что для всякого j и всякого входа (x, y) верно $|t_j| \leqslant 1$.

Рассмотрим многочлен

$$p(x, y) = \sum_{j=1}^{|K|} 2^j t_j.$$

Мы утверждаем, что он представляет нашу функцию своим знаком.

Действительно, зафиксируем некоторый вход (x, y). Если на этом входе все t_j равны нулю, то $f(x, y) = 1$ и $p(x, y) = 0$. В противном случае, пусть набор α^j — максимальный относительно введенного порядка, такой что $t_j \neq 0$. Тогда все t_i для $i > j$ равны нулю, а коэффициенты многочлена p подобраны таким образом, что вклад t_j превышает сумму вкладов всех t_i для $i < j$. Следовательно, знак $p(x, y)$ совпадает со знаком t_j. ■

Перейдем к основному результату этого раздела.

Теорема 2.1. *Пусть $k_i \geqslant 2$ четны при $i < d$, и $k_d \geqslant 3$. Тогда*

$$\deg_{\pm}(f) = d,$$

$$W(f, d) \geqslant 2^{(k_d - 2) \prod_{i=1}^{d-1} k_i \; - d}.$$

Замечание 2.1. *Аналогичную теорему можно сформулировать для произвольных $k_i \geqslant 2$ при $i < d$, а не только для четных. Однако, с этим предположением доказательство и оценка получаются более простыми, и при этом теорема все равно дает оценку $2^{\Omega(2^{n/4})}$.*

Сначала мы выведем некоторые следствия из теоремы 2.1, а затем перейдем к ее доказательству.

Если мы положим $k_i = 2$ для $i < d$ и $k_d = 3$ в теореме 2.1, то мы получим

$$W \geqslant W(f, \frac{n-2}{4}) \geqslant 2^{2^{\frac{n-6}{4}}-d},$$

где W определяется формулой (2) во введении.

В более общем виде, верно следующее.

Следствие 2.2. *Для всех n и всех $d \leqslant \frac{n-2}{4}$ существует (явно заданная) функция f от n переменных, такая что*

$$W(f,d) \geqslant 2^{(2\lfloor\frac{n-2}{4d}\rfloor)^d-(2\lfloor\frac{n-2}{4d}\rfloor)^{d-1}-d}.$$

Доказательство. Положим $k_i = 2\lfloor\frac{n-2}{4d}\rfloor$ для $i < d$ и $k_d = 2\lfloor\frac{n-2}{4d}\rfloor + 1$. Рассмотрим функцию из теоремы 2.1 от первых $2\sum_{i=1}^{d} k_i$ переменных, а остальные переменные оставим несущественными. ■

Аналогично можно доказывать и другие оценки. Например, мы можем доказать следующую оценку с более простой формулировкой:

$$W(f,d) \geqslant 2^{(2\lfloor\frac{n-4}{4d}\rfloor)^d-d}.$$

2.2.1 Доказательство теоремы 2.1

Рассмотрим произвольный пороговый элемент p степени не больше d для функции f. То есть, для всякой пары $x, y \in \{0,1\}^m$ верно

$$f(x,y) = \operatorname{sgn}(p(x,y)).$$

Нам будет удобно работать в переменных

$$u_j^i = x_j^i - y_j^i, \qquad v_j^i = x_j^i + y_j^i. \tag{2.2}$$

Произведем замену переменных

$$x_j^i = (u_j^i + v_j^i)/2, \quad y_j^i = (u_j^i - v_j^i)/2$$

и домножим многочлен на 2^d, чтобы его коэффициенты стали целыми. В результате мы получим многочлен p' от переменных $u_j^i,\ v_j^i$, который представляет функцию f своим знаком, а именно:

$$f(x,y) = \operatorname{sgn}(p'(x-y, x+y)).$$

Нетрудно видеть, что вес нового многочлена почти такой же, как вес многочлена p (по сравнению с величиной нашей оценки). Более точно, мы получаем следующую оценку.

Лемма 2.3. $W(p') \leqslant 2^d W(p)$.

Доказательство. Рассмотрим один из мономов g степени $l \leqslant d$ в многочлене p. Описанное выше преобразование можно рассматривать как замену каждой переменной на сумму (или разность) двух переменных, а затем домножение на 2^{d-l}. После раскрытия скобок мы получим 2^l новых мономов, каждый из которых будет иметь вес 2^{d-l}. Таким образом, общий вес новых мономов, полученных из монома g, будет равен 2^d, домноженному на коэффициент g. Поскольку это происходит со всеми мономами, мы получаем требуемую верхнюю оценку на вес многочлена p'. ■

Замечание 2.2. *Похожее неравенство верно и в обратную сторону, но нам оно не потребуется.*

Теперь нам нужно доказать, что

$$W(p') \geqslant 2^{(k_d-2)\prod_{i=1}^{d-1} k_i}.$$

Сначала мы докажем, что можно предполагать, что p' имеет хорошую структуру. Похожие утверждения ранее встречались в [73,135] (см. более общую версию в [136]).

Лемма 2.4. *Если заменить на* 0 *все коэффициенты мономов многочлена p', в которых не встречаются переменные из хотя бы одной из групп $u^1, \ldots, u^d$, то полученный многочлен q также представляет f своим знаком.*

Доказательство. Пусть I — множество входов (x, y) функции f, таких что $x^i \neq y^i$ для всех $i = 1, \ldots, d$. Это означает, что для каждого входа из I существует набор $\alpha = (\alpha_1, \ldots, \alpha_d) \in K$, такой что

$$\prod_{i=1}^{d} (x^i_{\alpha_i} - y^i_{\alpha_i}) \neq 0.$$

Тогда знак указанного произведения для наибольшего такого α определяет значение функции f.

Рассмотрим произвольный вход (x, y) из множества I и произвольное $i \in [d]$. Переставим переменные x^i и y^i друг с другом. Нетрудно видеть, что после такой перестановки функция f изменит свой знак, а следовательно, и знак многочлена p' должен измениться.

Теперь посмотрим, что происходит с многочленом $p'(u, v)$. Заметим, что после указанной перестановки, все переменные u и v останутся прежними, кроме u^i, которые сменят свой знак. Обозначим через A сумму всех мономов многочлена p', которые содержат четное число переменных из u^i, а через B — сумму всех мономов многочлена p', содержащих нечетное число переменных из u^i. Тогда

$$p'(u, v) = A(u, v) + B(u, v).$$

Заметим, что после указанной перестановки переменных A останется неизменным, а B сменит знак. Поскольку p' меняет знак, мы получаем, что абсолютное значение B больше, чем абсолютное значение A. Мы показали, что это верно для любого входа из I, а значит, для всех таких входов знак функции f определяется знаком суммы B. Следовательно, мы можем удалить все мономы, входящие в A, и получившийся многочлен по-прежнему будет представлять своим знаком функцию f на всех входах из множества I.

Повторяя это рассуждение для всех $i \in [d]$, мы получим пороговый элемент q для функции f, такой что в каждом мономе q содержится нечетное число переменных из каждой из групп $u^1, \ldots, u^d$. При этом степень многочлена q не больше d, так что каждый моном многочлена q содержит ровно одну

переменную из каждой группы $u^1, \ldots, u^d$ (и не содержит переменных из групп $v^1, \ldots, v^d$).

Мы доказали, что новый многочлен q корректно представляет своим знаком функцию f на всех входах из множества I. Далее заметим, что для любого входа из $\{0,1\}^n \setminus I$ существует $i \in [d]$, такое что $x^i = y^i$, или эквивалентно, все переменные в u^i равны нулю. По определению значение функции f на таком входе равно 1, а значение многочлена q равно 0. Значит, многочлен q на данных входах также представляет функцию f своим знаком. ■

В качестве дополнительного следствия из доказательства этой леммы мы получаем следующее.

Следствие 2.5. $\deg_{\pm}(f) = d$.

Поскольку $W(p') \geqslant W(q)$, достаточно доказать, что

$$W(q) \geqslant 2^{(k_d-2)\prod_{i=1}^{d-1} k_i}.$$

Теперь нам потребуется лемма, касающаяся пороговых элементов степени 1 для функции GT. Это рассуждение достаточно стандартно (см. [103, 105]).

Лемма 2.6. *Пусть* $p = \sum_{i=1}^{k} w_i u_i$ *является пороговым элементом степени* 1 *для функции* $\mathrm{GT}(x, y)$, *где* $x, y \in \{0,1\}^k$. *Тогда для* $j \geqslant 2$

$$w_j \geqslant 2^{j-2} w_1 > 0 \tag{2.3}$$

и

$$w_j \geqslant w_{j-1}. \tag{2.4}$$

Доказательство. В действительности мы докажем, что для всякого j $w_j > 0$, и для всякого $j \geqslant 2$

$$w_j \geqslant \sum_{i=1}^{j-1} w_i. \tag{2.5}$$

Отсюда немедленно будет следовать неравенство (2.4), а неравенство (2.3) легко доказать по индукции.

Чтобы доказать неравенство (2.5), рассмотрим следующий вход:

$$u = (\overbrace{-1, \ldots, -1}^{j-1}, 1, 0 \ldots, 0).$$

Нетрудно видеть, что на этом входе функция GT равна 1. Это означает, что $p(u) \geqslant 0$. Отсюда легко следует неравенство (2.5).

Для того, чтобы доказать, что $w_j > 0$, просто положим $u_j = -1$ и $u_i = 0$ для $i \neq j$. На таком входе функция GT принимает значение 0. Значит, $p(u) < 0$. ■

Нам будет удобно рассматривать два варианта функции GT: обозначим через GT_1 обычную функцию GT, а через GT_0 — аналогичную функцию, но на входе, в котором переменные записаны в обратном порядке. То есть $\mathrm{GT}_0(x, y) = 1$ тогда и только тогда, когда $x \geqslant y$, где $x = (x_1, \ldots, x_k), y = (y_1, \ldots, y_k)$ являются двоичными записями целых чисел, в которых x_1, y_1 являются старшими разрядами. Нетрудно видеть, что если

$$p = \sum_{i=1}^{k} w_i u_i$$

является пороговым элементом для функции GT_0, то выполнены неравенства

$$w_{j-1} \geqslant w_j$$

и

$$w_{n-j+1} \geqslant 2^{j-2} w_n > 0,$$

где $j = 2, \ldots n$.

Теперь мы можем перейти к доказательству основной леммы.

Лемма 2.7. *Для всех $l \leqslant d$, если $\alpha \in K$ такое, что $\mathrm{num}_{\alpha,i}\alpha_i = 1$ для любого $i \geqslant l$ и $\beta = (\alpha_1, \ldots, k_l - \alpha_l + 1, \ldots, \alpha_d)$, то*

$$w_\beta \geqslant w_\alpha 2^{(k_d - 2)\prod_{i=l}^{d-1} k_i}.$$

Идея доказательства заключается в следующем. Зафиксируем переменные во всех группах $u^1, \ldots, u^d$, кроме одной. Тогда по сути функция f превратится в функцию GT, и мы сможем воспользоваться леммой 2.6. Повторяя этот прием, мы можем накопить большой коэффициент благодаря особенностями конструкции нашего порядка. Более подробно, доказательство происходит индукцией по убывающему l. Для базы индукции $l = d$ мы фиксируем все переменные, кроме u^d, и, применяя неравенство (2.3), сразу получаем требуемый результат. Для шага индукции мы сначала применяем предположение индукции для $l + 1$, а затем применяем неравенство (2.4) для l-й координаты. Затем мы вновь применяем предположение индукции для $l+1$ и так далее. Таким образом мы можем применить предположение индукции k_l раз и получить требуемый результат. Перейдем к подробному изложению доказательства.

Доказательство. Доказательство проходит индукцией по убывающему l.

База индукции $l = d$. Зафиксируем все переменные u^i, кроме u^d, следующим образом: для всякого i положим $u^i_{\alpha_i} = 1$ и $u^i_j = 0$ для любого $j \neq \alpha_i$.

Мы получили функцию от переменных u^d, и нетрудно видеть, что эта функция совпадает либо с функцией GT_0, либо с функцией GT_1. Применяя неравенство (2.3) (или соответствующее неравенство для GT_0) для $j = k_d$, получаем

$$w_\beta \geqslant 2^{k_d - 2} w_\alpha.$$

Шаг индукции. Для доказательства леммы для $l < d$ повторим несколько раз следующую процедуру, состоящую из двух шагов. После i-го применения процедуры мы получим набор α^i, такой что $\mathrm{num}_{\alpha^i, l} \alpha^i_l = i + 1$ и $\mathrm{num}_{\alpha^i, j} \alpha^i_j = 1$ для всех $j > l$. Для единообразия обозначений положим $\alpha^0 = \alpha$.

Во время процедуры мы не будем менять значения первых $l - 1$ координат. Это означает, что для всех рассматриваемых наборов порядок, соответствующий l-й координате, будет одним и тем же. Без ограничения общности будем считать, что это порядок $<_1$. В частности, это означает, что $\alpha_l = 1$.

Также мы не будем менять координаты $\alpha_{l+2}, \ldots, \alpha_d$. Заметим, что это означает, что если $\mathrm{num}_{\alpha^i, l+1}\alpha^i_{l+1}$ является нечетным (как в начале), то все величины

$$\mathrm{num}_{\alpha^i, l+2}\alpha^i_{l+2}, \ldots, \mathrm{num}_{\alpha^i, d}\alpha^i_d$$

равны 1.

Шаг 1. Применим предположение индукции к координате $l+1$. Получаем, что для набора $\widetilde{\alpha}^{i+1} = (\alpha_1, \ldots, \alpha^i_l, k_{l+1} - \alpha^i_{l+1} + 1, \ldots, \alpha_d)$ выполнено

$$w_{\widetilde{\alpha}^{i+1}} \geqslant w_{\alpha^i} 2^{(k_d - 2)\prod_{i=l+1}^{d-1} k_i}.$$

Заметим, что теперь порядковый номер $(l+1)$-й координаты (относительно соответствующего порядка) равен k_{l+1}.

Шаг 2. Зафиксируем все переменные u^j, кроме u^l, следующим образом: для всякого j пусть $u^j_{\widetilde{\alpha}^{i+1}_j} = 1$ и $u^j_m = 0$ для любого $m \neq \widetilde{\alpha}^{i+1}_j$. Мы получаем функцию от переменных u^l. Нетрудно видеть, что эта функция совпадает с функцией GT_1 (это так, поскольку мы договорились, что порядок, соответствующий l-й компоненте — это порядок $<_1$; если бы это был порядок $<_0$, то функция совпадала бы с функцией GT_0). Применим неравенство (2.4) к координате l. В результате получим

$$\alpha^{i+1} = (\alpha_1, \ldots, \alpha_l + i + 1, k_{l+1} - \alpha^i_{l+1} + 1, \ldots, \alpha_d),$$

такое что

$$w_{\alpha^{i+1}} \geqslant w_{\widetilde{\alpha}^{i+1}}.$$

Согласно правилу (2.1), определяющему порядок на следующей компоненте набора, мы получаем, что на $(l+1)$-й координате порядок изменился. Это означает, что порядковый номер $(l+1)$-й координаты относительно соответствующего порядка, снова равен 1. Отсюда следует, как мы и писали выше, что для всех $j \geqslant l+1$ выполнено $\mathrm{num}_{\alpha^{i+1}, j}\alpha^{i+1}_j = 1$. И мы вновь оказываемся в ситуации, когда можно применить шаг 1.

Мы повторяем эти два шага до тех пор, пока l-я координата набора $\widetilde{\alpha}^i$ не достигнет значения k_l (в конце мы повторяем шаг 1, а шаг 2 повторить уже не сможем, поскольку l-я координата уже будет равна k_l, и не может быть увеличена, так что в конце мы получим $\widetilde{\alpha}^i$ для подходящего i). Поскольку l-я координата на каждой итерации увеличивается на 1 (на шаге 2), мы сможем повторить шаг 2 ровно $k_l - 1$ раз, а шаг 1 мы повторим k_l раз. Таким образом, в результате мы получим вектор $\widetilde{\alpha}^{k_l}$, и нетрудно увидеть, что

$$w_{\widetilde{\alpha}^{k_l}} \geqslant w_\alpha \prod_{j=1}^{k_l} 2^{(k_d-2)\prod_{i=l+1}^{d-1} k_i} = w_\alpha 2^{(k_d-2)\prod_{i=l}^{d-1} k_i}.$$

Проверим, что $\beta = \widetilde{\alpha}^{k_l}$. Легко заметить, что во время выполнения нашей процедуры в наборе α менялись только координаты l и $l+1$. В конце процедуры номер l-й координаты стал равен k_l относительно порядка, соответствующего l-й координате набора α. Это означает, что $\widetilde{\alpha}_l^{k_l} = k_l - \alpha_l + 1 = \beta_l$. Отметим также, что из этого и из четности k_l следует, что α_l и $\widetilde{\alpha}_l^{k_l}$ задают различные порядки на следующей координате. Посмотрим теперь, что происходит с координатой $l+1$. После выполнения процедуры порядковый номер $\widetilde{\alpha}_{l+1}^{k_l}$ относительно порядка, соответствующего координате $(l+1)$ набора $\widetilde{\alpha}^{k_l}$, равен k_{l+1}. Это означает, что порядковый номер $\widetilde{\alpha}_{l+1}^{k_l}$ относительно другого порядка равен 1. Поскольку порядки, соответствующие $(l+1)$-м координатам наборов α и $\widetilde{\alpha}^{k_l}$ различны, получаем, что $\widetilde{\alpha}_{l+1}^{k_l} = \alpha_{l+1} = \beta_{l+1}$ (напомним, что $\mathrm{num}_{\alpha,l+1}\alpha_{l+1} = 1$). ■

Теперь нетрудно завершить доказательство теоремы 2.1. Применив лемму 2.7 при $l = 1$, мы получаем

$$w_\beta \geqslant w_\alpha 2^{(k_d-2)\prod_{i=1}^{d-1} k_i}.$$

Легко видеть, что $w_\alpha > 0$ (просто подставим $u^1_{\alpha_1} = -1$, $u^i_{\alpha_i} = 1$ для всех $i \neq 1$ и $u^i_j = 0$ для всех i и всех $j \neq \alpha_i$). Отсюда следует, что $w_\alpha \geqslant 1$ и

$$w_\beta \geqslant 2^{(k_d-2)\prod_{i=1}^{d-1} k_i}.$$

2.3 Улучшенная нижняя оценка

В этом разделе мы усилим рассуждение предыдущих разделов и докажем более сильную нижнюю оценку. А именно, мы докажем, что

$$W \geqslant 2^{\Omega(2^{2n/5})}.$$

Мы будем работать с булевыми переменными $\{-1, +1\}$, так что для удобства изменим определение функции sgn на следующее: $\operatorname{sgn}(x) = 1$, если $x \geqslant 0$, в противном случае $\operatorname{sgn}(x) = -1$.

Идея заключается в том, чтобы использовать другую функцию вместо GT в качестве строительного блока в нашей конструкции. Действительно, можно попробовать провести наше доказательство с использованием любой функции $f\colon \{-1,+1\}^n \to \{-1,+1\}$, задаваемой следующим образом: рассмотрим однородные линейные формы $L_1(x), \ldots, L_k(x)$, и для любого $x \in \{-1,+1\}^n$ положим $f(x)$ равной знаку $L_i(x)$, где i — максимальный индекс, такой что $L_i(x)$ ненулевая. Однородность линейных форм здесь требуется для того, чтобы прошло доказательство на основе симметричности из леммы 2.4. Отметим также, что мы можем использовать различные функции на различных координатах, и, вообще говоря, это осмысленно, поскольку последняя координата играет совсем другую роль, нежели остальные. По сути, мы уже использовали различные функции на различных координатах, когда выбирали количество переменных k_i различным для различных i.

Заметим, что функция GT на координатах $1, \ldots, d-1$ оказывается не очень экономичной. Действительно, мы используем $2k$ переменных и получаем только k итераций для одной координаты в доказательстве леммы 2.7 (то есть, k_l применений шага 1 в доказательстве этой леммы). Следовательно, мы можем получить порядка $n/2k$ координат с k итерациями в каждой, что дает оценку порядка $2^{\Omega(k^{n/2k})}$. Если с какой-то другой функцией мы сможем проделать боль-

ше итераций при меньшем числе переменных, то мы сможем улучшить нижнюю оценку.

Мы докажем, что для любого $k \geqslant 3$ существует функция, которая с использованием k переменных позволяет сделать $k-1$ итерацию.

Определение 2.2. *Для набора $x = (x_1, \ldots, x_k) \in \{-1, +1\}^k$ положим функцию $g(x_1, \ldots, x_k)$ равной $-x_k$, если не все разряды $x_1, \ldots, x_k$ совпадают, а в противном случае положим равной x_k.*

Эту функцию легко представить в виде линейного порогового элемента:

$$g(x_1, \ldots, x_k) = \operatorname{sgn}(\sum_{i=1}^{k-1} x_i - (k-2)x_k).$$

Однако, для того, чтобы функцию g можно было использовать в качестве строительного блока в нашей комбинаторной конструкции, нам нужно выразить её в терминах линейных форм $L_1(x), \ldots, L_k(x)$ (иначе мы не можем ввести порядок). Рассмотрим k линейных форм $L_i(x) = x_i - x_{i+1}$ (L_i будут играть роль u^i из предыдущего доказательства) для $i = 1, \ldots, k-1$ и $L_0(x) = x_1 + x_k$. Другое (эквивалетное) определение функции g таково: $g(x)$ равна знаку последней ненулевой формы в последовательности $L_0(x), L_1(x), L_2(x), \ldots, L_{k-1}(x)$. Заметим, что теперь удобнее начинать нумерацию L_i с нуля. Это связано с тем, что полезными для нас будут только линейные формы $L_1, \ldots, L_{k-1}$. Форма L_0 нужна только по техническим причинам (такую же роль ранее играли переменные v^i).

Заметим, что в доказательстве более слабой оценки нам требовались не одна, а две базовые функции, которые, впрочем, были достаточно похожи — это функции GT_0 и GT_1. В случае более сильной оценки две функции будут различаться более существенно. В качестве функции g_1 мы возьмем функцию g, определенную выше. Что касается функции g_0, положим $g_0(x)$ равной x_1, если не все биты входа совпадают, и $g_0(x) = -x_1$, если все биты входа одинаковы. Таким образом, теперь мы не только меняем порядок переменных на обратный, но и умножаем

значение функции на -1. Заметим, что значение $g_0(x)$ равно знаку последней ненулевой формы в последовательности $-L_0(x), L_{k-1}(x), L_{k-2}(x), \ldots, L_1(x)$.

Теперь мы можем применить схему из предыдущего доказательства, используя функции g_1 и g_0 на первых $d-1$ компонентах и функцию GT на последней компоненте. Вновь обозначим новую функцию через f. Ниже мы указываем, что изменяется в доказательстве.

Построение упорядочивания для новой функции происходит таким же образом, как раньше, за исключением того, что мы используем другие упорядочивания $<_0^{'}$ и $<_1^{'}$ для первых $d-1$ координат. А именно, мы полагаем $<_1'$ равным $0, 1, 2, \ldots, k-2, k-1$ и $<_0'$ равным $0, k-1, k-2, \ldots, 2, 1$. Таким образом, 0 всегда является наименьшим элементом. Упорядочивания на последних координатах остаются такими же, как были в доказательстве выше (также как и правило (2.1), которое определяет порядок каждой последующеей координаты).

В определении 2.1 теперь остаются только переменные $x^1, x^2, \ldots, x^d, y^d$, и мы полагаем

$$f(x) = \operatorname{sgn}((-1)^{c_1+\ldots+c_{d-1}} L_{\alpha_1}(x^1) L_{\alpha_2}(x^2) \ldots L_{\alpha_{d-1}}(x^{d-1})(x^d_{\alpha_d} - y^d_{\alpha_d}))$$

для наибольшего α, для которого это выражение отлично от нуля, где $c_i = 1$, если $\alpha_i = 0$ и порядок, соответствующий координате i набора α равен $<_0'$, и $c_i = 0$ в противном случае. Если такого α не существует (что может случиться только если $x^d = y^d$), мы полагаем $f(x)$ равной 1. Заметим, что количество переменных $n = \sum_{i=1}^{d-1} k_i + 2k_d$ оказывается почти в два раза меньше, чем в прошлом рассуждении.

Мы докажем следующую теорему.

Теорема 2.2. *Пусть $k_i \geqslant 3$ нечетны при $i < d$, и $k_d \geqslant 3$. Тогда*

$$\deg_{\pm}(f) = d,$$

$$W(f, d) \geqslant 2^{(k_d-2)\prod_{i=1}^{d-1}(k_i-1) - d\log n}.$$

Доказательство теоремы следует прошлому доказательству с незначительными изменениями. Для полноты изложения мы приведем его полностью.

Рассмотрим произвольный пороговый элемент p степени не больше d для функции f. То есть, для любого $x^1, \ldots, x^{d-1}, x^d, y^d$ верно

$$f(x^1, \ldots, x^{d-1}, x^d, y^d) = \operatorname{sgn}(p(x^1, \ldots, x^{d-1}, x^d, y^d)).$$

Нам будет удобнее работать в терминах переменных

$$u_j^i = L_j(x^i)$$

для $i = 1, \ldots, d-1$ и

$$u_j^d = x_j^d - y_j^d, \qquad v_j^d = x_j^d + y_j^d.$$

После подстановки переменных

$$x_j^i = (u_0^i - u_1^i - \ldots - u_{j-1}^i + u_j^i + \ldots + u_{k-1}^i)/2$$

для $i = 1, \ldots, d-1$ и

$$x_j^d = (u_j^d + v_j^d)/2, \quad y_j^d = (u_j^d - v_j^d)/2$$

и умножения многочлена на 2^d, чтобы коэффициенты стали целыми, мы получим многочлен p' от переменных $u_j^i,\ v_j^d$, который представляет функцию f своим знаком. То есть,

$$f(x^1, \ldots, x^{d-1}, x^d, y^d) = \operatorname{sgn}(p'(u^1, \ldots, u^{d-1}, u^d, v^d)).$$

Нетрудно видеть, что вес нового многочлена почти такой же, как вес многочлена p (в сравнении с величиной нашей оценки). А именно, верна следующая оценка.

Лемма 2.8. $W(p') \leqslant n^d W(p)$.

Доказательство. Рассмотрим отдельно моном g степени $l \leqslant d$ многочлена p. Описанное выше преобразование можно рассматривать как замену каждой переменной на суммы не больше, чем $\max_i k_i \leqslant n$, переменных, а затем домножение на 2^{d-l}. После раскрытия скобок мы получим не больше, чем n^l новых мономов, вес каждого из которых 2^{d-l}. Таким образом, общий вес новых мономов, полученных из монома g, не больше, чем n^d, умноженное на коэффициент монома g. Поскольку эту происходит во всеми мономами, мы получаем требуемую верхнюю оценку на вес многочлена p'. ■

Далее докажем, что мы можем предполагать, что p' имеет хорошую структуру.

Лемма 2.9. *Если заменить на* 0 *все коэффициенты мономов многочлена* p'*, в которых не встречаются переменные из групп* $u^1, \ldots, u^d$*, то полученный многочлен* q *также представляет функцию* f *своим знаком.*

Доказательство. Пусть I — множество входов (x, y) функции f, таких что $x^d \neq y^d$. Из этого условия следует, что для каждого такого набора существует $\alpha = (\alpha_1, \ldots, \alpha_d) \in K = [k_1 - 1]_0 \times \ldots \times [k_{d-1} - 1]_0 \times [k_d]$, такое что

$$u^1_{\alpha_1} u^2_{\alpha_2} \ldots u^{d-1}_{\alpha_{d-1}} (x^d_{\alpha_d} - y^d_{\alpha_d}) \neq 0,$$

где через $[k]_0$ мы обозначаем множество $\{0, \ldots k\}$. То есть, значение функции определяется знаком этого произведения для наибольшего из таких наборов α.

Рассмотрим произвольный вход (x, y) из множества I. Сначала переставим переменные x^d и y^d друг с другом. Нетрудно видеть, что после такой перестановки функция f изменит знак, а значит, знак многочлена p' тоже должен измениться.

Теперь посмотрим, что происходит с многочленом $p'(u^1, \ldots, u^d, v^d)$. Заметим, что после указанной перестановки все переменные u и v^d останутся прежними, кроме u^d, которые сменят знак. Обозначим через A сумму мономов многочлена p', которые содержат четное число переменных из u^d, а через B — сумму

всех мономов многочлена p', которые содержат нечетное число переменных из u^d. Тогда

$$p'(u, v^d) = A(u, v^d) + B(u, v^d).$$

Заметим, что после указанной перестановки переменных A останется неизменным, а B сменит знак. Поскольку p' сменит знак, мы получаем, что абсолютное значение B больше, чем абсолютное значение A. Мы доказали, что это верно для любого входа из множества I, а значит, для всех таких входов знак функции f определяется знаком суммы B. Следовательно, мы можем удалить все мономы, входящие в A, и получившийся многочлен по-прежнему будет представлять своим знаком функцию f на всех входах из множества I.

Теперь рассмотрим произвольное $i \in [d-1]$. Заменим вектор x^i на вектор $-x^i$. Как и прежде, нетрудно видеть, что после такой подстановки функция f сменит знак, а следовательно, и знак p' должен смениться.

Посмотрим, что происходит при этом с $p'(u^1, \ldots, u^d, v^d)$. Заметим, что после такой подстановки все переменные u и v^d остаются прежними, кроме u^i, которые меняют знак. Обозначим через A сумму всех мономов многочлена p', которые содержат четное число переменных из u^i, а через B — сумму всех мономов многочлена p', которые содержат нечетное число переменных из u^i. Тогда

$$p'(u, v^d) = A(u, v^d) + B(u, v^d).$$

После указанной подстановки сумма A не изменится, а сумма B сменит знак. Как и прежде, удалим все мономы из A, тогда полученный многочлен будет по-прежнему представлять своим знаком функцию f на всех входах из множества I.

Повторяя рассуждение для всех $i \in [d-1]$, мы получаем пороговый элемент q для функции f, такой что каждый моном q содержит нечетное число переменных из групп $u^1, \ldots, u^d$. Однако, степень многочлена q не больше d, так что это возможно лишь в том случае, когда каждый моном из q содержит ровно одну переменную из каждой из групп $u^1, \ldots, u^d$ (и не содержит переменных из v^d).

Мы доказали, что новый многочлен q корректно представляет своим знаком функцию f на всех входах из множества I. Теперь заметим, что для любого входа из множества $\{-1,1\}^n \setminus I$ верно, что $x^d = y^d$, или эквивалентно, все переменные из u^d нулевые. По определению, значение функции f на таком входе равно 1, а значение q равно 0. Следовательно, q представляет знаком функцию f также и на этих входах. ■

В качестве дополнительного следствия из доказательства этой леммы мы получаем следующее.

Следствие 2.10. $\deg_{\pm}(f) = d$.

Поскольку $W(p') \geqslant W(q)$, достаточно доказать, что

$$W(q) \geqslant 2^{(k_d-2)\prod_{i=1}^{d-1}(k_i-1)}.$$

Теперь докажем аналог леммы 2.6.

Лемма 2.11. *Пусть $p = \sum_{i=0}^{k-1} w_i u_i$ является пороговым элементом степени 1 для функции $g_1(x)$, где $x \in \{-1,+1\}^k$. Тогда для $j = 0,1,\ldots,k-1$ $w_j > 0$, и для $j = 2,\ldots,k-1$ $w_j > w_{j-1}$.*

Для функции g_0 верны аналогичные утверждения.

Лемма 2.12. *Пусть $p = \sum_{i=0}^{k-1} w_i u_i$ является пороговым элементом степени 1 для функции $g_0(x)$, где $x \in \{-1,+1\}^k$. Тогда $w_0 < 0$, для $j = 1,\ldots,k-1$ верно $w_j > 0$, и для $j = 2,\ldots,k-1$ верно $w_{j-1} > w_j$.*

Доказательство леммы 2.11. Чтобы доказать первую часть леммы, для $j \neq 0$ положим $x_1 = \ldots = x_j = -1$ и $x_{j+1} = \ldots = x_k = 1$. Тогда $g_1(x) = -1$, а следовательно, $p(x) = -2w_j < 0$.

Для $j = 0$ положим $x_1 = \ldots = x_k = -1$. Тогда снова получаем, что $g_1(x) = -1$ и $p(x) = -2w_0 < 0$.

Для доказательства второй части леммы положим $x_j = -1$ и $x_l = 1$ для $l \neq j$. Тогда получим, что $g_1(x) = -1$ и $p(x) = 2(w_{j-1} - w_j + w_0) < 0$. А следовательно, $w_j > w_{j-1} + w_0 > w_{j-1}$. ■

Доказательство леммы 2.12. Для $j \neq 0$, полагая $x_1 = \ldots = x_j = -1$, $x_{j+1} = \ldots = x_k = 1$, получаем, что $-w_j < 0$. Полагая $x_1 = \ldots = x_k = 1$, получаем $w_0 < 0$ (заметим, что у нас есть $-L_0$ в последовательности, определяющей g_0). Для $j = 2, \ldots, k-1$, полагая $x_j = 1$ и $x_l = -1$ для $l \neq j$, получаем $-w_{j-1} + w_j - w_0 < 0$, и следовательно, $w_{j-1} > w_j$, поскольку w_0 отрицательно. ■

Аналог леммы 2.7 очень похож на предыдущее утверждение, но формулируется более громоздко, поскольку приходится отдельно выделять случаи $l = d$ и $l < d$.

Лемма 2.13. *Для всех $l \leqslant d$, если $\alpha \in K$ такое, что $\mathrm{num}_{\alpha,i}\alpha_i = 1$ для любого $i \geqslant l$, и $\beta = (\alpha_1, \ldots, k_l - \alpha_l + \delta_{l,d}, \ldots, \alpha_d)$, где $\delta_{l,d}$ — символ Кронекера (то есть, $\delta_{ij} = 1$, если $i = j$, и $\delta_{ij} = 0$ иначе), тогда*

$$w_\beta \geqslant w_\alpha 2^{(k_d-2)\prod_{i=l}^{d-1}(k_i-1)}.$$

В доказательстве леммы база индукции остается ровно такой же, что и в прошлой оценке (заметим, что само утверждение тоже не меняется). Что касается шага индукции, то он остается таким же, за исключением того, что в данном случае мы можем применить предположение индукции $k_l - 1$ раз, вместо k_l раз, как это было в предыдущем доказательстве. Для полноты изложения мы приведем доказательство целиком.

Доказательство. В начале доказательство почти повторяет доказательство леммы 2.7.

Доказательство проходит индукцией по убывающему l.

База индукции $l = d$. Зафиксируем все переменные u^i, кроме u^d, следующим образом: для всякого i положим $u^i_{\alpha_i} = 1$ и $u^i_j = 0$ для любого $j \neq \alpha_i$ (как это сделать, см. в доказательстве леммы 2.11).

Мы получили функцию от переменных u^d. Нетрудно видеть, что эта функция совпадает либо с функцией GT_0, либо с функцией GT_1. Применяя неравенство (2.3) (или соответствующее неравенство для GT_0) для $j = k_d$, получим

$$w_\beta \geqslant 2^{k_d-2} w_\alpha.$$

Шаг индукции. Для доказательства леммы в случае $l < d$, повторим несколько раз процедуру, состоящую из двух шагов. После i-й итерации этой процедуры мы получим набор α^i, такой что $\mathrm{num}_{\alpha^i,l}\alpha^i_l = i + 1$ и $\mathrm{num}_{\alpha^i,j}\alpha^i_j = 1$ для любого $j > l$. Для единообразия обозначений положим $\alpha^0 = \alpha$.

Во время процедуры мы не будем менять значения первых $l - 1$ координат. Это означает, что для всех рассматриваемых наборов порядок, соответствующий l-й координате, будет одним и тем же. Без ограничения общности будем считать, что это порядок $<'_1$. В частности, это означает, что $\alpha_l = 1$.

Также мы не будем менять координаты $\alpha_{l+2}, \ldots, \alpha_d$. Заметим, что это означает, что если $\mathrm{num}_{\alpha^i,l+1}\alpha^i_{l+1}$ является нечетным (как в начале), то все величины

$$\mathrm{num}_{\alpha^i,l+2}\alpha^i_{l+2}, \ldots, \mathrm{num}_{\alpha^i,d}\alpha^i_d$$

равны 1.

Шаг 1. Применим гипотезу индукции к координате $l + 1$. Получаем, что для набора $\widetilde{\alpha}^{i+1} = (\alpha_1, \ldots, \alpha^i_l, k_{l+1} - \alpha^i_{l+1} + \delta_{l+1,d}, \ldots, \alpha_d)$ выполнено

$$w_{\widetilde{\alpha}^{i+1}} \geqslant w_{\alpha^i} 2^{(k_d-2)\prod_{i=l+1}^{d-1}(k_i-1)}.$$

Заметим, что теперь порядковый номер $(l + 1)$-й координаты (относительно соответствующего порядка) равен $k_{l+1} - 1 + \delta_{l+1,d}$.

Шаг 2. Зафиксируем все переменные u^j, кроме u^l, следующим образом: для всякого j положим $u^j_{\widetilde{\alpha}^{i+1}_j} = 1$ и $u^j_m = 0$ для любого $m \neq \widetilde{\alpha}^{i+1}_j$. Мы получаем функцию от переменных u^l. Нетрудно видеть, что эта функция совпадает с

функцией g_1 (это так, поскольку мы условились, что порядок, соответствующий l-й компоненте, — это порядок $<'_1$; если бы это был порядок $<'_0$, то функция совпадала бы с функцией g_0). Применим неравенство из леммы 2.11 к координате l. В результате получим $\alpha^{i+1} = (\alpha_1, \ldots, \alpha_l + i + 1, k_{l+1} - \alpha^i_{l+1} + \delta_{l+1,d}, \ldots, \alpha_d)$, такое что

$$w_{\alpha^{i+1}} \geqslant w_{\widetilde{\alpha}^{i+1}}.$$

Согласно правилу (2.1), определяющему порядок на следующей компоненте набора, мы получаем, что на $(l+1)$-й координате порядок изменился. Это означает, что порядковый номер $(l+1)$-й координаты относительно соответствующего порядка, снова равен 1. Отсюда следует, как мы писали выше, что для всех $j \geqslant l+1$ выполнено $\mathrm{num}_{\alpha^{i+1},j}\alpha^{i+1}_j = 1$. И мы вновь оказываемся в ситуации, когда применим шаг 1.

Мы повторяем эти два шага до тех пор, пока l-я координата набора $\widetilde{\alpha}^i$ не достигнет величины $k_l - 1$ (в конце мы повторяем шаг 1, а шаг 2 уже повторить не сможем, поскольку l-я координата уже будет равна $k_l - 1$, и не может быть увеличена, так что в конце мы получим $\widetilde{\alpha}^i$ для подходящего i). Поскольку l-я координата на каждой итерации увеличивается на 1 (на шаге 2), мы сможем повторить шаг 2 ровно $(k_l - 2)$ раз, а шаг 1 мы повторим $(k_l - 1)$ раз. Таким образом, в результате мы получим вектор $\widetilde{\alpha}^{k_l-1}$. Нетрудно видеть, что

$$w_{\widetilde{\alpha}^{k_l-1}} \geqslant w_\alpha \prod_{j=1}^{k_l-1} 2^{(k_d-2)\prod_{i=l+1}^{d-1}(k_i-1)} = w_\alpha 2^{(k_d-2)\prod_{i=l}^{d-1}(k_i-1)}.$$

Проверим, что $\beta = \widetilde{\alpha}^{k_l-1}$. Легко заметить, что во время выполнения нашей процедуры в наборе α менялись только координаты l и $l+1$. В конце процедуры номер l-й координаты стал равен $k_l - 1$ относительно порядка, соответствующего l-й координате набора α. Это означает, что $\widetilde{\alpha}^{k_l-1}_l = k_l - \alpha_l = \beta_l$. Отметим также, что из этого и из нечетности k_l следует, что α_l и $\widetilde{\alpha}^{k_l-1}_l$ задают различные порядки на следующей координате. Посмотрим теперь, что происходит с координатой $(l+1)$. После выполнения процедуры порядковый номер $\widetilde{\alpha}^{k_l-1}_{l+1}$ относительно

порядка, соответствующего координате $(l+1)$ набора $\widetilde{\alpha}^{k_l-1}$, равен $k_{l+1}-1+\delta_{l+1,d}$. Это означает, что порядковый номер $\widetilde{\alpha}_{l+1}^{k_l-1}$ относительно другого порядка, равен 1. Поскольку порядки, соответствующие $(l+1)$-м координатам наборов α и $\widetilde{\alpha}^{k_l-1}$ различны, получаем, что $\widetilde{\alpha}_{l+1}^{k_l-1} = \alpha_{l+1} = \beta_{l+1}$ (напомним, что $\mathrm{num}_{\alpha,l+1}\alpha_{l+1} = 1$). ■

Чтобы завершить доказательство нашей нижней оценки, нам нужно подобрать значения k_i так, чтобы максимизировать полученную нижнюю оценку. Легко заметить, что оптимально положить $k_d = 3$, как и раньше, и положить $k_1 = k_2 = \ldots = k_{d-1}$, обозначим их значения через k. Тогда экспонента в нашей оценке получится порядка $(k-1)^{n/k}$. Несложный анализ показывает, что максимум здесь (по целым значениям) достигается, когда $k = 5$. Таким образом, мы получаем нижнюю оценку $2^{2^{2(n-6)/5}-n}$.

Глава 3

Булевы схемы с небольшим числом пороговых элементов

В этой главе мы доказываем экспоненциальную нижнюю оценку на размер схем постоянной глубины, содержащих логарифмическое число пороговых элементов, и вычисляющих функций PARITY.

3.1 Предварительные результаты

Случайные подстановки переменных

В нашем анализе нам потребуется лемма Хостада о переключении [72]. Точнее, нам будет удобно использовать стандартное следствие из нее (см., напр., [67]). Сначала мы введем необходимые обозначения, а затем сформулируем лемму.

Пусть $X = \{x_1, \ldots, x_n\}$ — множество булевых переменных. *Подстановкой переменных* мы называем функцию $\rho\colon X \to \{0, 1, *\}$. Интуитивно, ρ фиксирует часть переменных X равными 0, часть переменных X равными 1, а часть переменных оставляет неизменными. То есть, если на переменных X задана функция $f\colon \{0,1\}^n \to \{0,1\}$, то $f|_\rho$ — это функция от переменных из $\rho^{-1}(*)$, полученная подстановкой вместо переменных из $\rho^{-1}(0)$ нулей, а вместо переменных из $\rho^{-1}(1)$ единиц. Пусть R_n^l обозначает множество всех подстановок на n переменных, оставляющих l переменных незафиксированными.

Лемма 3.1 ([67]). *Пусть C — схема из AC^0 глубины h и размера S. Пусть d — положительное число. Выберем случайную подстановку $\rho \in R_n^{n_h}$ равновероятно, где $n_h = \frac{n}{14(14d)^{h-1}}$. Тогда с вероятностью большей $1 - S2^{-d}$ после применения подстановки ρ все функции, вычисляемые всеми элементами схемы C, можно вычислить разрешающими деревьями глубины d.*

Мы не будем приводить определении разрешающих деревьев, поскольку для нас будет важно лишь то, что всякое разрешающее дерево глубины d может быть вычислено целочисленным многочленом степени не больше d (см. [27]).

Лемма о дискриминаторе

Пусть $f, g\colon \{0,1\}^n \to \{0,1\}$ — булевы функции. Обозначим через

$$Corr(f,g) = \left|\mathrm{Prob}_{x\in\{0,1\}^n}[f(x) = g(x)] - \mathrm{Prob}_{x\in\{0,1\}^n}[f(x) \neq g(x)]\right|$$

корреляцию между f и g. Здесь x берется равновероятно из $\{0,1\}^n$.

Нам потребуется следующая лемма из [66].

Лемма 3.2 ([66]). *Если функция f вычисляется схемой вида $\mathrm{MAJ}_k \circ G$ для некоторого класса подсхем G, то существует $g \in G$, такая что*

$$\left|\mathrm{Prob}_{x\in\{0,1\}^n}[g(x) = 1 \mid f(x) = 1] - \mathrm{Prob}_{x\in\{0,1\}^n}[g(x) = 1 \mid f(x) = 0]\right| \geqslant 1/k \tag{3.1}$$

Мы выведем из этой леммы следствие для функции PARITY.

Следствие 3.3. *Если в предыдущей лемме $f = \mathrm{PARITY}$, то мы получаем*

$$Corr(f,g) \geqslant 1/k.$$

Доказательство. Для краткости обозначим $\mathrm{Prob}[g(x) = a, f(x) = b]$ через $\mathrm{Prob}[a,b]$ и $\mathrm{Prob}[g(x) = a \mid f(x) = b]$ через $\mathrm{Prob}[a|b]$. Заметим, что поскольку

PARITY равна 1 ровно на половине своих входных наборов, то для любых a, b верно, что $\mathrm{Prob}[a, b] = \mathrm{Prob}[a|b]/2$. Тогда мы получаем

$$Corr(f, g) = |\mathrm{Prob}[0,0] + \mathrm{Prob}[1,1] - \mathrm{Prob}[1,0] - \mathrm{Prob}[0,1]| =$$

$$|2\,(\mathrm{Prob}[0,0] + \mathrm{Prob}[1,1]) - 1| = |\mathrm{Prob}[0|0] + \mathrm{Prob}[1|1] - 1| =$$

$$|\mathrm{Prob}[1|1] - \mathrm{Prob}[1|0]| \geqslant 1/k.$$

■

Приближение PARITY

Нам потребуется следующая лемма из [10].

Лемма 3.4 ([10]). *Пусть p — целочисленный многочлен степени d над n переменными и пусть f — его знаковая функция. Тогда*

$$Corr(\mathrm{PARITY}, f) \leqslant \frac{\sum_{k=\frac{1}{2}(n-d-1)}^{\frac{1}{2}(n+d+1)} \binom{n}{k}}{2^n}.$$

Из этого неравенства и из стандартной оценки

$$\binom{n}{k} \leqslant \frac{2^n}{\sqrt{n}}$$

на биномиальные коэффициенты для всех k сразу получается следующая связь между степенью многочлена и корреляцией с PARITY.

Следствие 3.5. *Если для знаковой функции f целочисленного многочлена p степени d над n переменными верно $Corr(\mathrm{PARITY}, f) = 1/C$, то $C(d+2) \geqslant n^{1/2}$.*

3.2 Нижняя оценка

Мы докажем следующую теорему.

Теорема 3.1. *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 $g(t) = (t+1)^2 2^{4t}$.

Таким образом для любых констант $0 < \epsilon' < 4\epsilon$ мы получаем, что схема глубины h с не более чем $\left(\frac{1}{4} - \epsilon\right) \log n$ пороговыми элементами, вычисляющая PARITY, имеет размер $S \geqslant 2^{n^{\epsilon'/(h+1)}}$ для достаточно больших n.

Доказательство. Пусть C — схема с элементами неограниченной входной степени, глубины h и размера S с не более чем t пороговыми элементами, вычисляющая PARITY от n переменных.

Общий план доказательства следующий: из схемы C мы получим многочлен, приближающий PARITY своей знаковой функцией. После этого мы применим неравенство из следствия 3.5, что даст нам требуемую оценку. Доказательство состоит из 4 шагов.

Шаг 1. Сначала мы перестроим схему с помощью стандартных для такого типа задач рассуждения (см. [18,35,55]). После перестройки будет выполняться, что на всяком пути от входов к выходу схемы есть только один элемент из THR.

Для этого обозначим через $C_1, \ldots, C_t$ подсхемы C с пороговыми элементами в вершинах. Для удобства изложения обозначим также C через C_0. Рассмотрим произвольный $\alpha \in \{0,1\}^t$ и для всех $i \in \{1, \ldots, t\}$ подставим во всех схемах $C_0, C_1, \ldots, C_{i-1}, C_{i+1}, \ldots, C_t$ (то есть, в изначальной схеме, а также во всех подсхемах, кроме C_i) константу α_i вместо i-го порогового элемента. Далее, для всех i, таких что $\alpha_i = 0$, возьмем отрицание соответствующей схемы и обозначим получившиеся схемы через $C_0(\alpha), C_1(\alpha), \ldots, C_t(\alpha)$. Каждая из этих

схем содержит не больше одного элемента из THR, расположенного в вершине схемы (заметим, что отрицание элемента из THR снова является элементом в THR).

Теперь нетрудно увидеть, что схема C эквивалентна (то есть, вычисляет ту же функцию) схеме

$$C' = \bigvee_{\alpha \in \{0,1\}^t} \bigwedge_{i=0}^{t} C_i(\alpha).$$

Схема C' содержит не больше $t2^t$ пороговых элементов, и на каждом пути от входов к выходу встречается не больше одного порогового элемента.

Шаг 2. На этом шаге мы применим случайную подстановку переменных в C'.

Для $i = 1, \ldots, t$ обозначим через $\widetilde{C}_i(\alpha)$ схему, получающуюся из $C_i(\alpha)$ удалением последнего элемента (то есть, порогового элемента). Также для единообразия обозначим через $\widetilde{C}_0(\alpha)$ схему $C_0(\alpha)$. Мы применяем лемму 3.1 с параметром $d = \log S + 2t + 1$ ко всем схемам $\widetilde{C}_i(\alpha)$. Тогда мы получаем, что для всякого $\widetilde{C}_i(\alpha)$ вероятность того, что какие-то из ее элементов не вычисляются разрешающим деревом глубины d после подстановки переменных, не превышает $S2^{-d}$. Тогда, оценив вероятность объединения событий через сумму их вероятностей, получаем, что вероятность того, что существует $\widetilde{C}_i(\alpha)$ (для какого-то i и α), такое что одна из его вершин не вычисляется разрешающим деревом глубины d, не превышает

$$(t+1)2^t S 2^{-d} = \frac{(t+1)}{2^{t+1}},$$

что меньше 1. Таким образом, существует подстановка $\rho \in R_n^{n_h}$, такая что все элементы всех $\widetilde{C}_i(\alpha)$ вычислимы разрешающими деревьями глубины d. Поскольку разрешающие деревья глубины d могут быть вычислены целочисленными многочленами степени d, а пороговый элемент от многочлена можно представить как пороговый элемент от элементов AND (заметим, что AND — это в точности перемножение для $\{0, 1\}$ переменных) мы получаем новую схему C''

вида

$$\mathsf{OR}_{2^t} \circ \mathsf{AND}_{t+1} \circ \mathsf{THR} \circ \mathsf{AND}_d,$$

вычисляющую PARITY (или ее отрицание) от n_h переменных.

Заметим, что $\mathrm{OR}_k \in \mathsf{MAJ}_k$, а значит, наша схема имеет вид

$$\mathsf{MAJ}_{2^t} \circ \mathsf{AND}_{t+1} \circ \mathsf{THR} \circ \mathsf{AND}_d.$$

Шаг 3. Теперь мы покажем (вновь, стандартным рассуждением), что

$$\mathsf{MAJ}_{2^t} \circ \mathsf{AND}_{t+1} \subseteq \mathsf{MAJ}_{2^{2t+1}} \circ \mathsf{XOR}_{t+1}. \tag{3.2}$$

Действительно, схема $\mathrm{MAJ}_{2^t} \circ \mathrm{AND}_{t+1}$ вычисляет знаковую функцию многочлена $p(x)$ над переменными $\{0,1\}$ степени не больше $t+1$ и с суммой абсолютных значений всех коэффициентов, кроме свободного члена, не больше 2^t. С другой стороны, если мы представим булевы переменные в виде $\{-1,+1\}$, где -1 соответствует «истине», а 1 соответствует «лжи», то мы получим, что схема $\mathrm{MAJ}_{2^{2t+1}} \circ \mathrm{XOR}_{t+1}$ вычисляет знаковую функцию многочлена $q(x)$ над переменными $\{-1,+1\}$ степени не больше $t+1$ и с суммой абсолютных значений всех коэффициентов, кроме свободного члена, не больше 2^{2t+1} (заметим, что XOR — это в точности умножение для $\{-1,+1\}$ переменных). Так что, начав со схемы вида $\mathrm{MAJ}_{2^t} \circ \mathrm{AND}_{t+1}$, мы можем рассмотреть соответствующий многочлен $p(x)$ и перейти в нем к новым переменным $\widetilde{x}_i = 1 - 2x_i$. Для этого мы подставляем $x_i = (1-\widetilde{x}_i)/2$, раскрываем скобки и умножаем многочлен на 2^{t+1}, чтобы сделать коэффициенты целыми. Легко видеть, аналогично главе 2, что после этой операции мы получаем целочисленный многочлен над переменными $\{-1,+1\}$, степени $t+1$, с суммой абсолютных значений всех своих коэффициентов, кроме свободного коэффициента, не большей 2^{2t+1} и представляющий своим знаком ту же функцию, рассматриваемую над переменными $\{-1,+1\}$. Знаковая функция этого многочлена может быть вычислена схемой из $\mathsf{MAJ}_{2^{2t+1}} \circ \mathsf{XOR}_{t+1}$, что и требовалось.

Шаг 4. Из (3.2) мы получаем, что PARITY от n_h переменных можно вычислить схемой вида

$$\mathsf{MAJ}_{2^{2t+1}} \circ \mathsf{XOR}_{t+1} \circ \mathsf{THR} \circ \mathsf{AND}_d.$$

По следствию 3.3 мы получаем, что PARITY имеет корреляцию не меньше $1/2^{2t+1}$ с некоторой схемой вида

$$\mathsf{XOR}_{t+1} \circ \mathsf{THR} \circ \mathsf{AND}_d.$$

Нетрудно видеть, что эта схема вычисляет знак целочисленного многочлена степени не больше $(t+1)d$. Действительно, схемы $\mathsf{THR} \circ \mathsf{AND}_d$ вычисляют знаки многочленов степени d, а взятие XOR означает перемножение этих многочленов (есть небольшая тонкость в том, что многочлены могут быть равны нулю в некоторых точках, но она легко преодолевается заменой такого многочлена p на многочлен $2p-1$, который всегда не равен нулю, и вместе с тем, имеет такую же знаковую функцию).

Теперь остается только использовать следствие 3.5. Замечая, что $d(t+1)+2 \leqslant (d+2)(t+1)$, мы получаем

$$(d+2)2^{2t+1}(t+1) \geqslant n_h^{1/2} = \frac{n^{1/2}}{\sqrt{14}(14d)^{(h-1)/2}} \geqslant \frac{n^{1/2}}{\sqrt{14}(14(d+2))^{(h-1)/2}}.$$

После простых преобразований и подстановки d мы получаем

$$(\log S + 2t + 3)^{(h+1)/2} 14^{h/2} (t+1) 2^{2t+1} \geqslant n^{1/2}. \tag{3.3}$$

Заметим, что для достаточно больших n для всякого постоянного $\delta > 0$ выполняется неравенство $2t+3 \leqslant \delta \log S$, поскольку иначе первая скобка в (3.3) есть $O(2t+1)$, и все неравенство противоречит тому, что $t \leqslant (\frac{1}{4} - \epsilon)\log n$. Фиксируя подходящее δ, мы получаем, что

$$\log S + 2t + 3 \leqslant \left(\frac{7}{2}\right)^{\frac{1}{h+1}} \log S$$

для достаточно большого n. Таким образом, после простых преобразований в (3.3), мы получаем неравенство

$$\log S \geqslant \frac{n^{\frac{1}{h+1}}}{14(t+1)^{\frac{2}{h+1}} 2^{\frac{4t}{h+1}}},$$

из которого следует результат теоремы. ■

Глава 4

Булевы схемы из точных пороговых элементов

В этой главе мы подробно обсуждаем булевы схемы, состоящие из точных пороговых элементов, и их связь с пороговыми схемами.

4.1 Точные пороговые функции

Для $w = (w_1, \ldots, w_n) \in \mathbb{R}^n$ и $t \in \mathbb{R}$ *точной пороговой функцией* называется функция $\mathrm{ETHR}_{w,t}$, такая что $\mathrm{ETHR}_{w,t}(x) = 1$ тогда и только тогда, когда $\sum_{i=1}^{n} w_i x_i = t$. Числа $w_1, \ldots, w_n$ мы называем *весами*, а t — *порогом*. Соответствующий линейный многочлен мы называем точным пороговым элементом. Как и в случае с пороговыми элементами, мы можем предполагать, что веса и порог — целые числа, по абсолютному значению не превышающие $2^{O(n \log n)}$.

Утверждение 4.1 ([12]). *Для любой точной пороговой функции от n переменных существует соответствующий ей точный пороговый элемент с целыми весами с абсолютным значением не больше $n^{n/2+1}$.*

Далее, если не сказано обратное, мы всегда предполагаем, что коэффициенты в точном пороговом элементе целые.

Как и для пороговых функций, мы будем выделять случай, когда все веса равны 1, а порог равен $\lfloor n/2 \rfloor$. Соответствующую функцию мы обозначаем через $\mathrm{EMAJ}(x)$. Мы также вводим обозначение ETHR для класса всех точных пороговых функций $\mathrm{ETHR}_{w,t}$ для всех w и t. Пусть EMAJ — класс всех функций

вида EMAJ. По аналогии с другими классами функций, мы используем те же обозначения для классов одноэлементных схем. Всюду, где может возникнуть путаница, мы поясняем используемые обозначения.

Нам также потребуется отдельный вид *не всюду определенных* элементов схемы. А именно, обозначим через LIN класс всех линейных комбинаций переменных с коэффициентами, ограниченными полиномом. Эти функции (как булевы функции) определены, только если линейная комбинация принимает значение 0 и 1. Всюду при использовании этих элементов в схемах мы будем подразумевать, что все попадающие на вход этим элементам наборы лежат в их области определения. Частным случаем такого элемента является дизъюнктивное OR, в котором по сравнению с обычным OR предполагается, что среди входов не больше одной единицы.

Для произвольного $d \geqslant 1$ обозначим через ELT_d класс булевых схем глубины d, состоящих из точных пороговых функций. Будем называть схемы такого типа *точными пороговыми схемами*. Через $\widehat{\mathsf{ELT}}_d$ обозначим класс схем глубины d, состоящий из таких точных пороговых функций, что для всех них есть точные пороговые элементы со всеми коэффициентами w_i равными ± 1.

4.1.1 Базовые свойства

Как упоминалось выше, из работ [34] и [106] вытекает, что любая пороговая функция может быть вычислена схемой из TC^0, то есть с использованием элементов только с полиномиальными весами, и как следствие мы получаем, что $\mathsf{TC}^0 = \cup_{i=1}^{\infty} \mathsf{LT}_i$. Этот факт уточнялся в серии работ, в последней из которых [52] было доказано, что любая пороговая функция лежит в $\widehat{\mathsf{LT}}_2$. В этой же работе было доказано следующее более сильное утверждение.

Теорема 4.1 ([52]). *Для всех $i \geqslant 1$ верно $\mathsf{MAJ} \circ \mathsf{LT}_i = \mathsf{MAJ} \circ \widehat{\mathsf{LT}}_i$. В частности, $\mathsf{MAJ} \circ \mathsf{THR} = \mathsf{MAJ} \circ \mathsf{MAJ}$.*

Доказательства этих результатов были упрощены в работах [53, 74, 7].

Дальше мы устанавливаем простую связь между ETHR элементами и THR элементами.

Утверждение 4.2.

1. $\mathsf{ETHR} \subseteq \mathsf{THR} \circ \mathsf{AND}_2$.

2. $\mathsf{EMAJ} \subseteq \mathsf{MAJ} \circ \mathsf{AND}_2$.

Доказательство. Пусть точный пороговый элемент задан равенством $L(x) = 0$, где

$$L(x) = w_1 x_1 + \cdots + w_n x_n - t \ .$$

Тогда легко видеть, что $L(x) = 0$ тогда и только тогда, когда $(L(x))^2 \leqslant 0$. Для всякого монома степени 2 в многочлене $(L(x))^2$ мы можем завести элемент AND от двух переменных. Мы подставляем выходы этих элементов, а также переменные, соответствующие мономам степени 1, в пороговый элемент, используя в качестве весов коэффициенты соответствующих мономов. Если коэффициенты $L(x)$ ограничены полиномом, то и коэффициенты $(L(x))^2$ ограничены полиномом. ■

Утверждение 4.3. *Классы точных пороговых функций удовлетворяют следующим свойствам замкнутости относительно функций* AND*:*

1. $\mathsf{AND}_k \circ \mathsf{EMAJ} = \mathsf{EMAJ}$ *для любого положительного целого* k.

2. $\mathsf{AND} \circ \mathsf{ETHR} = \mathsf{ETHR}$.

3. $\mathsf{AND} \circ \mathsf{EMAJ} \subseteq \mathsf{EMAJ} \circ \mathsf{AND}_2$.

Доказательство. Для доказательства первых двух утверждений рассмотрим AND от k точных пороговых функций. Пусть j-я точная пороговая функция задается линейным уравнением $L_j(x) = 0$. Пусть B — наименьшее целое число, такое что $|L_j(x)| < B$ для всех $x \in \{0,1\}^n$ и всех j. Тогда для всех $x \in \{0,1\}^n$

мы получаем, что $\sum_{j=1}^{k} B^j L_j(x) = 0$ тогда и только тогда, когда $L_j(x) = 0$ для всех j. Нетрудно видеть, что веса этой новой точной пороговой функции ограничены B^{k+1}. В случае, если B полиномиально ограниченно и k — константа, эта величина также ограничена полиномом.

Наконец, для последнего утверждения, предположим, что k точных функций голосования заданы линейными формами $L_1, \ldots, L_k$. Тогда верно, что $L_j(x) = 0$ выполняется для всех j тогда и только тогда, когда выполняется $\sum_{j=1}^{k} (L_j(x))^2 = 0$. Мы можем проверить это равенство схемой вида $\mathsf{EMAJ} \circ \mathsf{AND}_2$, как в доказательстве утверждении 4.2. ■

4.2 Включения между классами

Теорема 4.2. *Всякий элемент* SYM *(вычисляющий симметрическую булеву функцию) представляется в виде дизъюнктивного* OR *от элементов* EMAJ. *Всякий элемент* THR *представляется в виде дизъюнктивного* OR *от элементов* ETHR. *Как следствие, верны равенства*

1. $\mathsf{LIN} \circ \mathsf{MAJ} = \mathsf{LIN} \circ \mathsf{SYM} = \mathsf{LIN} \circ \mathsf{EMAJ}$,

2. $\mathsf{LIN} \circ \mathsf{THR} = \mathsf{LIN} \circ \mathsf{ETHR}$.

Доказательство. В работе [66] по существу доказано, что $\mathsf{LIN} \circ \mathsf{MAJ} = \mathsf{LIN} \circ \mathsf{SYM}$. Для первой части теоремы нам остается доказать, что всякая симметрическая функция f от n переменных является дизъюнктивным OR от элементов EMAJ. Функция f задается множеством $S \subseteq \{0, 1, \ldots, n\}$, где $f(x) = 1$ тогда и только тогда, когда $\sum_{i=1}^{n} x_i \in S$. Так что мы можем переписать это как дизъюнктивное OR от элементов EMAJ, заданных уравнениями $\sum_{i=1}^{n} x_i = t$ для всех $t \in S$.

Включение $\mathsf{ETHR} \subseteq \mathsf{LIN} \circ \mathsf{THR}$ несложно, поскольку $\sum_{i=1}^{n} w_i x_i = t$ эквивалентно разности $(\sum_{i=1}^{n} w_i x_i \geqslant t)$ и $(\sum_{i=1}^{n} w_i x_i \geqslant t + 1)$.

Дальше мы показываем, что всякий элемент THR представляется в виде дизъюнктного OR от элементов ETHR. Доказательство использует идеи из [74, 7]. Рассмотрим пороговую функцию $\sum_{i=1}^{n} w_i x_i + w_0 \geqslant 0$, заданную линейной формой $F(x) = \sum_{i=1}^{n} w_i x_i + w_0$. Пусть L — минимальное целое число, такое что $|w_i| < 2^L$ для всех i. По утверждению 1.1 мы можем предполагать, что $L = O(n \log n)$. Введем следующие обозначения (близкие к [7]) для всех $l \leqslant L$:

$$w_i^{(l)} = \lfloor w_i / 2^l \rfloor,$$
$$F^{(l)}(x) = \sum_{i=1}^{n} w_i^{(l)} x_i + w_0^{(l)},$$
$$E^{(l)}(x) = F^{(l-1)}(x) - 2F^{(l)}(x).$$

Заметим, что $2F^{(l)}(x) \leqslant F^{(l-1)}(x)$, или, что то же самое, $E^{(l)}(x) \geqslant 0$. Также заметим, что $E^{(l)}(x) \leqslant n + 1$. Пусть

$$E_{max} = \max_{l} \max_{x \in \{0,1\}^n} E^{(l)}(x).$$

Мы утверждаем, что $F(x) \geqslant 0$ тогда и только тогда, когда

$$\bigvee_{l=0}^{L} \Big(\Big(F^{(l)}(x) \in [0, E_{max}] \Big) \wedge \Big(F^{(l-1)}(x) \in [E_{max} + 1, 3E_{max}] \Big) \Big), \qquad (4.1)$$

и более того, элемент OR в этой формуле дизъюнктный. Для $l = 0$ в (4.1) подразумевается, что правая часть в конъюнкции истинна. Доказательство этой эквивалентности вытекает из следующего утверждения.

Утверждение.

1. *Если* $F^{(l-1)}(x) > 3E_{max}$, *то* $F^{(l)}(x) > E_{max}$.
2. *Если* $F^{(l-1)}(x) > E_{max}$, *то* $F^{(l)}(x) > 0$.
3. *Если* $F(x) < 0$, *то* $F^{(l)}(x) < 0$ *для всех* l.
4. $F^{(L)}(x) \leqslant 0$.

Первая часть этого утверждения вытекает из следующего вычисления:

$$F^{(l)}(x) = \frac{F^{(l-1)}(x) - E^{(l-1)}(x)}{2} > \frac{3E_{max} - E_{max}}{2} = E_{max} \ .$$

Доказательство второй части утверждения полностью аналогично. Третья часть вытекает из того, что $F(x) \equiv F^{(0)}(x)$ и $2F^{(l)}(x) \leqslant F^{(l-1)}(x)$. Последняя часть утверждения сразу следует из определения $w_i^{(L)}$.

Теперь мы готовы завершить доказательство. Ясно, что мы можем записать $F^{(l)}(x) \in [a, b]$ как дизъюнктное OR от элементов ETHR. Более того, конъюнкция двух таких условий также раскрывается в дизъюнктивное OR от элементов ETHR с помощью утверждения 4.3. Комбинируя все шаги вместе, мы получаем дизъюнктивное OR от элементов ETHR, вычисляющее наш пороговый элемент. ■

Следствие 4.1. *Пусть* $\mathcal{C}$ *— один из классов* LIN, MAJ, THR, EMAJ, ETHR. *Тогда для всех* $i \geqslant 1$ *верно* $\mathcal{C} \circ \widehat{\mathsf{LT}}_i = \mathcal{C} \circ \widehat{\mathsf{ELT}}_i$ *и* $\mathcal{C} \circ \mathsf{LT}_i = \mathcal{C} \circ \mathsf{ELT}_i$.

Доказательство. Для доказательства леммы мы применяем теорему 4.2 последовательно ко всем уровням схемы, используя тот факт, что элемент LIN «содержится» в MAJ, THR, EMAJ и ETHR. ■

Мы можем переформулировать результат теоремы 4.2 в виде следующего комбинаторного утверждения: всякое пересечение булевого куба с полупространством может быть разбито на полиномиальное число непересекающихся множеств, каждое из которых является пересечением булевого куба с гиперплоскостью.

Как мы доказали, в случае полиномиально ограниченных весов эти множества можно выбрать так, чтобы они отвечали параллельным гиперплоскостям. Естественно спросить, верно ли это для произвольных коэффициентов. Мы показываем, что для функции GT требуется экспоненциально много параллельных гиперплоскостей.

Утверждение 4.4. *Пусть* $w_1, \ldots, w_n$ *и* $w'_1, \ldots, w'_n$ *— веса, а* $t_1, \ldots, t_k$ *— пороги, такие что* $\mathrm{GT}(x, y) = 1$ *тогда и только тогда, когда существует* j*, такое что* $\sum_{i=1}^{n} w_i x_i + w'_i y_i = t_j$*. Тогда* $k \geqslant 2^n$*.*

Доказательство. Зафиксируем $x_i = 1$ для всех i. Тогда верно, что $\mathrm{GT}(x, y) = 1$ для всех y. Предположим от противного, что y и y' различны, но (x, y) и (x, y') попадают в одну гиперплоскость, соответствующую t_j. Тогда $\sum_{i=1}^{n} w'_i y_i = \sum_{i=1}^{n} w'_i y'_i$. Пусть, для определенности, $\mathrm{GT}(y, y') = 1$. Тогда мы получаем, что $\mathrm{GT}(y', y') = 1$ и $\mathrm{GT}(y', y) = 0$. Из первого мы получаем, что существует t_l, такое что $\sum_{i=1}^{n} w_i y'_i + w'_i y'_i = t_l$, но тогда мы также получаем $\sum_{i=1}^{n} w_i y'_i + w'_i y_i = t_l$, что означало бы, что $\mathrm{GT}(y', y) = 1$. ■

Теперь перейдем к результатам о связи точных пороговых элементов с ограничениями на веса и без.

Теорема 4.3. *Всякая функция, вычислимая точным пороговым элементом, также вычисляется схемой глубины 2 из точных пороговых элементов с полиномиальными весами, то есть* $\mathsf{ETHR} \subseteq \mathsf{EMAJ} \circ \mathsf{EMAJ}$*.*

Доказательство. Сначала докажем, что $\mathsf{ETHR} \subseteq \mathsf{AND} \circ \mathsf{SYM}$. Для этого воспользуемся стандартной техникой, опирающейся на китайскую теорему об остатках. Рассмотрим точную пороговую функцию, задаваемую уравнением $w_1 x_1 + \cdots + w_n x_n = t$. Зададим линейную форму $E(x) = \sum_{i=1}^{n} w_i x_i - t$. Положим W равным целому числу, такому что $|E(x)| < W$ для всех $x \in \{0, 1\}^n$. По утверждению 4.1 мы можем выбрать $W = 2^{O(n \log n)}$. Пусть $p_1, \ldots, p_k$ — k наименьших простых чисел, таких что $p_1 \cdot \ldots \cdot p_k \geqslant W$. Тогда по теореме о распределении простых чисел $p_k = O(n \log n)$. Чтобы проверить, верно ли $E(x) = 0$, по китайской теореме об остатках мы можем вместо этого проверить, верно ли $E(x) \equiv 0 \pmod{p_j}$ для всех j. Теперь рассмотрим какое-нибудь конкретное значение j. Определим E_j как функцию, получающуюся из E заменой всех коэффициентов их остатками от деления на p_j, то есть, определим

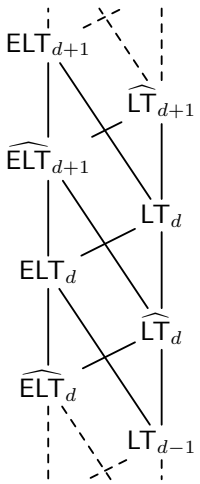


Рисунок 4.1: Произвольные уровни иерархии.

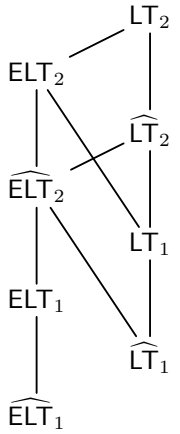


Рисунок 4.2: Первые два уровня иерархии.

$E_j(x) = \sum_{i=1}^{n}(w_i \mod p_j)x_i + (-t \mod p_j)$. Нетрудно видеть, что $E(x) \equiv 0 \pmod{p_j}$ тогда и только тогда, когда $E_j(x) \in \{0, p_j, \ldots, np_j\}$. Последнее можно проверить элементом SYM, который получает на вход $(w_i \mod p_j)$ копий x_i для всех i. Применив функцию AND ко всем этим симметрическим функциям, мы получим схему вида $\mathsf{AND} \circ \mathsf{SYM}$, вычисляющую данную точную пороговую функцию.

Теперь мы можем вывести результат теоремы. Используя теорему 4.2, мы получаем $\mathsf{AND} \circ \mathsf{SYM} \subseteq \mathsf{EMAJ} \circ \mathsf{SYM} = \mathsf{EMAJ} \circ \mathsf{EMAJ}$. ■

Теперь мы готовы показать, что классы точных пороговых схем образуют иерархию, тесно переплетающуюся с иерархией классов пороговых схем, см. рисунки 4.1 и 4.2.

Теорема 4.4. *Для всех $i \geqslant 1$ верно*

1. $\widehat{\mathsf{ELT}}_i \subseteq \mathsf{ELT}_i \subseteq \widehat{\mathsf{ELT}}_{i+1}$ *(это аналог теоремы 4.1 для точных пороговых элементов).*

2. $\widehat{\mathsf{LT}}_i \subseteq \widehat{\mathsf{ELT}}_{i+1} \subseteq \widehat{\mathsf{LT}}_{i+1}$.

3. $\mathsf{LT}_i \subseteq \mathsf{ELT}_{i+1} \subseteq \mathsf{LT}_{i+1}$.

Доказательство. 1. Включение $\widehat{\mathsf{ELT}}_i \subseteq \mathsf{ELT}_i$ очевидно. Заметим, что включение $\mathsf{ELT}_i \subseteq \widehat{\mathsf{ELT}}_{i+1}$ доказано в теореме 4.3 для случая $i = 1$. Для $i > 1$ мы получаем

$$\begin{aligned}\mathsf{ELT}_i \subseteq\ & \mathsf{EMAJ} \circ \mathsf{EMAJ} \circ \mathsf{ELT}_{i-1} \subseteq \\ & \mathsf{EMAJ} \circ \mathsf{MAJ} \circ \mathsf{LT}_{i-1} \subseteq \\ & \mathsf{EMAJ} \circ \mathsf{MAJ} \circ \widehat{\mathsf{LT}}_{i-1} \subseteq \\ & \mathsf{EMAJ} \circ \mathsf{EMAJ} \circ \widehat{\mathsf{ELT}}_{i-1} = \widehat{\mathsf{ELT}}_{i+1}.\end{aligned}$$

В этой цепочке мы применили теорему 4.3, теорему 4.2, теорему 4.1 и следствие 4.1.

2. Во-первых, верно, что $\widehat{\mathsf{LT}}_i \subseteq \mathsf{EMAJ} \circ \widehat{\mathsf{LT}}_i = \widehat{\mathsf{ELT}}_{i+1}$. Для доказательства второго включения мы применяем утверждения 4.2, 4.3 и следствие 4.1:

$$\begin{aligned}\widehat{\mathsf{ELT}}_{i+1} = \mathsf{EMAJ} \circ \widehat{\mathsf{ELT}}_i \subseteq\ & \\ & \mathsf{MAJ} \circ \mathsf{AND}_2 \circ \mathsf{EMAJ} \circ \widehat{\mathsf{ELT}}_{i-1} = \\ & \mathsf{MAJ} \circ \mathsf{EMAJ} \circ \widehat{\mathsf{ELT}}_{i-1} = \\ & \mathsf{MAJ} \circ \widehat{\mathsf{ELT}}_i = \widehat{\mathsf{LT}}_{i+1}.\end{aligned}$$

3. Доказательство этих включений полностью аналогично предыдущему пункту.

■

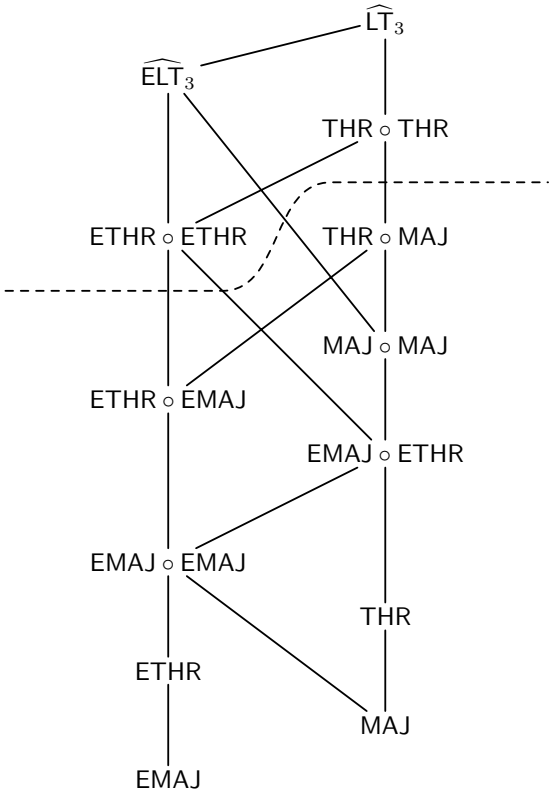


Рисунок 4.3: Подробная нижняя часть иерархии. Штриховая линия отделяет классы, для которых известны сильные нижние оценки.

4.3 Разделение классов

На рисунке 4.3 изображены классы в нижней части иерархии. Нижние оценки известны для всех классов ниже штриховой линии (см. обзор этих результатов в [69]).

Что касается разделения классов на рисунке 4.3, для большинства классов ниже штриховой линии отделение их от всех остальных классов известно (см. [69]). Разделение классов $\mathrm{THR} \circ \mathrm{MAJ}$ и $\mathrm{THR} \circ \mathrm{THR}$ было доказано в [36].

Ниже мы доказываем отделение классов $\mathrm{EMAJ} \circ \mathrm{ETHR}$, $\mathrm{ETHR} \circ \mathrm{ETHR}$ и $\widehat{\mathsf{ELT}}_3$ от классов в иерархии пороговых схем. Вместе с результатами, перечисленными выше, это доказывает, что все классы, расположенные ниже штриховой линии, отличаются от всех остальных классов иерархии.

Теорема 4.5. *Верны следующие разделения классов:*

1. $\mathsf{THR} \circ \mathsf{MAJ} \neq \mathsf{ETHR} \circ \mathsf{ETHR}$.

2. $\mathsf{MAJ} \circ \mathsf{MAJ} \neq \mathsf{ETHR} \circ \mathsf{ETHR}$.

3. $\mathsf{THR} \circ \mathsf{MAJ} \neq \widehat{\mathsf{ELT}}_3$.

Доказательство. В этом доказательстве мы пользуемся результатами о том, что $\mathsf{AC}^0 \not\subseteq \mathsf{MAJ} \circ \mathsf{MAJ}$ ([28, 118]) и $\mathsf{AC}^0 \not\subseteq \mathsf{THR} \circ \mathsf{MAJ}$ ([112]). Теорема сразу вытекает из следующих двух утверждений.

Утверждение 4.5. *Классы* $\mathsf{ETHR}\circ\mathsf{ETHR}$, $\mathsf{ETHR}\circ\mathsf{EMAJ}$, $\mathsf{EMAJ}\circ\mathsf{ETHR}$, $\mathsf{EMAJ}\circ\mathsf{EMAJ}$ *и* $\widehat{\mathsf{ELT}}_3$ *замкнуты относительно конъюнкции. То есть, если* $\mathcal{C}$ *— один из перечисленных выше классов, то* $\mathsf{AND} \circ \mathcal{C} = \mathcal{C}$.

Доказательство. Для примера докажем теорему для $\mathcal{C} = \mathsf{EMAJ} \circ \mathsf{ETHR}$. Для остальных классов доказательство аналогично. Верна следующая цепочка включений:

$$\mathsf{AND} \circ \mathsf{EMAJ} \circ \mathsf{ETHR} \subseteq$$
$$\mathsf{EMAJ} \circ \mathsf{AND}_2 \circ \mathsf{ETHR} \subseteq$$
$$\mathsf{EMAJ} \circ \mathsf{ETHR}.$$

Здесь первое включение следует из третьей части утверждения 4.3, а второе — из второй части того же утверждения. ■

Утверждение 4.6. *Классы* $\mathsf{MAJ}\circ\mathsf{MAJ}$ *и* $\mathsf{THR}\circ\mathsf{MAJ}$ *не замкнуты относительно конъюнкции, то есть* $\mathsf{AND} \circ \mathsf{MAJ} \circ \mathsf{MAJ} \neq \mathsf{MAJ} \circ \mathsf{MAJ}$ *и* $\mathsf{AND} \circ \mathsf{THR} \circ \mathsf{MAJ} \neq \mathsf{THR} \circ \mathsf{MAJ}$.

Доказательство. Мы знаем, что эти классы не содержат AC^0. Мы также знаем, что эти классы замкнуты относительно отрицания (мы даже знаем, что $\mathsf{NOT} \circ \mathsf{MAJ} = \mathsf{MAJ}$ и $\mathsf{NOT}\circ\mathsf{THR} = \mathsf{THR}$). Предположим, от противного, что эти классы замкнуты относительно конъюнкции. Поскольку AC^0 порождается функциями AND и NOT, отсюда вытекает, что классы содержат AC^0. ■

Это завершает доказательство теоремы. ■

Нетрудно видеть, что это же рассуждение позволяет доказать, что $\mathsf{EMAJ} \circ \mathsf{ETHR} \neq \mathsf{MAJ} \circ \mathsf{MAJ}$. Поскольку мы также знаем, что $\mathsf{EMAJ} \circ \mathsf{ETHR} \subseteq \mathsf{MAJ} \circ \mathsf{MAJ}$, мы получаем, что $\mathsf{MAJ} \circ \mathsf{MAJ} \not\subseteq \mathsf{EMAJ} \circ \mathsf{ETHR}$. Но в этом случае мы можем довести наше рассуждение до получения конкретной разделяющей функции.

Теорема 4.6. *Пусть* $\overline{\mathrm{DISJ}}$ *— отрицание функции* DISJ*. Тогда* $\overline{\mathrm{DISJ}} \in \mathsf{MAJ} \circ \mathsf{MAJ}$*, но* $\overline{\mathrm{DISJ}} \notin \mathsf{EMAJ} \circ \mathsf{ETHR}$*.*

Доказательство. Из определения DISJ легко видеть, что $\overline{\mathrm{DISJ}}(x, y) = \bigvee_{i=1}^{n}(x_i \wedge y_i)$. Поскольку $\mathrm{OR}, \mathrm{AND} \in \mathsf{MAJ}$, мы получаем $\overline{\mathrm{DISJ}} \in \mathsf{MAJ} \circ \mathsf{MAJ}$.

В работе [112] доказано, что функция $\bigwedge_{j=1}^{n} \bigvee_{i=1}^{n}(x_{ji} \wedge y_{ji})$ не лежит в $\mathsf{THR} \circ \mathsf{MAJ}$, а следовательно, она не лежит и в $\mathsf{EMAJ} \circ \mathsf{ETHR}$. Поскольку $\mathsf{EMAJ} \circ \mathsf{ETHR}$ замкнут относительно AND (утверждение 4.5), мы получаем, что функция $\bigvee_{i=1}^{n}(x_i \wedge y_i)$ также не лежит в $\mathsf{EMAJ} \circ \mathsf{ETHR}$, а это и есть функция $\overline{\mathrm{DISJ}}$. ■

Глава 5

Пороговые элементы над {1,2}

5.1 Предварительные сведения

Полиномиальные пороговые функции

Мы изучаем пороговые функции, в которых булевы переменные принимают значения $\{a, b\}$ для произвольных a и b.

Для данных оценок на длину $l(n)$ и на степень $d(n)$, мы обозначаем через $\mathsf{PTF}_{a,b}(l(n), d(n))$ класс булевых $f\colon \{a, b\}^n \to \{0, 1\}$, вычислимых полиномиальными пороговыми элементами длины не больше $l(n)$ и степени не больше $d(n)$. То есть, $f \in \mathsf{PTF}_{a,b}(l(n), d(n))$ тогда и только тогда, когда существует многочлен $p(x) \in \mathbb{Z}[x]$ 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.

Некоторые из областей определения $\{a, b\}^n$ по существу не отличаются от стандартных случаев $\{0, 1\}^n$ и $\{-1, 1\}^n$, а именно, это относится к случаям $\{0, a\}^n$ и $\{a, -a\}^n$, получающимся домножением на константу. Мы не будем рассматривать эти случаи. Под общими булевыми областями определения мы будем понимать все остальные области $\{a, b\}$.

Важно отметить, что для общих областей определения $\{a, b\}^n$ уже нельзя без ограничения общности предполагать, что многочлены мультилинейны, в

отличие от областей определения $\{0,1\}^n$ и $\{-1,1\}^n$. Мы все еще можем преобразовать любой полиномиальный пороговый элемент в мультилинейный, но при таком преобразовании число мономов может вырасти экспоненциально.

Мы будем приводить наши результаты для случая $\{a,b\} = \{1,2\}^n$. Однако, в большинстве наших результатов мы можем заменить $\{1,2\}$ любой другой областью определения $\{a,b\}$, где $|a| \neq |b|$ и $a,b \neq 0$. Исключениями являются результаты о полиномиальных пороговых функциях постоянной длины[1], а именно, утверждения 5.1 и 5.2. Эти результаты выполняются при дополнительном предположении $\mathrm{sgn}(a) = \mathrm{sgn}(b)$.

Экспоненциальная форма полиномиальных пороговых элементов

В этой главе нам будет удобно переходить обратно к переменным $\{0,1\}^n$, даже когда мы рассматриваем полиномиальные пороговые элементы над переменными $\{1,2\}^n$. По данным переменным $y_1,\ldots,y_n \in \{1,2\}$ мы определяем соответствующие переменные $x_1,\ldots,x_n \in \{0,1\}$ через $x_i = \log_2(y_i)$. Соответственно, верно равенство $y_i = 2^{x_i}$. При такой замене переменных мономы превращаются в экспоненциальные функции $y_1^{a_1}\ldots y_n^{a_n} = 2^{a_1x_1+\ldots+a_nx_n}$, а многочлены $P(y) = \sum_{j=1}^{l} c_j \prod_{i=1}^{n} y_i^{a_{ij}}$ превращаются во взвешенные суммы экспоненциальных функций:

$$P(y) = \sum_{j=1}^{l} c_j 2^{\sum_{i=1}^{n} a_{ij}x_i} \ ,$$

где $a_{ij} \geqslant 0$ — неотрицательные целые степени многочлена. Такое представление полиномиального порогового элемента мы будем называть *экспоненциальной формой*. Для удобства мы будем также допускать отрицательные целые коэффициенты a_{ij} в экспонентах. Но заметим, что простым умножением всего выражения на множитель $2^{\sum_{i=1}^{n} b_i x_i}$, где $b_i = \max(0, \max_j -a_{ij})$, мы можем сде-

[1]Нетрудно заметить, что функцию XOR можно вычислить полиномиальной пороговой функцией длины 1 над переменными $\{1,-2\}$, но не над $\{1,2\}$.

лать все коэффициенты положительными, не изменяя знака выражения. Чтобы сохранить связь с многочленами при допущении отрицательных целых экспонент, мы распространим на этот случай определение степени и будем считать ее равной $\max_j(\sum_{i=1}^n \max(0, a_{ij})) + \max_j(\sum_{i=1}^n \max(0, -a_{ij}))$.

Иногда также нам может быть удобно перенести абсолютное значение коэффициента $|c_j|$ в экспоненту как аддитивное слагаемое $\log_2(|c_j|)$, чтобы все коэффициенты экспоненциальной формы были по модулю равны 1.

5.2 Описание полиномиальных пороговых функций через через пороговые схемы

Сначала заметим, что полиномиальными пороговыми элементами длины 2 над переменными $\{1, 2\}^n$ уже можно вычислить все линейные пороговые функции, и оказывается, что эти классы совпадают. Более того, случай полиномиальной степени соответствует случаю полиномиального веса.

Утверждение 5.1. $\mathsf{PTF}_{1,2}(2, \infty) = \mathsf{THR} \quad u \quad \mathsf{PTF}_{1,2}(2, poly(n)) = \mathsf{MAJ}$.

Доказательство. Рассмотрим сначала линейную пороговую функцию $\mathrm{THR}_{w,t}$, заданную линейным неравенством $\sum_{i=1}^n w_i x_i - t \geqslant 0$. Применяя к каждой стороне неравенства экспоненциальную функцию с основанием 2, мы сразу получаем экспоненциальную форму требуемой полиномиальной пороговой функции длины 2.

В обратную сторону, рассмотрим полиномиальную пороговую функцию длины 2, определенную в экспоненциальной форме неравенством $c_1 2^{\sum_{i=1}^n a_i x_i} + c_2 2^{\sum_{i=1}^n b_i x_i} \geqslant 0$. Если $\mathrm{sgn}(c_1) = \mathrm{sgn}(c_2)$, эта булева функция равна константе, а значит, очевидно является линейной пороговой функцией. Так что предположим, что $\mathrm{sgn}(c_1) \neq \mathrm{sgn}(c_2)$. Без ограничения общности, пусть $c_1 > 0$ и $c_2 < 0$. Тогда неравенство равносильно линейному неравенству $\sum_{i=1}^n (a_i - b_i)x_i + \log_2 c_1 - \log_2(-c_2) \geqslant 0$, задающему линейную пороговую функцию.

Легко видеть, что описанные сведения работают и в случае полиномиальной степени и полиномиального веса. ■

Мы можем обобщить рассуждение в утверждении 5.1 в одну из сторон.

Лемма 5.1. *Всякая функция, вычислимая схемой вида* $\mathsf{AND}_k \circ \mathsf{THR}$ *или* $\mathsf{OR}_k \circ \mathsf{THR}$*, может быть вычислена полиномиальным пороговым элементом над* $\{1,2\}^n$ *длины* $k+1$*. Аналогично, всякая функция, вычислимая схемой вида* $\mathsf{AND}_k \circ \mathsf{MAJ}$ *или* $\mathsf{OR}_k \circ \mathsf{MAJ}$*, может быть вычислена полиномиальным пороговым элементом над* $\{1,2\}^n$ *длины* $k+1$ *и степени* $poly(n)$*.*

Доказательство. Мы проведем доказательство для случая схем $\mathsf{OR}_k \circ \mathsf{THR}$. Случай схем $\mathsf{AND}_k \circ \mathsf{THR}$ выводится применением правил де Моргана. Пусть k пороговых функций в схеме заданы знаками линейных выражений $l_1(x), \ldots, l_k(x)$ с целыми коэффициентами. Положим $c = \lceil \log_2 k \rceil + 2$ и определим новые линейные выражения $\widehat{l_1}(x), \ldots, \widehat{l_k}(x)$ как $\widehat{l_i}(x) = c(l_i(x) + 1)$. Тогда мы можем определить полиномиальную пороговую функцию экспоненциальной формой

$$E(x) = 2^{\widehat{l_1}(x)} + \cdots + 2^{\widehat{l_k}(x)} - 2k \ .$$

В случае, если существует i, такое что $l_i(x) \geqslant 0$, то $\widehat{l_i}(x) \geqslant c$, а значит $E(x) \geqslant 2^c - 2k > 0$. В случае, если для всех i верно $l_i(x) < 0$, то мы также имеем $\widehat{l_i}(x) \leqslant 0$ для всех i, а значит, $E(x) \leqslant k - 2k < 0$. Вновь, легко видеть, что описанное сведение работает и в случае полиномиальной степени и полиномиального веса. ■

Поскольку полиномиальные пороговые функции являются знаковыми функциями многочленов, легко видеть, что они замкнуты относительно операции взятия XOR постоянной входной степени (этот результат не зависит от области определения $\{a, b\}$ переменных).

Лемма 5.2. *Если функции $f_1, \ldots, f_k$ вычисляются полиномиальными пороговыми элементами длины s над переменными $\{1,2\}^n$, то* $\mathrm{XOR}(f_1, \ldots, f_k)$ *вычисляется полиномиальным пороговым элементом длины s^k над переменными $\{1,2\}^n$. Более того, если каждый из k полиномиальных пороговых элементов имеет степень не больше d, то новый полиномиальный пороговый элемент имеет степень не выше kd.*

Доказательство. Пусть $E_1(x), \ldots, E_k(x)$ — экспоненциальные формы полиномиальных пороговых элементов, вычисляющих $f_1, \ldots, f_k$, причем все формы E_i не обращаются в ноль на булевых входах. Тогда $-\prod_{j=1}^{k}(-E_j(x))$ — экспоненциальная форма полиномиального порогового элемента, вычисляющего $\mathrm{XOR}(f_1(x), \ldots, f_k(x))$. ■

Замечание 5.1. *Заметим, что классы* $\mathsf{THR}\circ\mathsf{THR}$, $\mathsf{MAJ}\circ\mathsf{MAJ}$ *и другие также замкнуты относительно функции* XOR *постоянной входной степени. Для этого достаточно, пользуясь результатом теоремы 4.2, перейти к элементам* ETHR *и* EMAJ *на нижнем уровне и использовать замкнутость этих элементов относительно* AND_k.

Теперь мы можем описать функции, вычислимые полиномиальными пороговыми элементами постоянной длины над переменными $\{1,2\}^n$ в терминах логических комбинаций постоянного числа линейных пороговых функций. Этот класс функций ранее рассматривался в контексте теории обучения [87].

Утверждение 5.2. $\mathsf{PTF}_{1,2}(O(1), \infty) = \mathsf{ANY}_{O(1)} \circ \mathsf{THR}$ *и* $\mathsf{PTF}_{1,2}(O(1), poly(n)) = \mathsf{ANY}_{O(1)} \circ \mathsf{MAJ}$.

Доказательство. Рассмотрим функцию $g(f_1(x), \ldots, f_k(x))$, где каждая f_i — линейная пороговая функция. Сначала выразим $g(y)$ в виде многочлена $p(y)$ от k переменных над полем $\mathbb{Z}_2$. По лемме 5.1 функции от переменных x, определяемые мономами p (это конъюнкции), можно вычислить полиномиальными

пороговыми элементами длины $k+1$. Используя лемму 5.2, мы можем выразить сумму над $\mathbb{Z}_2$ этих не более чем 2^k функций полиномиальным пороговым элементом длины $(k+1)^{2^k}$.

В обратную сторону, мы покажем, как вычислить знак полиномиального порогового элемента длины k булевой комбинацией постоянного числа линейных пороговых функций. Мы опишем это вычисление в терминах разрешающего дерева, где в каждой вершине дерева вычисляется линейная пороговая функция.

Эта модель вычислений описывается корневым двоичным деревом, каждая внутренняя вершина которого помечена линейной пороговой функцией, каждый лист помечены 0 или 1, из каждой внутренней вершины выходит два ребра, одно из которых помечено 0, а другое помечено 1. Вычисление таким деревом происходит следующим образом. На произвольном входном наборе мы начинаем из корня и постепенно спускаемся к листьям дерева. В каждой промежуточной вершине мы вычисляем пороговую функцию, приписанную данной вершине, на нашем входе и переходим по ребру, метка которого совпадает со значением вычисленной пороговой функции. Когда мы приходим в лист вычисление заканчивается, и результатом является метка листа.

Рассмотрим полиномиальный пороговый элемент в экспоненциальной форме

$$s_1 2^{l_1(x)} + \cdots + s_k 2^{l_k(x)},$$

где $s_i \in \{-1, +1\}$, а коэффициенты каждой l_i, кроме, возможно, свободного коэффициента, целые. Положим $c = \lceil \log_2 k \rceil$ и рассмотрим вход $x \in \{0,1\}^n$. Сначала с помощью разрешающего дерева глубины $O(k)$ мы находим индексы i_1 и i_2, такие что

$$l_{i_1}(x) \geqslant l_{i_2}(x) \geqslant l_j(x)$$

для всех $j \notin \{i_1, i_2\}$. Если $l_{i_1}(x) \geqslant c + l_{i_2}(x)$, то знак $E(x)$ совпадает с s_{i_1}. Иначе, мы получаем, что $l_{i_1}(x) = d + l_{i_2}$ для некоторого числа $0 \leqslant d < c$. Заметим, что есть не больше c возможных значений d, поскольку коэффициенты $l_{i_1}(x)$ и $l_{i_2}(x)$,

кроме, возможно, свободных коэффициентов, целые. Мы можем найти значение d разрешающим деревом глубины не больше $\lceil \log_2 c \rceil$. Для фиксированного d (и фиксированного x) мы можем теперь переписать экспоненциальную форму в виде

$$(s_{i_1} 2^d + s_{i_2}) 2^{l_{i_2}(x)} + \sum_{j \notin \{i_1, i_2\}} s_j 2^{l_j(x)} = s 2^{l(x)} + \sum_{j \notin \{i_1, i_2\}} s_j 2^{l_j(x)}$$

для подходящих s и l, зависящих от s_{i_1}, s_{i_2}, l_{i_2} и d, но в остальном не зависящих от конкретного x. Поскольку мы получили выражение того же типа, что и выше, но с $k-1$ слагаемым, мы можем повторять эту процедуру. В результате мы получаем разрешающее дерево глубины $O(k^2)$, определяющее знак выражения. По такому дереву мы в свою очередь можем построить булеву комбинацию не более чем $2^{O(k^2)}$ линейных пороговых функций (всех функций в вершинах дерева), вычисляющих ту же функцию. Вновь, легко видеть, что рассуждения без изменений переносятся на случай полиномиальной степени и полиномиального веса. ■

В случае полиномиальной степени мы можем описать булевы функции, вычислимые полиномиальными пороговыми элементами над $\{1, 2\}^n$ полиномиальной длины, в терминах пороговых схем.

Теорема 5.1.

$$\mathsf{PTF}_{1,2}(poly(n)) = \mathsf{THR} \circ \mathsf{MAJ}.$$

Доказательство. Сначала мы построим полиномиальную пороговую функцию по схеме из $\mathsf{THR} \circ \mathsf{MAJ}$. Пусть выходной элемент схемы задается неравенством $(\sum_{k=1}^{s} w_k y_k) - t \geqslant 0$. Пусть $l_1(x), \ldots, l_s(x)$ — линейные формы с целыми коэффициентами, определяющие функции голосования на нижнем уровне схемы. Пусть $p(n)$ — многочлен, такой что $|l_k(x)| \leqslant p(n)$ для всех $x \in \{0, 1\}^n$ и всех k.

Рассмотрим $m = 2p(n) + 1$ и определим матрицу $A = (a_{ij})$ размера $m \times m$ формулой $a_{ij} = 2^{(i-p(n)-1)(j-1)}$ для $i, j = 1, \ldots, m$. Заметим, что A — матрица Вандермонда с различными строками, а значит, матрица A обратима.

Рассмотрим $u = (\underbrace{0,\ldots,0}_{p(n)},\underbrace{1,\ldots,1}_{p(n)+1})^{\mathsf{T}}$, и положим $v = A^{-1}u$. Рассмотрим полиномиальные пороговые элементы с экспоненциальными формами $E_1(x),\ldots,E_s(x)$, равными

$$E_k(x) = \sum_{j=1}^{m} v_j 2^{(j-1)l_k(x)} \ . \tag{5.1}$$

По построению мы получаем $E_k(x) = u_{l_k(x)+p(n)+1}$. Другими словами, если $l_k(x) < 0$, то $E_k(x) = 0$, а если $l_k(x) \geqslant 0$, то $E_k(x) = 1$. Тогда полиномиальный пороговый элемент для всей схемы в экспоненциальной форме имеет вид $E(x) = (\sum_{k=1}^{s} w_k E_k(x)) - t$.

В обратную сторону, рассмотрим полиномиальный пороговый элемент с экспоненциальной формой $E(x) = \sum_{k=1}^{s} c_k 2^{l_k(x)}$, в котором коэффициенты $l_k(x)$ — положительные числа полиномиальной величины. Тогда существует многочлен $p(n)$, такой что $0 \leqslant l_k(x) \leqslant p(n)$ для всех $x \in \{0,1\}^n$ и всех k. Теперь мы можем построить схему $\mathsf{THR} \circ \mathsf{EMAJ}$ следующим образом. Для всякого $k \in \{1,\ldots,s\}$ и всякого $j \in \{0,\ldots,p(n)\}$ рассмотрим элемент EMAJ, задаваемый уравнением $l(x) = j$, и подставим выход этого элемента в выходной элемент THR с весом $c_k 2^j$. Эту $\mathsf{THR} \circ \mathsf{EMAJ}$ схему можно преобразовать в $\mathsf{THR} \circ \mathsf{MAJ}$ схему, пользуясь результатом теоремы 4.2. ■

Из этого результата вытекает также структурный результат о пороговых схемах глубины 2.

Лемма 5.3. *Всякая схема вида* $\mathsf{THR} \circ \mathsf{MAJ}$ *полиномиального размера эквивалентна схеме полиномиального размера в том же классе, такой что все функции голосования на нижнем уровне в ней монотонны.*

Доказательство. Начиная со схемы вида $\mathsf{THR} \circ \mathsf{MAJ}$, мы сначала переходим к полиномиальной пороговой функции в экспоненциальной форме, затем, умножая все выражение на достаточно большой множитель $2^{c\sum_i x_i}$, мы делаем все коэффициенты в экспонентах положительными, и наконец, переходим обратно

к схеме вида $\mathsf{THR} \circ \mathsf{MAJ}$. Заметим, что доказательство теоремы 5.1 дает схему с монотонными элементами на нижнем уровне. ■

Предыдущая лемма может быть доказана напрямую теми же методами, что и в доказательстве теоремы 5.1. Это прямое доказательство дает и аналогичный результат для $\mathsf{MAJ} \circ \mathsf{MAJ}$ схем. Мы приводим это рассуждение в разделе 5.6.

5.3 Нижние оценки для полиномиальных пороговых функций

Знаковым рангом действительной матрицы $A = (a_{ij})$ с ненулевыми коэффициентами называется минимальный ранг действительной матрицы $B = (b_{ij})$ того же размера, что и A, удовлетворяющей равенству $\operatorname{sgn}(a_{ij}) = \operatorname{sgn}(b_{ij})$ для всех i, j. Нас интересует знаковый ранг матриц, задаваемых булевыми функциями. Пусть $f : \{a,b\}^n \times \{a,b\}^n \to \{-1,+1\}$ — булева функция от $2n$ битов, разбитых на два блока, по n битов в каждом. Мы сопоставляем с f так называемую *коммуникационную матрицу* M_f размера $2^n \times 2^n$, проиндексированную наборами $x, y \in \{a,b\}^n$ и определяемую как $(M_f)_{x,y} = f(x,y)$.

Лемма 5.4. *Пусть $f : \{1,2\}^n \times \{1,2\}^n \to \{-1,+1\}$ вычисляется полиномиальным пороговым элементом над $\{1,2\}^n \times \{1,2\}^n$ длины s. Тогда матрица M_f имеет знаковый ранг не больше s.*

Доказательство. Рассмотрим полиномиальный пороговый элемент, вычисляющий f, в экспоненциальной форме $E(x,y) = \sum_{j=1}^{s} c_j 2^{l_j(x,y)}$. Для каждого j зададим матрицу B_j размера $2^n \times 2^n$, проиндексированную $x, y \in \{0,1\}^n$, формулой $(B_j)_{x,y} = 2^{l_j(x,y)}$. Из этого определения сразу видно, что матрица $B = \sum_{j=1}^{s} c_j B_j$ является знаковым представлением M_f. Заметим, что мы можем разложить $l_j(x,y) = l_j^{(1)}(x) + l_j^{(2)}(y)$. Следовательно, B_j представляется в виде $B_j = b_j^{(1)} b_j^{(2)\mathsf{T}}$, где $b_j^{(1)}, b_j^{(2)} \in \mathbb{R}^n$ определяются как $(b_j^{(1)})_x = 2^{l_j^{(1)}(x)}$ и

$(b_j^{(2)})_y = 2^{l_j^{(2)}(y)}$. Следовательно, B_j имеет ранг не больше 1, а значит, $\operatorname{rank}(B) \leqslant \sum_{j=1}^{s} \operatorname{rank}(B_j) \leqslant s$. ■

Таким образом, из нижних оценок знакового ранга коммуникационной матрицы булевой функции сразу следуют нижние оценки длины полиномиальных пороговых элементов над $\{1,2\}^n$ независимо от их степени. Сильные нижние оценки на знаковый ранг известны для ряда булевых функций. Отметим два результата на эту тему. Форстер [46] показал, что матрица размера $2^n \times 2^n$, соответствующая функции $\mathrm{IP}_2(x,y)$, вычисляющей скалярное произведение векторов по модулю 2, имеет знаковый ранг $2^{\frac{n}{2}}$. Разборов и Шерстов [112] доказали, что знаковый ранг матрицы размера $2^{m^3} \times 2^{m^3}$, соответствующей булевой функции $f_m(x,y) = \bigwedge_{i=1}^{m} \bigvee_{j=1}^{m^2} (x_{ij} \wedge y_{ij})$, равен $2^{\Omega(m)}$. Комбинируя эти результаты с леммой 5.4, мы получаем следующее следствие.

Следствие 5.5. *Всякий полиномиальный пороговый элемент над* $\{1,2\}^n \times \{1,2\}^n$*, вычисляющая* IP_2 *имеет длину не меньше* $2^{\frac{n}{2}}$*. Всякая полиномиальная пороговая функция над* $\{1,2\}^{m^3} \times \{1,2\}^{m^3}$ *вычисляющая* f_m *имеет длину* $2^{\Omega(m)}$*.*

Знаковый ранг ранее использовался для доказательства нижних оценок для $\mathsf{THR} \circ \mathsf{MAJ}$ схем [47] и знаковый ранг остается единственным методом для доказательства таких оценок. Поскольку по теореме 5.1 полиномиальные пороговые элементы вычисляют все функции, вычислимые $\mathsf{THR} \circ \mathsf{MAJ}$ схемами, уже в случае полиномиальной степени следствие 5.5 указывает, что техника доказательства нижних оценок через знаковый ранг применима к более сильным моделям вычисления. Доказательство того, что эти модели действительно являются (строго) более сильными, требует другого метода доказательства нижних оценок для $\mathsf{THR} \circ \mathsf{MAJ}$ схем. Тем не менее, мы свяжем вопрос о том, являются ли полиномиальные пороговые элементы без ограничения на степень более выразительной моделью, чем полиномиальные пороговые элементы полиномиальной степени, с вопросом о соотношении классов пороговых схем.

Для этого нам потребуется следующая лемма.

Лемма 5.6. *Для всякого s верно включение* $\mathsf{THR}_s \circ \mathsf{ETHR} \subseteq \mathsf{PTF}_{1,2}(s+1,\infty) \circ \mathsf{AND}_2$. *В частности,* $\mathsf{THR} \circ \mathsf{THR} \subseteq \mathsf{PTF}_{1,2}(\infty) \circ \mathsf{AND}_2$.

Доказательство. Из следствия 4.1 мы знаем, что $\mathsf{THR} \circ \mathsf{THR} = \mathsf{THR} \circ \mathsf{ETHR}$, так что второе утверждение вытекает из первого. Рассмотрим схему C вида $\mathsf{THR}_s \circ \mathsf{ETHR}$ с элементами $g_1, \ldots, g_s$ вида ETHR, заданными линейными формами $l_1(x), \ldots, l_s(x)$, и предположим, что выходной элемент вида THR задан как $\operatorname{sgn}(\sum_{j=1}^s w_j y_j - t)$, где $w_j \neq 0$ для всех j. Рассмотрим многочлены $p_1, \ldots, p_s$ вида $p_j(x) = -C_j l_j(x)^2$ для достаточно больших констант C_j. Тогда $2^{p_j(x)} = 1$, если $l_j(x) = 0$, и $2^{p_j(x)}$ очень близки к нулю, если $l_j(x) \neq 0$, так что $2^{p_j(x)}$ хорошо приближает элемент вида ETHR, соответствующий l_j. Более точно, пусть $0 < m \leqslant \min_{y \in \{0,1\}^s} |\sum_{j=1}^s w_j y_j - t|$ таково, что $m/(2s|w_j|) < 1$ для всех j (мы предполагаем, что линейная форма элемента THR не обращается в ноль). Положим $m_j = \min_{\{x \in \{0,1\}^n | l_j(x) \neq 0\}} l_j(x)^2$ и положим $C_j = \lfloor \log_2((2s|w_j|)/m)/m_j \rfloor$. Пусть $x \in \{0,1\}^n$, определим $y \in \{0,1\}^s$ равным $y_j = 1$ тогда и только тогда, когда $l_j(x) = 0$. Тогда нетрудно видеть, что $|y_j - 2^{p_j(x)}| \leqslant m/2s|w_j|$, а значит, $\left|\sum_{j=1}^s w_j y_j - \sum_{j=1}^s w_j 2^{p_j(x)}\right| \leqslant \frac{m}{2}$. Следовательно, знак выражения $\sum_{j=1}^s w_j 2^{p_j(x)} - t$ соответствует выходу схемы. С другой стороны, нетрудно видеть, что после раскрытия скобок в экспонентах это выражение соответствует схеме вида $\mathsf{PTF}_{1,2}(s+1,\infty) \circ \mathsf{AND}_2$ (заметим, что коэффициенты многочленов p_j целые). ■

Теорема 5.2. *Если* $\mathsf{THR} \circ \mathsf{THR} \not\subseteq \mathsf{THR} \circ \mathsf{MAJ} \circ \mathsf{AND}_2$, *то* $\mathsf{PTF}_{1,2}(\mathit{poly}(n)) \subsetneq \mathsf{PTF}_{1,2}(\infty)$.

Доказательство. Предположим, что $\mathsf{PTF}_{1,2}(\mathrm{poly}(n)) = \mathsf{PTF}_{1,2}(\infty)$. Тогда

$$\mathsf{THR} \circ \mathsf{THR} \subseteq \mathsf{PTF}_{1,2}(\infty) \circ \mathsf{AND}_2 = \mathsf{PTF}_{1,2}(\mathrm{poly}(n)) \circ \mathsf{AND}_2 = \mathsf{THR} \circ \mathsf{MAJ} \circ \mathsf{AND}_2,$$

где первое включение следует из леммы 5.6, а последнее равенство следует из теоремы 5.1. ■

Нам представляется, что включение $\mathsf{THR} \circ \mathsf{THR} \subseteq \mathsf{THR} \circ \mathsf{MAJ} \circ \mathsf{AND}_2$ маловероятно. Заметим, что из него, в том числе, вытекало бы, что $\mathsf{THR} \circ \mathsf{THR} \circ \mathsf{AND} = \mathsf{THR} \circ \mathsf{MAJ} \circ \mathsf{AND}$.

5.4 Макс-плюс полиномиальные пороговые функции

В этом разделе мы введем еще один сложностной класс, который представляет собой «предельный» класс для наших классов полиномиальных пороговых функций, строящийся в духе макс-плюс алгебры. Оказывается, что этот класс связан с булевыми схемами вида $\mathsf{AC}^0 \circ \mathsf{THR}$.

Рассмотрим целочисленный многочлен $p(x) \in \mathbb{Z}[x]$ и будем рассматривать его над переменными $\{1, b\}$. Этот многочлен вычисляет некоторую функцию в $\mathsf{PTF}_{1,b}(l, d)$, где l — длина p, а d — степень p. Сначала проделаем предварительную работу, чтобы привести p в «общее положение». Во-первых, мы можем предполагать, что $p(x) \neq 0$ для всех $x \in \{1, b\}^n$. Для этого, как обычно, просто перейдем к многочлену $2p(x) + 1$ вместо $p(x)$. Далее, заменяя коэффициенты p на близкие рациональные числа и умножая весь многочлен на подходящее целое число так, чтобы все коэффициенты вновь стали целыми, мы можем добиться того, чтобы для каждого $x \in \{1, b\}^n$ никакие два монома не были равны друг другу.

Теперь рассмотрим экспоненциальную форму p:

$$P(x) = \sum_{i=1}^{l_1} b^{L_i(x)} - \sum_{j=1}^{l_2} b^{M_j(x)}, \quad L_i(x) = \sum_{k=1}^{n} v_{ki} x_k + v_{0i}, \quad M_j(x) = \sum_{k=1}^{n} u_{kj} x_k + u_{0j}.$$

Здесь мы помещаем коэффициенты многочлена в экспоненты.

Теперь начнем увеличивать в этом выражении b (для удобства будем считать, что b положителен). Тогда функция, вычисляемая p, может начать меняться. Поскольку все линейные формы различны для всех входов $x \in \{0, 1\}^n$,

нетрудно видеть, что для достаточно большого b и для любого x знак $P(x)$ равен знаку самого большого монома. То есть, $P(x) \geqslant 0$ тогда и только тогда, когда

$$\max_{i=1,\ldots,l_1}(L_i(x)) \geqslant \max_{j=1,\ldots,l_2}(M_j(x)). \tag{5.2}$$

Определение 5.1. *Макс-плюс полиномиальным пороговым элементом мы называем выражение вида* (5.2). *Длиной полиномиального порогового элемента* (5.2) *мы называем* $l_1 + l_2$, *степенью — максимальную сумму абсолютных значений коэффициентов* $L_1, \ldots, L_{l_1}$ *и* $M_1, \ldots, M_{l_2}$, *кроме свободного коэффициента. Заметим, что макс-плюс полиномиальный пороговый элемент по сути является полиномиальным неравенством в макс-плюс алгебре.*

Обозначим через $\mathsf{mpPTF}(l(n), d(n))$ *класс всех булевых функций, вычислимых макс-плюс полиномиальными пороговыми элементами длины* $l(n)$ *и степени* $d(n)$. *Как и раньше, обозначим через* $\mathsf{mpPTF}(d(n))$ *множество булевых функций, вычислимых макс-плюс полиномиальными пороговыми элементами длины* $poly(n)$ *и степени* $d(n)$. *Здесь* $d(n)$ *может быть равно* ∞.

Оказывается, что класс $\mathsf{mpPTF}(\infty)$ связан с булевыми схемами вида $\mathsf{AC}^0 \circ \mathsf{THR}$. Более конкретно, мы можем рассмотреть иерархию схем полиномиального размера вида $\mathsf{AC}^0_{d,\mathrm{OR}} \circ \mathsf{THR}$ и $\mathsf{AC}^0_{d,\mathrm{AND}} \circ \mathsf{THR}$. В этой иерархии нижние оценки известны только для случая $d = 1$, то есть для схем вида $\mathsf{AND} \circ \mathsf{THR}$ и $\mathsf{OR} \circ \mathsf{THR}$ (работает, например, стандартное доказательство нижней оценки на размер ДНФ для функции PARITY). Для схем вида $\mathsf{AND} \circ \mathsf{OR} \circ \mathsf{THR}$ и $\mathsf{OR} \circ \mathsf{AND} \circ \mathsf{THR}$ не известно сверхполиномиальной нижней оценки на сложность явно заданных функций. Оказывается, что класс $\mathsf{mpPTF}(\infty)$ лежит между этими двумя уровнями в иерархии.

Сначала заметим некоторое простое свойство макс-плюс полиномиальных пороговых функций.

Утверждение 5.3. *Классы* $\mathsf{mpPTF}(\infty)$ *и* $\mathsf{mpPTF}(poly(n))$ *замкнуты относительно взятия отрицания.*

Доказательство. Это напрямую следует из определения макс-плюс полиномиальных пороговых функций и того факта, что всякую макс-плюс полиномиальную пороговую функцию можно легко перестроить в таком виде, что для всех $x \in \{0,1\}^n$ в (5.2) не выполняется равенство. Для этого достаточно для каждого i рассмотреть $2L_i + 1$ вместо L_i и для всякого j рассмотреть $2M_j$ вместо M_j. Это увеличивает степень не более чем на постоянный множитель. ■

Теперь свяжем макс-плюс полиномиальные пороговые функции с описанной иерархией.

Лемма 5.7. $\mathsf{AND} \circ \mathsf{THR}, \mathsf{OR} \circ \mathsf{THR} \subseteq \mathsf{mpPTF}(\infty)$ *и* $\mathsf{mpPTF}(\infty) \subseteq \mathsf{AND} \circ \mathsf{OR} \circ \mathsf{THR}, \mathsf{OR} \circ \mathsf{AND} \circ \mathsf{THR}$.

Доказательство. Пусть нам дана схема вида $\mathsf{OR} \circ \mathsf{THR}$ и $l_1 \geqslant 0, \ldots, l_k \geqslant 0$ — ее пороговые элементы на нижнем уровне. Тогда нетрудно видеть, что макс-плюс полиномиальный пороговый элемент

$$\max(l_1, \ldots, l_k) \geqslant 0$$

вычисляет ту же функцию. Для класса $\mathsf{AND} \circ \mathsf{THR}$ работает аналогичное доказательство. Другое доказательство для этого класса можно получить с помощью утверждения 5.3.

Теперь рассмотрим макс-плюс полиномиальный пороговый элемент (5.2). Он выдает значение 1 тогда и только тогда, когда существует $i \in [l_1]$, такое что для всех $j \in [l_2]$ выполняется $L_i(x) \geqslant M_j(x)$. То есть, этот макс-плюс полиномиальный пороговый элемент эквивалентна формуле

$$\bigvee_{i=1}^{l_1} \bigwedge_{j=1}^{l_2} \left(L_i(x) \geqslant M_j(x)\right),$$

которая очевидно лежит в классе $\mathsf{OR} \circ \mathsf{AND} \circ \mathsf{THR}$. Вновь включение в $\mathsf{AND} \circ \mathsf{OR} \circ \mathsf{THR}$ вытекает из утверждения 5.3. ■

Теперь мы покажем, что макс-плюс полиномиальные пороговые элементы не сильнее обычных полиномиальных пороговых элементов.

Лемма 5.8. *Для любого $b > 1$ существует константа C, такая что* $\mathsf{mpPTF}(l(n), d(n)) \subseteq \mathsf{PTF}_{1,b}(l(n), C \cdot d(n) \log l(n))$.

Доказательство. Пусть нам дан макс-плюс полиномиальный пороговый элемент (5.2). Сначала преобразуем линейные формы так, чтобы для всякого $x \in \{0,1\}^n$ не выполнялось равенство.

Теперь рассмотрим следующий полиномиальный пороговый элемент P над $\{1, b\}$ в экспоненциальной форме:

$$P(x) = \sum_{i=1}^{l_1} b^{C \log l(n) L_i(x)} - \sum_{j=1}^{l_2} b^{C \log l(n) M_j(x)} \ ,$$

где C — некоторая константа. Нетрудно видеть, что если C таково, что $b^{C \log l(n)} > l(n)$, то для каждого $x \in \{0,1\}^n$ абсолютное значение максимального монома в $P(x)$ больше абсолютного значения суммы всех мономов противоположного знака. Следовательно, знак $P(x)$ равен знаку самого большого монома в нем, и $P(x) \geqslant 0$ тогда и только тогда, когда неравенство (5.2) верно. ■

Из этой леммы и следствия 5.5 мы сразу получаем следующее следствие.

Следствие 5.9. *Всякий макс-плюс полиномиальный пороговый элемент, вычисляющий* IP_2*, имеет длину* $2^{\frac{n}{2}}$*. Всякий макс-плюс полиномиальный пороговый элемент, вычисляющий* f_m*, имеет длину* $2^{\Omega(m)}$.

Таким образом, $\mathsf{mpPTF}(\infty)$ образует класс, промежуточный в $\mathsf{AC}^0 \circ \mathsf{THR}$ иерархии, для которого нам известны нижние оценки. С другой стороны, этот класс оказывается достаточно сильным. Мы покажем, что он содержит некоторые функции, которые оказываются трудными для других известных сложностных классов.

Лемма 5.10. $\mathrm{PARITY} \in \mathsf{mpPTF}(\mathit{poly}(n))$, $\mathsf{OMB} \circ \mathsf{THR} \subseteq \mathsf{mpPTF}(\infty)$.

Доказательство. То, что PARITY вычисляется в mpPTF, несложно вывести из анализа в [14, Теорема 4.1]. Положим $X = x_1 + \ldots + x_n$ и

$$L_i(x) = i(X - i) + C_i$$

для $i = 0, \ldots n$, где $C_0 = 0$, а остальные C_i определяются рекурсивно равенством $C_i = L_{i-1}(i) + 1/2$. Нетрудно видеть, что линейные формы L_i устроены так, что на входе с i единицами L_i принимает самое большое значение среди всех форм, на $1/2$ превышая предыдущую форму. Если мы поместим все L_i с нечетным i в левую часть (5.2), а все L_i с четным i — в правую часть (5.2), нетрудно видеть, что получившийся макс-плюс полиномиальный пороговый элемент вычисляет PARITY.

Предположим теперь, что $f \in \mathsf{OMB} \circ \mathsf{THR}$ и $l_1 \geqslant 0, \ldots, l_k \geqslant 0$ — пороговые элементы на нижнем уровне схемы. То есть $f(x) = 1$ тогда и только тогда, когда самое большое i, такое что $l_i(x) \geqslant 0$, нечетно (если такого i нет, то функция равна 0). Во-первых, как мы уже делали раньше, будем предполагать, что все формы l_i не обращаются в ноль. Положим

$$B = \max_{i=1,\ldots,k,\ x \in \{0,1\}^n} |l_i(x)| + 1.$$

Рассмотрим $l'_i(x) = B^{i-1} l_i(x)$ и макс-плюс полиномиальный пороговый элемент, которому в левую часть мы помещаем все l'_i для нечетных i, а в правую часть — все l'_i для четных i, а также дополнительно линейную форму, тождественно равную нулю. Нетрудно увидеть, что для любого x положительная линейная форма с наибольшим номером больше всех остальных линейных форм, а значит, построенный макс-плюс полиномиальный пороговый элемент вычисляет f. ■

Заметим, что в работе [28] доказано, что функция $\mathrm{OMB} \circ \mathrm{AND}_2$ не лежит в классе $\mathsf{MAJ} \circ \mathsf{MAJ}$. Как следствие, мы получаем следующее соотношение:

$$\mathsf{mpPTF}(\infty) \not\subseteq \mathsf{MAJ} \circ \mathsf{MAJ}.$$

Кроме макс-плюс полиномиальных пороговых функций, которые задаются просто полиномиальными неравенствами в макс-плюс алгебре, мы также можем рассмотреть системы макс-плюс полиномиальных неравенств и задаваемые ими функции. Ясно, что их можно выразить как AND от макс-плюс

полиномиальных пороговых функций. Но используя полученные выше результаты, мы можем в точности описать вычислительную силу систем макс-плюс полиномиальных пороговых элементов в терминах $\mathsf{AC}^0 \circ \mathsf{THR}$ схем.

Следствие 5.11. *Функции, вычислимые системами макс-плюс полиномиальных пороговых элементов суммарной полиномиальной длины, это в точности функции, вычислимые схемами вида* $\mathsf{AND} \circ \mathsf{OR} \circ \mathsf{THR}$ *полиномиального размера.*

Доказательство. Функции, вычислимые системами макс-плюс полиномиальных пороговых элементов, также вычисляются схемами вида $\mathsf{AND} \circ \mathsf{OR} \circ \mathsf{THR}$, поскольку по лемме 5.7 каждая функция, вычислимая макс-плюс полиномиальным пороговым элементом, вычисляется схемой вида $\mathsf{AND} \circ \mathsf{OR} \circ \mathsf{THR}$, а система — это просто AND своих полиномиальных пороговых элементов. С другой стороны, системы макс-плюс полиномиальных пороговых элементов могут вычислить любую функцию из $\mathsf{AND} \circ \mathsf{OR} \circ \mathsf{THR}$, поскольку по лемме 5.7 мы можем представить схемы из $\mathsf{OR} \circ \mathsf{THR}$ в виде макс-плюс полиномиальных пороговых элементов, а затем промоделировать элемент AND схемы взятием системы. ■

5.5 Соотношения между областями определения

Хотя соотношения между классами полиномиальных пороговых функций для разных областей определения остаются не до конца изученными, мы приводим некоторые частичные продвижения в этом направлении. В частности, мы устанавливаем связь для областей определения $\{1, 2\}$ и $\{1, -2\}$. Мы начнем с простых наблюдений.

Утверждение 5.4. *Для всех* $a, b \in \mathbb{R}$, *таких что* $a, b \neq 0$ *и* $|a| \neq |b|$, *верно* $\mathsf{PTF}_{a,b}(poly(n)) = \mathsf{PTF}_{1,2}(poly(n))$.

Доказательство. Это прямое следствие теоремы 5.1 (заметим, что доказательство теоремы проходит для всех указанных областей определения). ■

Утверждение 5.5. *Для всех $a, b \in \mathbb{R}$, таких что $a, b \neq 0$ и $|a| \neq |b|$, верно* $\mathsf{PTF}_{a,b}(l(n), d(n)) = \mathsf{PTF}_{1,\frac{b}{a}}(l(n), d(n))$.

Доказательство. Заметим, что если $y \in \{a, b\}$, то $z = y/a$ — соответствующая переменная над $\{1, \frac{b}{a}\}$. ■

Лемма 5.12. *Для всех $a, b \in \mathbb{R}$, таких что $a, b \neq 0$ и $|a| \neq |b|$, и для всякого натурального k выполняется* $\mathsf{PTF}_{a,b}(\infty) = \mathsf{PTF}_{a^k,b^k}(\infty)$.

Доказательство. Заметим, что $\mathsf{PTF}_{a^k,b^k}(\infty) \subseteq \mathsf{PTF}_{a,b}(\infty)$, поскольку все, что можно вычислить над $\{a^k, b^k\}$, можно вычислить и над $\{a, b\}$. Действительно, просто рассмотрим тот же многочлен, но увеличим все степени в k раз.

Чтобы доказать включение в другую сторону, сначала заметим, что по утверждению 5.5 мы можем предполагать, что $a = 1$.

Далее, заметим, что для $y \in \{1, b\}$ мы можем определить $x \in \{0, 1\}$ равным $x = \log_{|b|}(|y|)$, и тогда $y = b^x$. Так что мы можем рассмотреть экспоненциальную форму аналогично случаю области определения $\{1, 2\}$.

Рассмотрим функцию f из $\mathsf{PTF}_{1,b}(\infty)$ и рассмотрим многочлен p, вычисляющий ее над $\{1, b\}$. Мы покажем, как построить многочлен q, такой что $p(x) = q(x)$ для всех $x \in \{1, b\}^n$, все степени во всех мономах q делятся на k, и, наконец, длина q больше длины p не больше чем на полиномиальный множитель. Для этого рассмотрим один из мономов C многочлена p в экспоненциальной форме:

$$C = b^{a_1x_1+a_2x_2+\ldots+a_nx_n}.$$

Здесь все коэффициенты a_i целые. Обозначим через r_i остатки a_i от деления на k и положим $q_i = (a_i - r_i)/k$. Тогда

$$C = b^{r_1x_1+r_2x_2+\ldots+r_nx_n} \cdot \left(b^k\right)^{q_1x_1+q_2x_2+\ldots+q_nx_n}. \tag{5.3}$$

Обозначим первый множитель через D. Заметим, что степень D полиномиально ограничена, более конкретно, она не превышает kn. Повторяя аргумент

из первой части доказательства теоремы 5.1, мы можем построить многочлен $p_C \in \mathbb{Z}[x]$ полиномиального размера и полиномиальной степени, такой что если мы рассмотрим его как полиномиальную пороговую функцию над $\{1, b^k\}$ и рассмотрим его экспоненциальную форму p'_C, то равенство $p'_C(x) = D(x)$ будет выполняться для всех $x \in \{0,1\}^n$. Более точно, для этого мы строим многочлен так же, как в (5.1), но мы полагаем основание экспоненты равным b^k в матрице A и мы полагаем u равным вектору возможных значений D.

Подставляя p'_C вместо D в (5.3), мы получаем представление C над $\{1, b^k\}$. Повторяя это рассуждение для всех мономов, мы завершаем доказательство леммы. ■

Из этой леммы мы, в частности, получаем, что

$$\mathsf{PTF}_{1,2}(\infty) = \mathsf{PTF}_{1,2^2}(\infty) = \mathsf{PTF}_{1,(-2)^2}(\infty) = \mathsf{PTF}_{1,-2}(\infty).$$

5.6 Пороговые схемы с монотонными элементами

В этом разделе мы докажем структурную лемму о схемах, состоящих из функций голосования.

Лемма 5.13. *Всякую схему вида* $\mathsf{MAJ} \circ \mathsf{MAJ}$ *полиномиального размера можно переделать в эквивалентную схему того же вида полиномиального размера так, что все элементы на нижнем уровне монотонны (и мы разрешаем функции голосования на верхнем уровне применять отрицания к некоторым своим входам).*

Доказательство. Доказательство аналогично доказательству теоремы 5.1 и упрощается до следующего прямого рассуждения. Рассмотрим схему вида $\mathsf{MAJ} \circ \mathsf{MAJ}$ и рассмотрим пороговый элемент $l(x) = \sum_i a_i x_i + a_0 \geqslant 0$ на нижнем уровне. Мы выразим этот пороговый элемент в виде линейной комбинации

полиномиального количества пороговых элементов с коэффициентами, ограниченными полиномом. Для этого обозначим через $A(x)$ сумму положительных мономов в $l(x)$ и через $B(x)$ — сумму отрицательных мономов в $l(x)$, взятую с отрицанием. То есть, $l(x) = A(x) - B(x)$ и все коэффициенты в A и B положительны. Коэффициенты в A и B ограничены полиномом, а значит, эти линейные формы принимают лишь полиномиальное число различных значений на множестве $\{0,1\}^n$. Определим $c = \max_{x\in\{0,1\}^n} A(x) + 1$ и рассмотрим линейную форму $M(x) = A(x) + c(2B(x) + 1)$. Эта линейная форма также принимает лишь полиномиальное число значений и более того, нетрудно видеть, что если для некоторых $x, x' \in \{0,1\}^n$ $(A(x), B(x)) \neq (A(x'), B(x'))$, то $M(x) \neq M(x')$. Теперь рассмотрим все возможные значения пар $(A(x), B(x))$, такие что $l(x) \geqslant 0$ и пусть $t_1, \ldots, t_k$ — соответствующие значения M. Нетрудно увидеть, что $l(x) \geqslant 0$ тогда и только тогда, когда ровно для одного i верно равенство $M(x) - t_i = 0$. То есть, мы выразили наши пороговые элементы как суммы точных пороговых элементов $M(x)-t_1 = 0, \ \ldots, M(x)-t_k = 0$. Остается лишь воспользоваться теоремой 4.2. ■

Заметим, что то же самое доказательство работает и для схем вида $\mathsf{THR} \circ \mathsf{MAJ}$.

Глава 6

Вычисление функции голосования с помощью функций голосования меньшего числа переменных

В этой главе мы исследуем вопрос о том, для каких k существует монотонная схема, состоящая из элементов MAJ_k, заданной постоянной глубины d, вычисляющая функцию MAJ_n. Нам будет удобно предполагать, что в элементах схемы порог может быть любым (это моделируется подстановкой констант в качестве части входов).

6.1 Обозначения и вспомогательные результаты

В этом разделе мы введем обозначения, специфические для этой главы, а также приведем необходимые нам вероятностные неравенства.

В этой главе, как и в главе 3, нам будет удобно обозначать переменные через $X = \{x_1, x_2, \ldots, x_n\}$. На значения для переменных мы будем смотреть как на функции $A\colon X \to \{0,1\}$, а через $w(A)$ будем обозначать вес A, то есть $\sum_{x\in X} A(x)$. Для подмножества переменных $S \subseteq X$ будем обозначать через $w_S(A)$ вес A по S: $w_S(A) = \sum_{x\in S} A(x)$. Через $\mathrm{MAJ}_S(X)$ мы обозначаем функцию голосования на S: $\mathrm{MAJ}_S(X) = 1$ тогда и только тогда, когда $\sum_{x\in S} x \geqslant |S|/2$. В частности, MAJ_X — это просто MAJ_n.

Набор значений $A\colon X \to \{0,1\}$ мы называем *мин-термом* MAJ_n, если $\mathrm{MAJ}_n(A) = 1$, но смена значения одной переменной с 1 на 0 в A дает набор

A', такой что $\mathrm{MAJ}_n(A') = 0$. *Макс-термы* определяются симметрично со сменой ролей 0 и 1.

Для пороговой функции $f(X)$, задаваемой неравенством $\sum_{i=1}^{n} a_i x_i \geq t$, мы определяем величину $\mathrm{diff}(f, A) = \sum_{i=1}^{n} a_i A(x_i) - t$. В частности, $f(A) = 1$ тогда и только тогда, когда $\mathrm{diff}(f, A) \geq 0$.

Вероятностные неравенства

Нам потребуется следующая версия неравенства Чернова-Хефдинга (см., напр., [43]).

Лемма 6.1 (Неравенство Чернова-Хефдинга). *Пусть $Y = \sum_{i=1}^{m} Y_i$, где Y_i, $i \in [m]$ — независимые случайные величины над $[0, 1]$. Тогда для всякого $\epsilon > 0$, $\mathrm{Prob}[Y > (1+\epsilon)E[Y]], \mathrm{Prob}[Y < (1-\epsilon)E[Y]] \leqslant e^{-\frac{\epsilon^2}{3}E[Y]}$.*

Нам также потребуются некоторые факты о гипергеометрическом распределении. *Гипергеометрическое распределение $Y = K(m, t, k)$* определяется следующим образом. Рассмотрим множество S размера m и его подмножество S' размера k. Выберем (равновероятно) подмножество T размера t в S. Тогда случайная величина $|T \cap S'|$ имеет гипергеометрическое распределение $K(m, t, k)$. Величины m, t и k — параметры распределения.

Нам потребуются следующие стандартные технические факты об этих распределениях.

Лемма 6.2. *Пусть для гипергеометрического распределения выполняется $k = k(m) \leqslant m/2$ (то есть, k может зависеть от m). Пусть $t = t(m)$ — функция с $\epsilon m < t < (1-\epsilon)m$ для некоторой константы $0 < \epsilon < 1/2$. Рассмотрим произвольную антицепь $\mathcal{A}$ в S' (то есть, семейство подмножеств S', ни одно из которых не вложено в другое). Тогда*

$$\mathrm{Prob}\left[T \cap S' \in \mathcal{A}\right] = O(k^{-1/2}),$$

где $O(\cdot)$ — при $m \to \infty$ и константа в $O(\cdot)$ может зависеть от ϵ, но не зависит от m, t и k.

Лемма 6.3. *Для S, S' и T, удовлетворяющих условиям выше, верно*

$$\mathrm{Prob}\{|T \cap S'| \geq l\} \leq (tk/m)^l .$$

Доказательства этих леммы стандартные и технические. Полные доказательства можно найти [94].

6.2 Верхняя оценка для случая глубины 3

Для случая глубины 3 мы построим схему с $k = O(n^{2/3})$.

Теорема 6.1. *Для $k = O(n^{2/3})$ существует монотонная схема глубины 3, состоящая из функций голосования входной степени не больше k, вычисляющая функцию голосования от n переменных.*

Доказательство. Общий план доказательства таков. Сначала мы потратим один уровень схемы на то, чтобы немного структурировать входные биты. Затем мы разобьем входы на $O(n^{1/3})$ блоков и на следующем уровне вычислим некоторые функции голосования на каждом из блоков. Наконец, на последнем уровне схемы мы вычислим функцию голосования от предвычисленных на прошлом уровне поблочных функций. Мы докажем, что такая схема всегда дает правильный результат.

Перейдем к формальному доказательству. Разобьем множество входных переменных на $b = n^{1/3}/2^{1/3}$ блоков размера $p = 2^{1/3}n^{2/3}$ каждый: $X = X_1 \sqcup X_2 \sqcup \ldots \sqcup X_b$. Для каждого блока X_i вычислим $[\sum_{x \in X_i} x \geq k]$ для всех $k \in [p]$. Это задает первый слой нашей схемы. Выходы этих p элементов — это просто перестановка X_i, упорядочивающая биты X_i в убывающем порядке.

На выходе первого слоя мы вновь получили вектор длины n, обозначим его через Y. В нем такое же количество нулей и единиц, что и во входном наборе, но

в каждом блоке биты упорядочены по убыванию. На втором уровне мы вновь разбиваем Y на b блоков размера p: $Y = Y_1 \sqcup Y_2 \sqcup \ldots \sqcup Y_b$. Но теперь блок Y_i состоит из битов Y с номерами $i, i+b, i+2b, \ldots, i+(p-1)b$. Для каждого блока Y_i мы вычисляем $[\sum_{y \in Y_i} y \geq k]$ для всех $k \in [\frac{p}{2} - (\frac{n}{2})^{1/3}; \frac{p}{2} + (\frac{n}{2})^{1/3}]$. Таким образом, на втором уровне у нас будет $2^{2/3} n^{1/3}$ элементов для каждого из $b = n^{1/3}/2^{1/3}$ блоков, то есть всего $2^{1/3} n^{2/3}$ элементов. Наконец, на третьем уровне мы вычисляем функцию голосования от всех элементов на втором уровне.

Теперь нам нужно доказать, что эта схема вычисляет функцию голосования на любом наборе входных переменных. Поскольку и эта схема, и функция голосования монотонны, нам достаточно проверить, что схема вычисляет функцию корректно на всех мин-термах и макс-термах функции голосования (то есть на минимальных наборах, на которых функция выдает 1, и на максимальных наборах, на которых функция выдает 0).

Рассмотрим вход $A\colon X \to \{0,1\}$ с $w(A) = n/2$. Мы покажем, что для каждого блока Y_i,

$$w_{Y_i}(A) \in \left[\frac{p}{2} - \left(\frac{n}{2}\right)^{1/3}, \frac{p}{2} + \left(\frac{n}{2}\right)^{1/3} \right]. \tag{6.1}$$

Действительно, поскольку переменные в X_j упорядочены и мы включаем в Y_i каждую b-ю переменную каждого X_j, мы получаем

$$w(A) \in [w_{Y_i}(A) \cdot b - b^2, w_{Y_i}(A) \cdot b + b^2],$$

где в $\pm b^2$ первый множитель b соответствует ошибке в каждом блоке X_i, а второй множитель b соответствует количеству блоков $X_1, \ldots, X_b$. С другой стороны, мы знаем, что $w(A) = n/2$. Следовательно,

$$\frac{n}{2} \in [w_{Y_i}(A) \cdot b - b^2, w_{Y_i}(A) \cdot b + b^2],$$

откуда сразу следует (6.1). Далее, из (6.1) вытекает, что вычисление построенной схемы на A корректно. Действительно, по (6.1) в блоке Y_i в наборе A будет не меньше $(\frac{p}{2} - b)$ нулей и не меньше $(\frac{p}{2} - b)$ единиц. Это, в свою очередь, означает, что вычисление $[\sum_{y \in Y_i} y \geq k]$ только для средних значений k (а именно, для

$k \in [p/2 - b, p/2 + b]$), а не для всех $k \in [p]$, не меняет баланс нулей и единиц:

$$\mathrm{MAJ}\left(\left\{\left[\sum_{y\in Y_i} A(y) \geq k\right]\right\}_{k\in[p]}\right) = \mathrm{MAJ}\left(\left\{\left[\sum_{y\in Y_i} A(y) \geq k\right]\right\}_{k\in[p/2-b,p/2+b]}\right).$$

Если $w(A) = n/2 + O(1)$, то ясно, что достаточно посчитать на $O(1)$ больше элементов на втором уровне в каждом блоке и затем включить их в выходной элемент. ■

6.3 Нижние оценки

В этом разделе мы докажем нижнюю оценку на k для схем глубины 2, а также и для схем произвольной глубины d.

Теорема 6.2. *Пусть схема вида* $\mathrm{MAJ}_k \circ \mathrm{MAJ}_k$ *вычисляет функцию голосования* MAJ_n. *Тогда*

$$k = \Omega\left(n^{13/19} \cdot (\log n)^{-2/19}\right).$$

В общем виде, если MAJ_n *вычисляется схемой из* MAJ_k *глубины* d, *то*

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

Отметим, что в таких схемах элементы на нижних уровнях могут получать одну и ту же переменную несколько раз, за счет этого веса переменных могут быть больше 1.

Мы также докажем следующий результат в частном случае схем с ограниченными весами.

Теорема 6.3. *Пусть схема вида* $\mathrm{MAJ}_k \circ \mathrm{MAJ}_k$ *вычисляет* MAJ_n *и использует веса не больше* W *в своих элементах. Тогда*

$$k = \Omega(n^{7/10} \cdot (\log n)^{-1/5} \cdot W^{-3/10}).$$

В общем виде, если MAJ_n *вычисляется схемой из* MAJ_k *глубины* d *с весами не больше* W*, то*

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

В частности, мы получаем следующее следствие для схем с весами 1.

Следствие 6.4. *Пусть схема вида* $\mathrm{MAJ}_k \circ \mathrm{MAJ}_k$ *вычисляет* MAJ_n *и каждая переменная встречается в каждом элементе на нижнем уровне не больше одного раза. Тогда* $k = \Omega(n^{7/10} \cdot (\log n)^{-1/5})$.

В общем виде, если MAJ_n *вычисляется схемой из* MAJ_k *глубины* d *и каждая переменная встречается в каждом элементе на нижнем уровне не больше одного раза, то*

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

Отметим, что в работе [36] для глубины 2 и была доказана оценка $k = \Omega(\frac{n}{W})$, это лучше результата теоремы 6.3 для $W \leqslant n^{\frac{6}{19}}$ с точностью до логарифмических множителей.

Оставшаяся часть этого раздела посвящена общему доказательству этих оценок. Чтобы доказательство покрывало общий случай, мы будем рассматривать схемы глубины 2 такого вида: первый уровень состоит из элементов MAJ_k, а второй уровень содержит произвольную функцию от q переменных. Это позволит нам вывести нижние оценки для схем глубины d из нашего рассуждения. Хотя параметры k и q, вообще говоря, могут (и будут) варьироваться в широком диапазоне, при чтении доказательства удобно держать в голове случай $k = q = n^{\frac{2}{3}+\varepsilon}$ для некоторого маленького $\epsilon > 0$. Это хорошо отражает случай схем $\mathrm{MAJ}_k \circ \mathrm{MAJ}_k$, и в конце рассуждения действительно окажется, что в этом случае $k = q = n^{\frac{2}{3}+\varepsilon}$ для небольшого ϵ с точностью до полилогарифмического множителя. В доказательстве мы будем аккуратно проводить все вычисления в терминах параметров n, k и q, но мы также будем указывать все значения для случая $k = q = n^{2/3+\epsilon}$. Мы указываем эти значения, чтобы было проще следить за доказательством на идейном уровне.

Пусть F — схема, вычисляющая MAJ_n на всех входах из $\{0,1\}^n$. Обозначим через W максимальный вес переменной в элементах на нижнем уровне F.

Нормализация схемы

Мы начнем с нормализации F, то есть, удалим некоторые патологические элементы из F. Мы сделаем это в два последовательных этапа.

Этап 1: удаление элементов с высоким порогом. Нам потребуется, чтобы в схеме не было плохих элементов, которые можно сделать равными нулю, зафиксировав нулем небольшое число переменных (здесь и в дальнейшем мы рассматриваем элементы только с первого уровня схемы). Чтобы этого достичь, предположим, что в схеме есть элемент, который можно сделать равным нулю, зафиксировав нулем меньше $n/(100q) = n^{1/3-\epsilon}/100$ переменных. Рассмотрим эти переменные и зафиксируем их нулем; это обнуляет элемент, и мы можем удалить его из схемы (и возможно, что это также приводит к появлению новых элементов с тем же свойством). Мы повторяем этот процесс, пока плохие элементы не закончатся. Напомним, что число элементов на нижнем уровне не больше $q = n^{2/3+\epsilon}$, так что мы можем сделать не больше $q = n^{2/3+\epsilon}$ шагов в этом процессе, а следовательно, в результате n заменится на число, не меньшее чем $99n/100$. Мы доказываем оценку с точностью до мультипликативного множителя, так что для простоты изложения будем считать, что $|X| = n$, и что F не содержит плохих элементов.

Этап 2: удаление других патологических элементов и переменных. Формула F содержит не больше $kq = n^{\frac{4}{3}+2\epsilon}$ вхождений переменных (с учетом кратности). Пусть $x^* \in X$ — наименее часто встречающаяся в листьях формулы переменная. Тогда число вхождений x^* не больше $kq/n = n^{1/3+2\epsilon}$. В рассуждениях ниже нас будут интересовать макс-термы, фик-

сирующие x^* равной 0:

$$\mathcal{A}^* = \{A\colon X \to \{0,1\} \mid \operatorname{diff}(\mathrm{MAJ}_n, A) = -1 \text{ и } A(x^*) = 0\}\,.$$

Нас также будут интересовать элементы на нижнем уровне, зависящие от x^*, и только они. Обозначим их множество через $\mathcal{G}^*$ (следовательно, $|\mathcal{G}^*| \le kq/n = n^{1/3+2\epsilon}$). Общее количество переменных в элементах из $\mathcal{G}^*$ (с учетом кратности) не больше $k|\mathcal{G}^*| \le k^2q/n = n^{1+3\epsilon}$.

Теперь мы дополнительно упростим схему. Мы избавимся от следующих плохих элементов и переменных:

1. элементы в $\mathcal{G}^*$, которые можно сделать равными 1, зафиксировав меньше, чем $n^2/(100kq) = n^{2/3-2\epsilon}/100$ переменных in $X \setminus \{x^*\}$ равными 1;
2. элементы в $\mathcal{G}^*$ с весом переменной x^* больше $100k^2q/n^2 = 100n^{3\epsilon}$;
3. переменные с суммарным весом во всех элементах в $\mathcal{G}^*$ большим, чем $100k^2q/n^2 = 100n^{3\epsilon}$.

Мы делаем это с помощью следующей процедуры. Если на некотором шаге у нас есть элемент, подпадающий под условие пункта 1, мы фиксируем меньше, чем $n^2/(100kq) = n^{2/3-2\epsilon}/100$ переменных элемента среди $X \setminus \{x^*\}$ равными 1 так, чтобы этот элемент стал константой (и мы удалили его из схемы). Если у нас есть элемент, подпадающий под условия пункта 2, мы фиксируем все переменные элемента среди $X \setminus \{x^*\}$ равными 1, чтобы этот элемент стал константой. Если у нас есть переменная, подпадающая под условия пункта 3, мы фиксируем эту переменную единицей.

Заметим, что если мы зафиксируем все переменные в $G \in \mathcal{G}^*$, кроме x^*, равными 1, то элемент становится равным константе. Действительно, если он не константа, то элемент выдает 0 на входе с $x^* = 0$ и остальными переменными равными 1. В силу монотонности элемента, это означает, что элемент можно зафиксировать равным 0, зафиксировав одну переменную x^* равной 0, а мы

избавились от элементов с таким свойством на первом этапе нормализации схемы.

Поскольку всего элементов в $\mathcal{G}^*$ не больше $kq/n = n^{1/3+2\epsilon}$, мы зафиксируем не больше $n/100$ переменных в пункте 1. Поскольку суммарный вес x^* не больше $kq/n = n^{1/3+2\epsilon}$, пункт 2 произойдет не больше $n/(100k) = n^{1/3-\epsilon}/100$ раз. Поскольку каждый элемент имеет не больше $k = n^{2/3+\epsilon}$ переменных, мы зафиксируем не больше $n/100$ переменных по пункту 2. Поскольку суммарный вес всех переменных в $\mathcal{G}^*$ не больше $k^2q/n = n^{1+3\epsilon}$, мы зафиксируем не больше $n/100$ переменных по случае 3.

В частности, мы зафиксировали все переменные веса больше, чем

$$100k^2q/n^2 = 100n^{3\epsilon}$$

в каком-либо элементе $\mathcal{G}^*$, так что с этого момента мы можем считать, что $W \leqslant 100k^2q/n^2$.

Еще одно важное наблюдение состоит в том, что теперь у нас в каждом элементе не меньше $n^2/(100kq)$ входов. Иначе элемент подпадает под условие пункта 1 выше.

После этих процедур число переменных вместо n становится равным $97n/100$. Для простоты изложения мы вновь будем считать, что $|X| = n$ и схема F нормализована. Заметим, что после переопределения n, порог функции MAJ_n, которую мы вычисляем, может быть не равен $n/2$, а вместо этого равен cn для некоторой константы c близкой к $1/2$. Это не сказывается на вычислениях в дальнейшем доказательстве.

Анализ

Ключевая идея состоит в том, что если у нас есть вход $A \in \mathcal{A}^*$ с $\mathrm{diff}(\mathrm{MAJ}_n, A) = -1$, то существует элемент $G \in \mathcal{G}^*$ с $-W \leq \mathrm{diff}(G, A) \leqslant -1$. Действительно, иначе мы можем сменить значение переменной x^*, при этом

значение MAJ_n сменится, но значения всех элементов на нижнем уровне останется прежним. План доказательства состоит в том, чтобы построить вход, который нарушает это условие для некоторых значений параметров. Это даст нам ограничения на параметры схемы, что позволит доказать оценку.

Для входа $A \in \mathcal{A}^*$ с $\operatorname{diff}(\mathrm{MAJ}_n, A) = -1$ и целых параметров s и d (которые мы зафиксируем позже), рассмотрим следующую процедуру $\texttt{walk}(A, s, d)$.

1: $A_0 \leftarrow A$
2: **for** $i = 1$ to s **do**
3: **if** для всех $G \in \mathcal{G}^*$, $\operatorname{diff}(G, A_{i-1}) \notin \{-d, -d+1, \ldots, -1\}$ **then**
4: заканчиваем процедуру
5: **else**
6: $G_i \leftarrow$ любой элемент из $\mathcal{G}^*$, такой что $-d \leq \operatorname{diff}(G, A_{i-1}) < 0$
7: $X_i \leftarrow$ множество переменных, от которых зависит G_i, и которые равны 1 во входе A_{i-1}
8: $y_i \leftarrow$ случайная равновероятная переменная из X_i
9: $A_i \leftarrow$ значения X, получающиеся из A_{i-1} сменой значения у y_i
10: **end if**
11: **end for**

Ясно, что этот процесс уменьшает вес изначального входного набора A на 1 на каждой итерации в течение не более чем s итераций. В частности, $w(A) - w(A_i) = i$. Мы рассмотрим три случая.

Случай 1. *Существует входной набор $A \in \mathcal{A}^*$ с $\operatorname{diff}(\mathrm{MAJ}_n, A) = -1$, такой что $\texttt{walk}(A, s, d)$ останавливается после менее чем s итераций для какого-то выбора случайных битов. Это означает, что после $t < s$ итераций для каждого элемента G в $\mathcal{G}^*$ верно либо, что $\operatorname{diff}(G, A_t) < -d$, либо, что $\operatorname{diff}(G, A_t) \geqslant 0$.*

Выберем случайное подмножество T, состоящее из t переменных из $Z = \{x \in X \setminus \{x^*\} \colon A_t(x) = 0\}$ и сменим их значение на противоположное. Обозначим получившейся входной набор через A'. Ясно, что $w(A) = w(A')$, а зна-

чит $\mathrm{diff}(\mathrm{MAJ}_n, A') = -1$. Следовательно, должен существовать элемент G в $\mathcal{G}^*$, такой что $-W \leqslant \mathrm{diff}(G, A') < 0$. Таким образом, до смены значений t случайных переменных, все элементы с отрицательным отклонением имеют отклонение меньшее, чем $-d$, тогда как после смены значений переменных хотя бы один элемент G имеет отрицательное отклонение, не меньшее $-W$. Пусть $Z' = \{x \in X(G) \setminus \{x^*\} \colon A_t(x) = 0\}$. Это означает, что смена значений переменных меняет значение не менее чем $r = (d - W)/W$ переменных G, то есть $|T \cap Z'| \geq r$.

Пусть p — вероятность того, что $|T \cap Z'| \geq r$, где вероятность берется по случайному выбору T. Подбирая параметры s и d, мы сделаем p достаточно маленьким, чтобы с ненулевой вероятностью ни для одного элемента из $\mathcal{G}^*$ это неравенство не выполнялось. В силу рассуждения выше, это приводит к противоречию, поскольку смена значения x^* меняет значение функции, но не меняет значение схемы. Вероятность того, что ни один элемент из $\mathcal{G}^*$ не удовлетворяет $|T \cap Z'| \geq r$, не меньше $1 - |\mathcal{G}^*|p$. Вероятность p можно оценить сверху: пользуясь леммой 6.3: $p \leq \left(\frac{t|Z'|}{|Z|}\right)^r \leq \left(\frac{sk}{n/2}\right)^r$, где второе неравенство следует из того, что $t < s$, $|Z'| \leqslant k$ и $|Z| \geqslant \frac{n}{2}$.

Мы хотим, чтобы вероятность $1 - |\mathcal{G}^*|p$ была положительна. Поскольку $|\mathcal{G}^*| \leq kq/n = n^{1/3+2\epsilon}$, мы получаем следующее неравенство на s, d, и k: $(kq/n)\cdot(2sk/n)^r < 1$. Мы выполним это неравенство, если $sk < n/4$ и $r \geqslant \log \frac{kq}{n}$. Поскольку в конце у нам будет выполняться $\log n > \log \frac{kq}{n}$, для второго неравенства достаточно, чтобы

$$d = W \log n. \tag{6.2}$$

В итоге, этот случай накладывает следующее ограничение на параметры:

$$sk \leq n/4\,. \tag{6.3}$$

Случай 2. *Для всякого входного набора $A \in \mathcal{A}^*$ (то есть, с $\mathrm{diff}(\mathrm{MAJ}_n, A) = -1$) процедура $\mathtt{walk}(A, s, d)$ проходит все s итераций для всех выборов случайных битов.*

Мы рассмотрим два подслучая.

Случай 2.1. *Для всякого входного набора* $A \in \mathcal{A}^*$ *(то есть, с* $\mathrm{diff}(\mathrm{MAJ}_n, A) = -1$*) существует выбор переменных* $y_1, \ldots, y_s$ *в строке 8 процедуры* $\texttt{walk}(A, s, d)$*, такой что для всякого элемента* $G \in \{G_1, \ldots, G_s\}$ *(напомним, что элементы* $G_1, \ldots, G_s$ *выбираются в строке 6 процедуры) верно* $\mathrm{diff}(G, A) \leqslant f$*, где* f *— еще один положительный параметр, который мы зафиксируем позже.*

Мы оценим ожидаемое число E элементов G из $\mathcal{G}^*$, для которых $-d \leqslant \mathrm{diff}(G, A) \leqslant f$, где матожидание берется по случайному выбору A. Заметим, что конкретный элемент $G \in \mathcal{G}^*$ может встретиться в последовательности $G_1, \ldots, G_s$ не больше d раз: первый раз, когда он встречается, должно выполняться $\mathrm{diff}(G, A_1) \leqslant -1$ для текущего набора A_1, в следующий раз должно выполняться $\mathrm{diff}(G, A_2) \leqslant -2$ для нового текущего набора A_2 и так далее. Если $Ed < s$, мы получаем противоречие: рассмотрим набор $A \in \mathcal{A}^*$ с $\mathrm{diff}(\mathrm{MAJ}_n, A) = -1$, такой что количество элементов G в $\mathcal{G}^*$ с $-d \leqslant \mathrm{diff}(G, A) \leqslant f$ не больше E, тогда невозможно, чтобы для всех $G_1, \ldots, G_s$ выполнялось $-d \leqslant \mathrm{diff}(G_i, A) \leqslant f$, у нас просто недостаточно элементов с таким отклонением.

Теперь оценим E сверху. Поскольку схема нормализована, каждый конкретный элемент содержит не меньше $n^2/(100kq) = n^{2/3-2\epsilon}/100$ переменных. Заметим, что множество входов B в элемент G, для которых $\mathrm{diff}(G, B) = i$ для всякого i образует антицепь. Тогда по лемме 6.2 вероятность того, что значение отклонения равно конкретному значению, не больше $O(\sqrt{kq}/n) = O(1/n^{1/3-\epsilon})$.

Следовательно,

$$E \leq |\mathcal{G}^*| \cdot (f+d) \cdot O\left(\frac{\sqrt{kq}}{n}\right) = \frac{kq}{n} \cdot (f+d) \cdot O\left(\frac{\sqrt{kq}}{n}\right) = O\left(\frac{(kq)^{3/2}(f+d)}{n^2}\right) = O\left(\frac{(kq)^{3/2} f}{n^2}\right),$$

где для последнего равенства мы добавляем ограничение

$$d = O(f)\,. \tag{6.4}$$

Мы получаем следующее ограничение на параметры в этом случае:

$$O\left(\frac{(kq)^{3/2} f d}{n^2}\right) = O(f d n^{3\epsilon}) < s\,. \tag{6.5}$$

Случай 2.2. *Существует входной набор $A \in \mathcal{A}^*$ (то есть, с $\mathrm{diff}(\mathrm{MAJ}_n, A) = -1$), такой что для всякого выбора переменных $y_1, \ldots, y_s$, хотя бы для одного элемента $G \in \{G_1, \ldots, G_s\}$ верно $\mathrm{diff}(G, A) > f$.*

Зафиксируем элемент $G \in \mathcal{G}^*$ с $\mathrm{diff}(G, A) > f$. Мы докажем верхнюю оценку на вероятность (по случайному выбору переменных $y_1, \ldots, y_s$) того, что G встречается среди $G_1, \ldots, G_s$ в нашей процедуре. Если эта вероятность меньше $1/l$, где через l мы обозначим число рассматриваемых элементов, то, оценивая вероятность объединения событий через сумму вероятностей, мы получим, что с положительной вероятностью ни один такой элемент не встречается среди $G_1, \ldots, G_s$, что дает противоречие с формулировкой этого случая.

Для того, чтобы G встретился среди $G_1, \ldots, G_s$, мы должны были выбрать переменную из G в строке 8 в нашем процессе много раз. Действительно, если G встречается в процессе, то его отклонение на текущем наборе отрицательно. В то же время, в начале процесса $\mathrm{diff}(G, A) > f$. Каждый раз, когда процесс уменьшает переменную в строке 8 (то есть, изменяет ее значение с 1 на 0), значение линейной функции, вычисляемой в G, уменьшается не больше чем на W (просто потому что W — максимальный вес переменной во всех элементах в $\mathcal{G}^*$). Таким образом, достаточно оценить сверху вероятность того, что для фиксированного элемента $G \in \mathcal{G}^*$ с $\mathrm{diff}(G, A) > f$, процесс выберет переменную из $X(G)$ не меньше f/W раз.

Пусть $Y_1, \ldots, Y_s$ — случайные переменные, принимающие значения в $\{0, 1\}$, определяемые следующим образом: $Y_i = 1$ тогда и только тогда, когда i-я уменьшаемая переменная входит в G (то есть, $y_i \in X(G)$). Пусть $Y = \sum_{i=1}^{s} Y_i$. Наша цель — оценить сверху $\mathrm{Prob}(Y \geq f/W)$.

Пусть $H_1, \ldots, H_{l'}$ — множество всех элементов, имеющих хотя бы одну общую переменную с G. Пусть на шаге j мы уменьшаем переменную из H_i. Тогда

$$\mathrm{Prob}\,[Y_j = 1] = \mathrm{Prob}\,[y_i \in X(G)] \leqslant \frac{|X(G) \cap X(H_i)|}{|\{x \in X(H_i)\colon A_{j-1}(x) = 1\}|}\,.$$

В силу шага 2.1 нормализации схемы,

$$|\{x \in X(H_i)\colon A_{j-1}(x) = 1\}| \geq \frac{n^2}{100kq} - d\,.$$

Чтобы убедиться в этом, предположим противное. Напомним, что

$$-d \leq \mathrm{diff}(H_i, A_{j-1}) < 0\,.$$

Это означает, что увеличив не больше d переменных (то есть, изменив их значение с 0 на 1) из $X(H_i)$ в наборе A_{j-1}, мы получим набор веса не больше $\frac{n^2}{100kq}$, который фиксирует H_i равным 1. А это противоречит нормализованности схемы.

Таким образом,

$$\mathrm{Prob}(Y_j = 1) \leq \frac{|X(G) \cap X(H_i)|}{\frac{n^2}{100kq} - d} \leq \frac{|X(G) \cap X(H_i)|}{\frac{n^2}{200kq}}\,,$$

где мы добавили ограничение

$$d \leq \frac{n^2}{200kq}\,. \tag{6.6}$$

Теперь мы используем факт, что переменные в процессе могут выбираться из фиксированного элемента H_i не больше d раз. Мы оценим сверху сумму $Y = \sum_{i=1}^{s} Y_i$ следующей случайной величиной: $Z = \sum_{i=1}^{l'} \sum_{j=1}^{d} Z_{ij}$, где каждая Z_{ij} – случайная величина, принимающая значения $\{0, 1\}$, такая что

$$\mathrm{Prob}\,[Z_{ij} = 1] = \frac{|X(G) \cap X(H_i)|}{\frac{n^2}{200kq}}\,,$$

и Z_{ij} независимы. То есть, вместо того, чтобы уменьшать переменные в каких-то H_i в каком-то случайном порядке, мы уменьшаем d переменных в каждом

H_i. Таким образом, мы уменьшаем максимально возможное число переменных во всех элементах. Ясно, что для всякого r верно $\mathrm{Prob}\,[Y \geqslant r] \leqslant \mathrm{Prob}\,[Z \geqslant r]$.

Оценим матожидание Z. Поскольку в силу нормализации схемы всякая переменная G встречается в остальных элементах не больше $100k^2q/n^2 = 100n^{3\epsilon}$ раз, мы получаем

$$\sum_{i,j} |X(G) \cap X(H_i)| \leqslant d \cdot (100k^2q/n^2) \cdot |X(G)| \leqslant 100 \cdot n^{2/3+4\epsilon} \cdot W \cdot \log n.$$

В итоге, мы получаем, что

$$EZ \leqslant \frac{100dk^3q/n^2}{n^2/200kq} = 2 \cdot 10^4 \cdot d\frac{k^4q^2}{n^4} = 2 \cdot 10^4 \cdot n^{6\epsilon} \cdot W \cdot \log n\,.$$

Применяя неравенство Чернова-Хефдинга (лемма 6.1), мы сразу получаем, что вероятность того, что Z в два раза больше своего матожидания, экспоненциально мала по $d \cdot \frac{k^4q^2}{n^4}$. После фиксации значений параметров окажется, что

$$d \cdot \frac{k^4q^2}{n^4} = W \cdot \log n \cdot n^{9\epsilon} \tag{6.7}$$

растет асимптотически быстрее, чем $\log n$. Так что мы получаем, что $\mathrm{Prob}(Z \geq 2 \cdot EZ) < \frac{1}{l}$. Следовательно, если $f/W \geq 2 \cdot EZ$, то

$$\mathrm{Prob}\,[Y \geq f/W] \leq \mathrm{Prob}\,[Z \geq 2 \cdot EZ] < \frac{1}{l},$$

что и требовалось. Этот случай дает следующее ограничение на параметры:

$$f \geqslant 4 \cdot 10^4 \cdot d \cdot W \cdot \frac{k^4q^2}{n^4} = 4 \cdot 10^4 \cdot n^{9\epsilon} \cdot W^2 \cdot \log n\,. \tag{6.8}$$

Подбор параметров

Нам остается зафиксировать параметры так, чтобы условия (6.2)–(6.8) выполнялись и k было максимально возможным. Неравенство (6.5) дает нижнюю оценку на s в терминах f, тогда как (6.8) дает нижнюю оценку на f. Из этих двух неравенств мы получаем нижнюю оценку на s:

$$s \geqslant C \cdot \frac{k^{11/2}q^{7/2}}{n^6} \cdot W^3 \cdot \log^2 n$$

для некоторой положительной константы C. Комбинируя это с верхней оценкой на s из (6.3) и обращая все неравенства в равенства, мы можем задать следующее уравнение на k, q и n:

$$\frac{n}{4k} = C \cdot \frac{k^{11/2} q^{7/2}}{n^6} \cdot W^3 \cdot \log^2 n \,. \tag{6.9}$$

Докажем, что остальные ограничения также выполняются. С точностью до логарифмических по n множителей мы получаем

$$n^7 = \widetilde{O}\left(k^{\frac{13}{2}} q^{\frac{7}{2}} W^3\right) = \widetilde{O}\left((k^{\frac{14}{2}} q^{\frac{7}{2}} W^{\frac{7}{2}})/(k^{\frac{1}{2}} W^{\frac{1}{2}})\right).$$

Поскольку во всех рассматриваемых нами случаях выполняется $q = k^c$ для некоторой константы c, мы получаем, что

$$n^{2+\epsilon} = \widetilde{O}(k^2 q W)$$

Для некоторого положительного ϵ. Вспоминая, что $W \leqslant 100k^2 q/n^2$, можно заключить, что

$$n^{2+\epsilon/2} = \widetilde{O}(k^2 q). \tag{6.10}$$

Из этого и из (6.8) вытекает, что выполняется ограничение (6.4). Также отсюда вытекает, что функция в (6.7) действительно растет сверхлогарифмически.

Далее, из (6.10), в частности, следует, что $\frac{n}{kq^{1/2}} = \widetilde{O}(\frac{1}{n^{\epsilon/4}})$. Так что из (6.9) можно получить, что с точностью до логарифмических по n множителей выполняется

$$W^3 = \widetilde{O}\left(\frac{n^7}{k^{13/2} q^{7/2}}\right) = \widetilde{O}\left(\frac{n^6}{k^3 q^3} \cdot \frac{1}{k^{5/2}} \cdot \frac{1}{n^{\epsilon/4}}\right).$$

Отсюда и из (6.2) нетрудно увидеть, что соотношение (6.6) также выполняется. Таким образом, мы зафиксировали параметры так, чтобы выполнялись все условия леммы.

Теперь мы можем вывести из проведенного анализа результаты этого раздела. Для схем вида $\mathrm{MAJ}_k \circ \mathrm{MAJ}_k$ у нас $k = q$, и из (6.9) мы получаем

$$k = \Omega\left(\frac{n^{7/10}}{(\log n)^{1/5} W^{3/10}}\right).$$

Для случая схем глубины d из функций голосования от k переменных, мы имеем, что $q = k^{d-1}$, и из (6.9) мы получаем

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

Это дает доказательство теоремы 6.3. Для $W = 1$, мы получаем, что

$$k = \Omega\left(n^{7/10} \cdot (\log n)^{-1/5}\right)$$

для схем глубины 2 и

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

для схем глубины d, что дает доказательство следствия 6.4.

Для неограниченного W напомним, что мы можем предполагать, что $W \leqslant \frac{100k^2q}{n^2}$. Таким образом,

$$k = \Omega\left(n^{13/19} \cdot (\log n)^{-2/19}\right)$$

для схем глубины 2 и

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

для произвольного d, что дает доказательство теоремы 6.2.

Глава 7

Базы данных, снабженные логическими теориями

В этой главе мы докажем результаты о гиперграфовых программах. Мы начнем с мотивации, определим базы данных с онтологическим доступом, опишем их связь с гиперграфовыми программами, и лишь затем перейдем к результатам о самих гиперграфовых программах.

В этой главе вектора переменных нам удобно будет обозначать через $\vec{x}$.

7.1 Теории, запросы и их преобразования

Под базой данных мы будем понимать теорию логики первого порядка. Эта теория не произвольна и обязана удовлетворять ряду ограничений, которые мы приведем ниже. Одновременно с описанием определений и базовых фактов мы будем пояснять стоящую за ними интуицию.

Во-первых, для описание структуры данных нам нужно зафиксировать множество предикатных символов (которые мы для краткости будем называть просто предикатами) в сигнатуре. Неформально, они соответствуют типам информации, содержащейся в структуре данных. Мы предполагаем, что в сигнатуре присутствуют только унарные и бинарные предикаты[1]. Сами данные представляют собой набор объектов и информации о них. Объекты в базе данных соответствуют константам в сигнатуре. Информация в базе данных соответ-

[1]Если в базе данных присутствуют также предикаты большей арности, их можно выразить через бинарные. Есть несколько разных способов это делать, об этом можно прочитать в [91].

ствует замкнутым атомарным формулам, то есть предикатам, примененным к константам. Множество этих атомарных формул образует теорию, соответствующую совокупности данных в базе. Мы обозначаем получившееся множество формул через D, а множество констант в сигнатуре — через Δ_D. Мы обозначаем сигнатуру (множество предикатных символов и констант) через Σ.

Таким образом, мы перевели описание базы данных на язык логики. Чтобы получить базу данных, снабженную логической теорией, мы добавляем к D более сложные формулы логики первого порядка. Множество этих новых формул мы будем обозначать через T и будем называть *онтологией* или просто логической теорией. Мы опишем, какие именно формулы могут встречаться в T немного позже. Теория $D \cup T$ как раз и называется базой данных, снабженной логической теорией, или *базой знаний*. Предикатные символы и теория T определяют структуру базы знаний, и таким образом будут зафиксированы. Константы Δ_D и атомарные формулы D, напротив, определяют текущее наполнение базы данных, то есть сами данные, так что они будут меняться.

Стандартным видом запросов в этой области являются конъюнктивные запросы. То есть, запрос — это формула вида

$$q(\vec{x}) = \exists \vec{y} \phi(\vec{x}, \vec{y}),$$

где ϕ — это конъюнкция атомарных формул (или для краткости, атомов). Мы будем рассматривать только такие виды запросов. Напомним, что через $\vec{x}$ и $\vec{y}$ мы обозначаем наборы переменных. Для простоты изложения мы будем предполагать, что q не содержит констант из Δ_D (в действительности, все построения проходят и без этого предположения [22]).

Что означает, что на запрос есть ответ в случае стандартной базы данных без онтологии? Это означает, что существуют значения $\vec{x}$ и $\vec{y}$ среди Δ_D, такие что запрос становится истинен на этих наборах в D. То есть, мы можем рассмотреть модель I_D, соответствующую данным D. Элементами этой модели I_D являются константы в Δ_D, а значения предикатов на I_D задаются формулами в D. То

есть, предикат $P \in \Sigma$ истинен на $\vec{a}$ из Δ_D тогда и только тогда, когда $P(\vec{a}) \in D$. Набор элементов $\vec{a}$ из I_D является *ответом* на запрос $q(\vec{x})$, если

$$I_D \models \exists \vec{y} \phi(\vec{a}, \vec{y}).$$

Вернемся к нашей постановке задачи. Теперь мы рассматриваем (возможно, неполные) данные, снабженные логической теорией. Это означает, что теперь нам не дана конкретная модель. Вместо этого нам дана теория $D \cup T$, и мы должны проверить, выполняется ли запрос в этой теории. То есть, нас интересует следующая задача: по данной базе знаний $D \cup T$ и запросу $q(\vec{x})$ найти $\vec{a}$ в Δ_D, такой что

$$D \cup T \models q(\vec{a}).$$

Если $\vec{x}$ — пустой набор переменных, то ответом на запрос будет являться «да» или «нет». В этом случае мы называем запрос *булевым*.

Основной подход в этой области к решению задачи поиска ответа на запрос состоит в том, чтобы сначала преобразовать запрос к такому виду, чтобы ответ на новый запрос не зависел от теории T, а затем применить технику, разработанную для стандартных баз данных. Это приводит нас к следующему определению. Формула первого порядка $q'(\vec{x})$ называется *преобразованием* запроса $q(\vec{x})$ относительно теории T, если

$$D \cup T \models q(\vec{a}) \;\Leftrightarrow\; I_D \models q'(\vec{a}) \tag{7.1}$$

для всех D и всех $\vec{a}$. Подчеркнем, что в левой части равносильности (7.1) символ '$\models$' означает логическое следование из теории, тогда как в правой части он означает истинность в модели.

Также отметим, что в (7.1) зафиксированы только предикатные символы в Σ и теория T. Теория D (а следовательно, и множество констант в сигнатуре) могут меняться, и преобразование должно работать сразу для всех D. Неформально, это означает, что структура данных зафиксирована заранее и известна, а конкретное текущее наполнение базы знаний может меняться. Мы требуем,

чтобы преобразование (а значит и весь подход к задаче поиска ответа на запрос) работало независимо от того, как меняются данные.

Чему соответствует модель теории $D \cup T$ на неформальном уровне? Поскольку данные D не предполагаются полными, I_D не обязательно является моделью этой теории. Вместо этого модель соответствует содержанию полных данных, отвечающему «реальности», дополняющему данные D. Мы предполагаем, что все формулы теории выполняются в модели, то есть, вся информация в базе знаний (включая формулы в T) корректна.

Однако, если мы допустим использование слишком сильных формул в онтологии, то может случиться, что преобразование запроса не существует, а задача поиска ответа на запрос может оказаться алгоритмически неразрешимой. Так что нам придется допускать в T только очень ограниченные формулы. С другой стороны, для практических целей в области исследования баз знаний также достаточно уже очень простых формул.

Есть несколько конкретных стандартных наборов ограничений на теории в базах знаний [99,33,9,29,13,30,31]. Мы будем использовать такой набор ограничений, который покрывает и обобщает большинство самых популярных стандартных наборов ограничений. Таким образом, наши нижние оценки будут также верны и для этих стандартных постановок. Что касается верхних оценок, мы не будем подробно о них говорить, но отметим, что они выполняются также и для существенно более сильных теорий и, в том числе, покрывают язык OWL 2 QL [99].

Формулы в теории T у нас будут ограничены следующим видом:

$$\forall x(\phi(x) \to \exists y \psi(x, y)), \tag{7.2}$$

где x и y — отдельные переменные, ϕ — унарный предикат, а $\psi(x, y)$ — конъюнкция атомарных формул.

Оказывается, что если T состоит только из формул вида (7.2), то преобразование запросов всегда возможно. Неформальная причина для этого состоит

в том, что в этом случае всегда есть универсальная модель M_D для данных D и T.

Теорема 7.1 ([56]). *Для всех теорий D и T, удовлетворяющих ограничениям, описанным выше, существует модель M_D, такая что*

$$D \cup T \models q(\vec{a}) \;\Leftrightarrow\; M_D \models q(\vec{a})$$

для всех конъюнктивных запросов q и всякого $\vec{a}$ в Δ_D.

Замечание 7.1. *Заметим, что модель M_D в действительности зависит как от D, так и от T. Мы не указываем T в нижним индексе, поскольку в интересующей нас постановке T фиксировано, а D меняется.*

Неформальный смысл этой теоремы состоит в том, что для теорий T, удовлетворяющих (7.2), всегда существует самая общая модель. Более формально, для любой другой модели M теории $D \cup T$ существует гомоморфизм из универсальной модели M_D в M. Для полноты изложения и для лучшего понимания происходящего мы приводим идею доказательства этой теоремы. Для нас будет полезно увидеть, как строится модель M_D.

Идея доказательства. Неформальная идея доказательства существования универсальной модели состоит в том, что мы можем построить ее из констант, представленных в данных D. А именно, сначала добавим в M_D все константы из Δ_D и положим все атомарные формулы из D истинными на этих константах. Далее, из теории T может следовать, что некоторые другие предикаты должны выполняться на некоторых элементах Δ_D. Мы также полагаем их истинными в M_D. Что более важно, из формул в T может также следовать существование новых элементов, связанных с константами (формула (7.2) говорит, что для элемента x, удовлетворяющего $\varphi(x)$, существует новый элемент y). Мы добавляем эти новые элементы в модель и распространяем предикаты на них, выводя все, что следует из T. Далее, из формул T может следовать существование новых

элементов, связанных с теми, которые были получены на предыдущем шаге. Мы продолжаем добавлять их в модель. Нетрудно доказать, что получившаяся (возможно, бесконечная) модель действительно является универсальной моделью. Полное формальное доказательство можно найти в [56]. ■

Таким образом, вместо рассмотрения запроса q над $D \cup T$ мы можем рассматривать его над M_D. Это наблюдение помогает изучать преобразования запросов.

Полезно рассмотреть граф (возможно, бесконечный), соответствующий модели M_D. Вершинами графа являются элементы модели, и мы проводим ориентированное ребро из элемента m_1 в элемент m_2, если существует бинарный предикат P, такой что $M_D \models P(m_1, m_2)$. Мы помечаем ребро метками P и P^-. Метки второго типа означают, что выполняется $P(m_2, m_1)$. Таким образом, мы проводим между вершинами ориентированное ребро только в одну сторону и проставляем все метки на нем. Тогда в процессе, описанном в доказательстве выше, мы начинаем с графа на константах из Δ_D и затем добавляем новые вершины, существование которых следует из T. Заметим, что посылка в формуле (7.2) состоит из унарного предиката. Это означает, что существование нового элемента в модели вытекает исключительно из выполнения унарного предиката на одной из уже построенных вершин. Таким образом, для каждой новой вершины модели мы можем проследить путь ее возникновения последовательно вершина за вершиной, пока не дойдем до константы a нашей теории и одной из атомарных формул $B(a) \in D$. Длина этого пути называется глубиной вершины.

Максимальное (по всем D) число шагов последовательного добавления новых элементов в модель называется *глубиной* теории T. То есть, глубина теории, это максимальная глубина добавленных вершин. Этот параметр будет для нас важен. Заметим, что как M_D, так и глубина теории T могут быть бесконечными.

В дальнейшем нам будет важно для всякого унарного предиката $A \in \Sigma$ рассматривать универсальную модель M_D теории $D = \{A(a)\}$. Универсальная модель для произвольной D на самом деле «собирается» из этих простых универсальных моделей. Мы кратко будем обозначать эту модель через M_A (вместо $M_{\{A(a)\}}$) и называть ее *универсальным деревом*, порожденным A. Вершина a в соответствующем графе называется *корнем* универсального дерева. Все остальные вершины дерева называются *внутренними вершинами*. Слово «дерево» в названии модели объясняется тем, что граф, соответствующий M_A, во всех интересных случаях (в частности, во всех наших конструкциях) является деревом, хотя это верно и не во всех случаях. Более точно, этот граф может быть не деревом, если какая-то из формул (7.2) в T не содержит бинарного предиката вида $R(x, y)$ или $R(y, x)$.

Пример 7.1. *Чтобы проиллюстрировать основные введенные понятия, рассмотрим следующую теорию T, описывающую часть структуры организации курсовых работ студентов:*

$$\forall x \left(\mathit{Студент}(x) \to \exists y \left(\mathit{РаботаетНад}(x, y) \wedge \mathit{Курсовая}(y)\right)\right),$$
$$\forall x \left(\mathit{Курсовая}(x) \to \exists y \left(\mathit{ПодРуководством}(x, y) \wedge \mathit{Преподаватель}(y)\right)\right),$$
$$\forall x, y \left(\mathit{РаботаетНад}(x, y) \to \mathit{Задействован}(x, y)\right),$$
$$\forall x, y \left(\mathit{ПодРуководством}(x, y) \to \mathit{Задействован}(y, x)\right).$$

Некоторые формулы в этой теории имеют другую форму по сравнению с (7.2) *(из-за последних двух формул), но это для нас не важно. Более того, нетрудно видеть, что эту теорию можно преобразовать в форму* (7.2) *(с небольшими изменениями в данных).*

Рассмотрим запрос $q(x)$, спрашивающий о тех, кто работает под руководством преподавателя:

$$q(x) = \exists y, z \left(\mathit{РаботаетНад}(x, y) \wedge \mathit{Задействован}(z, y) \wedge \mathit{Преподаватель}(z)\right). \tag{7.3}$$

Нетрудно проверить, что следующая формула является преобразованием q:

$$\begin{aligned} q'(x) \quad = \quad & \exists y, z \left[\mathit{РаботаетНад}(x, y) \wedge \right. \\ & \big(\mathit{РаботаетНад}(z, y) \vee \mathit{ПодРуководством}(y, z) \vee \mathit{Задействован}(z, y) \big) \wedge \\ & \qquad\qquad\qquad\qquad \left. \mathit{Преподаватель}(z) \right] \vee \\ \exists y \left[\mathit{РаботаетНад}(x, y) \wedge \mathit{Курсовая}(y) \right] \quad \vee \quad & \mathit{Студент}(x). \end{aligned}$$

То есть, для любых данных D и произвольной константы a в D верно

$$D \cup T \models q(a) \;\Leftrightarrow\; I_D \models q'(a).$$

Для иллюстрации понятия универсальной модели рассмотрим такие данные:

$$D = \big\{ \mathit{Студент}(c),\ \mathit{РаботаетНад}(c, b),\ \mathit{Курсовая}(b),\ \mathit{ПодРуководством}(b, a) \big\}.$$

Универсальная модель M_D представлена на рис. 7.1. Область слева соответствует данным D, область справа сверху соответствует универсальному дереву, порожденному предикатом $\mathit{Курсовая}(b)$, а область справа снизу соответствует универсальному дереву, порожденному $\mathit{Студент}(c)$. Напомним, что метка вида P^- на ребре, где P — предикат сигнатуры, означает, что выполняется предикат P для переставленных местами переменных. В этом примере глубина теории равна 2.

Заметим, что для нашего запроса $q(x)$ оказывается, что $q(c)$ следует из $D \cup T$, и можно увидеть, что $q(c)$ верно в M_D. Заметим, однако, что $q(c)$ не верно в D в силу неполноты данных D: в данных неизвестно, что a — преподаватель.

Из конструкции универсальной модели также нетрудно увидеть, как именно мы построили преобразование запроса: по сути мы просто перебрали все случаи означивания переменных под кванторами элементами универсальных деревьев.

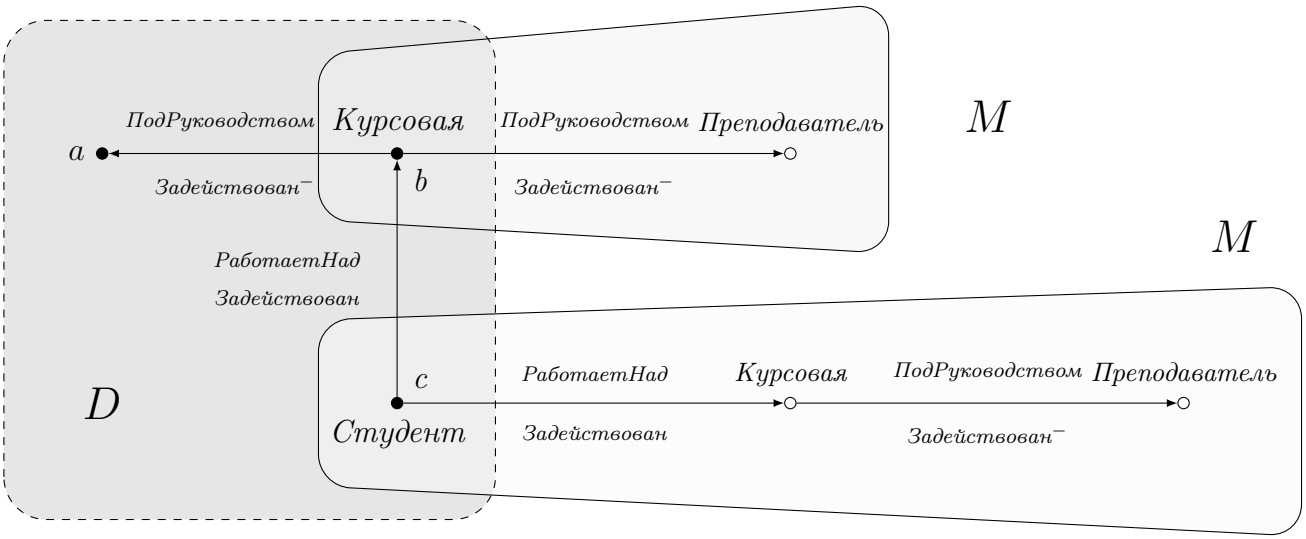


Рисунок 7.1: Пример универсальной модели.

Из существования универсальной модели (и простоты ее структуры) можно вывести, что для всякого q существует преобразование запроса q' в форме (предваренной кванторами существования) дизъюнкции конъюнкций атомарных формул. Однако, нетрудно привести пример, для которого это преобразование имеет экспоненциально больший размер по сравнению с q (см. [56]). Под *размером* преобразования мы понимаем число символов в формуле.

Для построения более коротких преобразований полезно рассматривать более широкие классы формул. Естественным выбором является рассмотрение произвольных формул первого порядка в качестве преобразований запросов. Такой тип преобразований называется преобразованиями первого порядка или FO-преобразованиями. Другой естественный вариант — это позитивно-экзистенциальные преобразования или PE-преобразования. Это специальный класс FO-преобразований, в котором не используются отрицания и разрешаются только кванторы существования. PE-преобразования более предпочтительны по сравнению с FO-преобразованиями, поскольку с ними значительно проще работать алгоритмическими методами, разработанными для обычных баз данных. Под размерами PE- или FO-преобразования мы будем понимать число символов в этих формулах.

Еще один стандартный тип преобразования — это нерекурсивные datalog преобразования или NDL-преобразования. Эти преобразования не имеют вид формул логики первого порядка, а вместо этого имеют вид схемного представления формул первого порядка. Более конкретно, *NDL-преобразование* состоит из множества Π формул вида

$$\forall \vec{x} \, (A_1 \wedge \ldots \wedge A_n \to A_0) \, ,$$

где A_i — это атомарные формулы (возможно, новые, не представленные в сигнатуре Σ), не обязательно арности 1 или 2. Каждый A_i зависит от (некоторых) переменных из $\vec{x}$, и каждая переменная A_0 должна встречаться и в $A_1 \wedge \ldots \wedge A_n$. Наконец, мы требуем ацикличности Π. Чтобы ее определить, рассмотрим ориентированный граф, вершинами которого являются предикаты A формул множества Π, и мы проводим ребро из A в B тогда и только тогда, когда существует формула в Π, такая что B находится в правой части, а A содержится в левой. И тогда Π называется *ациклическим*, если получившийся граф является ациклическим. Также в NDL-преобразовании указывается целевой предикат G, и мы говорим, что $\vec{a}$ из Δ_D выполняет (Π, G) над данными D тогда и только тогда, когда

$$D \cup \Pi \models G(\vec{a}).$$

Таким образом, (Π, G) называется NDL-преобразованием запроса q, если

$$D \cup T \models q(\vec{a}) \;\; \Leftrightarrow \;\; D \cup \Pi \models G(\vec{a})$$

для всех D и всех $\vec{a}$. *Размером* NDL-преобразования (Π, G) называется число символов в нем.

Пример 7.2. *Для иллюстрации понятия NDL-преобразования мы приводим преобразование запроса q из примера 7.1:*

$$\forall y, z\,(\mathit{РаботаетНад}(z, y) \to N_1(y, z))\,,$$
$$\forall y, z\,(\mathit{ПодРуководством}(y, z) \to N_1(y, z))\,,$$
$$\forall y, z\,(\mathit{Задействован}(z, y) \to N_1(y, z))\,,$$
$$\forall x, y, z\,(\mathit{РаботаетНад}(x, y) \wedge N_1(y, z) \wedge \mathit{Преподаватель}(z) \to G(x))\,,$$
$$\forall x, y\,(\mathit{РаботаетНад}(x, y) \wedge \mathit{Курсовая}(y) \to G(x))\,,$$
$$\forall x\,(\mathit{Студент}(x) \to G(x))\,,$$

где N_1 — новый бинарный предикат, а G — целевой предикат этого NDL-преобразования.

Нетрудно видеть, что это преобразование похоже на PE-преобразование q' из примера 7.1. Действительно, $N_1(y, z)$ эквивалентно подформуле

$$\big(\mathit{РаботаетНад}(z, y) \vee \mathit{ПодРуководством}(y, z) \vee \mathit{Задействован}(z, y)\big)$$

из q', а $G(x)$ эквивалентен самой $q'(x)$.

Оказывается, что NDL-преобразования являются более общими, чем PE-преобразования. Действительно, PE-преобразование q' имеет вид $\exists\vec{y}\phi(\vec{x}, \vec{y})$, где ϕ — монотонная булева формула, примененная к атомарным формулам (заметим, что кванторы существования можно вынести в начало, поскольку в формуле нет отрицаний). Формулы в Π могут моделировать операции $\vee$ и $\wedge$, как в примере выше, и таким образом могут промоделировать всю формулу ϕ. Для этого для каждой подформулы ϕ мы можем ввести новый предикатный символ, который зависит от всех переменных, от которых зависит эта подформула. Мы моделируем операции $\vee$ и $\wedge$ на подформулах одну за другой. В конце мы получаем атомарную формулу $F(\vec{x}, \vec{y})$. Наконец, мы добавляем в Π формулу

$$\forall\vec{x}, \vec{y}\ \big(F(\vec{x}, \vec{y}) \to G(\vec{x})\big). \tag{7.4}$$

Тогда мы получаем, что для любых $\vec{a}, \vec{b}$ формула $\phi(\vec{a}, \vec{b})$ истинна в D тогда и только тогда, когда $F(\vec{a}, \vec{b})$ истинна в $D \cup \Pi$. Наконец, $\exists \vec{y} \phi(\vec{a}, \vec{y})$ истинна в D тогда и только тогда, когда существует набор констант $\vec{b}$, такой что $\phi(\vec{a}, \vec{b})$ истинна. С другой стороны, в Π мы можем вывести $G(\vec{a})$ тогда и только тогда, когда существует $\vec{b}$, такой что $F(\vec{a}, \vec{b})$ истинна. Таким образом, по данному PE-преобразованию мы можем построить NDL-преобразование примерно такого же размера. С другой стороны, не исключено, что существуют NDL-преобразования меньшие, чем самые маленькие PE-преобразования: NDL-преобразования могут переиспользовать некоторые свои предикаты несколько раз.

Неизвестно, есть ли соотношения между NDL-преобразованиями и FO-преобразованиями. С одной стороны, NDL-преобразования имеют структуру, похожую на структуру булевых схем, а FO-преобразования имеют структуру, похожую на структуру булевых формул. С другой стороны, FO-преобразования могут использовать отрицания, а NDL-преобразования монотонны.

Как мы упоминали выше, мы будем рассматривать только конъюнктивные запросы $q(x)$ к базам данных, снабженным логическими теориями. Однако, во многих случаях запросы имеют даже более простую структуру. Чтобы описать ограниченные классы запросов, рассмотрим граф, соответствующий запросу. Вершинами графа являются переменные, встречающиеся в q. Две вершины соединены тогда и только тогда, когда соответствующие переменные встречаются в одной атомарной формуле в q. Если этот граф является деревом, мы говорим что запрос *древесный*. Если граф является путем, мы говорим, что запрос *линейный*.

7.2 Нижние оценки размера преобразований: общий подход

В этом разделе мы опишем общую идею, стоящую за доказательствами нижних оценок на размер преобразований запросов.

Очень неформально, мы кодируем булевы функции внутри запросов таким образом, чтобы преобразования соответствовали булевым схемам, вычисляющим эти функции. Если нам удастся закодировать достаточно трудные функции, то для них не будет булевых схем небольшого размера, а значит, не будет маленьких преобразований для соответствующих запросов.

Как именно мы кодируем функции в запросах? Во-первых, мы ограничимся данными D с только одной константой a. Это существенное ограничение на данные. Но поскольку наше преобразование должно работать для всех данных, и мы доказываем нижние оценки, это ограничение может только осложнить нашу задачу. С другой стороны, это ограничение делает наши оценки более общими.

Далее мы вводим несколько предикатов $A_1, A_2, \ldots, A_n$ и рассматриваем формулы $A_i(a)$. Эти предикаты будут соответствовать переменным $x_1, \ldots, x_n$ кодируемой функции f: переменная x_i истинна тогда и только тогда, когда $A_i(a) \in D$. У нас будут и другие предикаты в сигнатуре, а также другие формулы в D. Их роль будет в том, чтобы гарантировать, что

$$D \cup T \models q(x)$$

тогда и только тогда, когда кодируемая функция f истинна на соответствующем входе.

Этот подход позволяет нам описать выразительную способность различных типов запросов и теорий. Результаты собраны в таблице 7.1.

Столбцы таблицы соответствуют классам теорий T. Строки таблицы соответствуют классам запросов q. В ячейке таблицы мы указываем класс функций,

	глубина 1	глубина $d > 1$	произвольная глубина
линейные запросы	$\leqslant \mathsf{AC}^0_4$	$\mathsf{NL}/\mathrm{poly}$	$\mathsf{NL}/\mathrm{poly}$
древесные запросы	$\leqslant \mathsf{AC}^0_4$	SAC^1	$\mathsf{NP}/\mathrm{poly}$ [56]
произвольные запросы	$\mathsf{NL}/\mathrm{poly}$	$\mathsf{NP}/\mathrm{poly}$	$\mathsf{NP}/\mathrm{poly}$ [56]

Таблица 7.1: Функции, кодируемые запросами и теориями.

который может быть закодирован запросами и теориями этих типов. Результаты в таблице дают как верхние, так и нижние оценки. Однако, в дальнейшем мы будем говорить о нижних оценках, поскольку нас интересует то, как закодировать трудные функции, и мы не будем обсуждать вопрос о том, почему более трудные функции не могут быть закодированы.

Далее, нам нужно рассмотреть преобразование одного из описанных выше типов и получить из него соответствующую вычислительную модель, вычисляющую f. Этот переход достаточно интуитивно понятен: преобразования имеют структуру, очень похожую на некоторые классы булевых схем. А именно, FO-преобразования похожи на булевы формулы, PE-преобразования похожи на монотонные булевы формулы, а NDL-преобразования похожи на монотонные булевы схемы. Таким образом, существование FO-преобразований полиномиального размера означает, что f лежит в NC^1, существование PE-преобразований полиномиального размера означает, что f лежит в mNC^1, а существование NDL-преобразований полиномиального размера означает, что f лежит в $\mathsf{mP}/\mathrm{poly}$. Мы опускаем доказательства этих сведений. Подробности можно найти в [22].

Вместе с таблицей выше это дает полный спектр результатов о размерах преобразований. Нам достаточно лишь использовать результаты о соотношениях между соответствующими сложностными классами. Например, в случае теорий глубины 1 и линейных или древесных запросов существуют полиномиальные преобразования всех трех типов. В случае теорий глубины 2 и линейных или древесных запросов не всегда существуют полиномиальные

PE-преобразования, не всегда существуют полиномиальные FO-преобразования при условии выполнения соответствующих стандартных предположений о соотношении некоторых сложностных классов, но всегда существуют полиномиальные NDL-преобразования. В случае теорий глубины 2 и произвольных запросов не всегда существуют полиномиальные PE- и NDL-преобразования и не всегда существуют полиномиальные FO-преобразования при условии выполнения соответствующих предположений о соотношении сложностных классов.

Ниже мы приводим дальнейшие подробности доказательств упомянутых результатов. Результаты из статьи [56] (произвольная глубина теорий, древовидные и произвольные запросы) были доказаны с помощью некоторой отдельной конструкции. Остальные результаты в таблице 7.1 доказываются с помощью общего подхода, связанного с моделью гиперграфовых программ. Отметим, что нижняя оценка в левом нижнем нижнем углу таблицы вытекает также и из результатов, полученных с помощью гиперграфовых программы (а именно, из результата для теорий ограниченной глубины и произвольных запросов). В следующем разделе мы перейдем к обсуждению этой модели. После этого мы подробно опишем результаты о сложности гиперграфовых программ.

7.3 Гиперграфовые програмы: связь с преобразованиями запросов

В этом разделе нам потребуется понятие гиперграфа. *Гиперграфом* H называется пара конечных множеств (V, E), где V — множество *вершин*, а E — семейство подмножеств V. Элементы E называются *гиперребрами*. *Степенью* вершины называется число гиперребер, содержащих эту вершину. Пара гиперребер называется непересекающейся, если они не пересекаются как множества. Множество гиперребер называется *непересекающимся*, если они попарно не пересекаются.

Для простоты изложения мы ограничимся лишь булевыми запросами. Рассмотрим запрос $q = \exists \vec{y} \phi(\vec{y})$ и рассмотрим соответствующий граф G. Вершины графа G соответствуют переменным q. Если в запросе есть бинарный предикат, связывающий две переменные, мы проводим между ними одно ориентированное ребро с метками P и P^- для всех предикатов, связывающих эти вершины (мы выбираем метку P или P^- в зависимости от того, совпадает ли направление ребра с порядком вхождения переменных в предикат). Также каждая вершина v помечена A, если $A(v)$ лежит в q.

Рассмотрим данные D. Мы можем построить универсальную модель M_D, просто добавив универсальные деревья к каждому элементу D. Рассмотрим, как запрос может выполняться элементами универсальной модели. Для этого нам нужно, чтобы для каждой переменной t запроса мы нашли соответствующий элемент в M_D, удовлетворяющий всем свойствам t, указанным в запросе. Этот элемент M_D может быть как элементом данных D, так и элементом универсального дерева.

Таким образом, чтобы запрос q был выполнен, нужно, чтобы он вкладывался в универсальную модель. То есть, нужно отобразить вершины G в вершины универсальной модели M_D так, чтобы для каждой метки в G была соответствующая метка в M_D. Мы называем такое вложение *гомоморфизмом*.

Теперь посмотрим, как вершина v графа G может отображаться во внутренний элемент w универсального дерева R. Это означает, что для всех меток v вершина w в универсальном дереве R должна иметь такие же метки и для всех смежных с v ребер должны быть соответствующие ребра, смежные с w в универсальном дереве. Следовательно, все смежные с v вершины должны также отображаться в универсальное дерево R. Мы можем повторить это рассуждение для соседей v и продолжать до тех пор, пока мы не достигнем вершин G, отображающихся в корень R. Таким образом, если одна из вершин G вкладывается в универсальное дерево R, то туда же вкладывается некоторое множество близ-

ких вершин. Граница этого множества вершин должна отображаться в корень универсального дерева.

Подытожим, что мы получили к настоящему моменту. Ответ на (булев) запрос соответствует существованию вложения G в универсальную модель M_D. Есть связные подграфы в G, которые отображаются в универсальные деревья. Границы этих подграфов (вершины, соединенные с внешними по отношению к подграфу вершинами) отображаются в корни универсальных деревьев. Два подграфа могут пересекаться только по граничным вершинам. Эти подграфы мы называем *свидетелями*.

При данном запросе мы можем рассмотреть всех потенциальных свидетелей в нем, то есть все подграфы, которые могут отобразиться в какие-нибудь универсальные деревья. Для любых данных D ответ на запрос положителен, если мы можем отобразить запрос в универсальную модель M_D. Такое отображение существует, если мы можем найти множество непересекающихся свидетелей, таких что мы можем отобразить все остальные вершины в D, а свидетелей — в соответствующие универсальные деревья.

Для нижних оценок нам будет достаточно рассмотреть D с единственным элементом a. Таким образом, D состоит из формул вида $A(a)$ и $P(a, a)$. Чтобы понять, положителен ли ответ на запрос, нам нужно проверить, существует ли множество свидетелей, которые не пересекаются (кроме как по граничным вершинам), и такие что все вершины G, кроме внутренних вершин свидетелей, могут быть отображены в a. Рассмотрим следующий гиперграф H: в нем есть по вершине для каждой вершины графа G и для каждого ребра графа G; для каждого свидетеля есть гиперребро в H, состоящее из вершин, соответствующих внутренним вершинам свидетеля, и вершин, соответствующих ребрам свидетеля. Для каждой вершины v гиперграфа H введем булеву переменную x_v и для каждого гиперребра e гиперграфа H введем булеву переменную x_e. Для данного D (с одним элементом a) положим x_v равным 1 тогда и только тогда, когда v может быть отображена в a, и положим x_e равным 1 тогда и

только тогда, когда унарный предикат, порождающий свидетеля, соответствующего гиперребру e, верен в a. Из рассуждения выше следует, что ответ на запрос положителен для данного D тогда и только тогда, когда существует подмножество непересекающихся гиперребер, для которых $x_e = 1$, и которые содержат все вершины с $x_v = 0$.

Это приводит нас к следующему определению.

Определение 7.1 (Гиперграфовая программа). *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 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. В этом случае мы будем писать $P(\vec{x}) = 1$. Гиперграфовая программа вычисляет булеву функцию $f\colon \{0,1\}^n \to \{0,1\}$ тогда и только тогда, когда для всех $\vec{x} \in \{0,1\}^n$ верно, что $P(\vec{x}) = f(\vec{x})$. 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.*

Замечание 7.2. *Заметим, что в обсуждении выше мы получили несколько другую модель. А именно, в ней также есть переменные, связанные с гиперребрами в гиперграфе. Заметим, однако, что наше определение также покрывает эту расширенную модель. Действительно, мы можем для каждого гиперребра e добавить пару новых вершин v_e и u_e и новое гиперребро e'. Мы добавляем v_e в гиперребро e и мы полагаем $e' = \{v_e, u_e\}$. Метку v_e полагаем равной 1, а метку u_e — равной переменной x_e. Легко видеть, что $x_e = 0$ тогда и только тогда, когда мы не можем использовать гиперребро e в нашем покрытии.*

Мы обсудили (без подробностей и неформально), как кодировать булевы функции с помощью запросов и теорий. Мы заметили, что получившаяся функция вычисляется гиперграфовой программой. Обозначим через HGP класс функций, вычислимых гиперграфовыми программами полиномиального размера (напомним, что в действительности мы рассматриваем последовательности функций и последовательности программ).

Различные ограничения на запросы и теории дают ограничения на получающиеся гиперграфовые программы. Если теория имеет глубину 1, то каждый свидетель имеет одну внутреннюю вершину, и каждое гиперребро состоит из вершины, соответствующей внутренней вершине свидетеля, и всех вершин, соответствующих смежным с ней ребрам. Таким образом, два различных гиперребра могут пересекаться только по одной вершине, соответствующей ребру G. Это происходит в том случае, если вершины этих гиперребер, соответствующие внутренним вершинам свидетеля, смежны в G. В частности, каждая вершина, соответствующая ребру G, может встречаться только в двух гиперребрах, и результирующий гиперграф имеет степень не больше 2. Мы обозначаем через HGP_k множество функций, вычислимых гиперграфовыми программами полиномиального размера степени не больше k.

Если запрос древесный (или линейный), то гиперграфовая программа будет в своей основе иметь древесную (или линейную) структуру и все гиперребра будут поддеревьями (подпутями). Мы обозначаем через HGP^{tree} (HGP^{path}) множество всех функций, вычислимых гиперграфовыми программами полиномиального размера, имеющими в своей основе древесную (линейную) структуру.

Однако, чтобы соответствие запросов и теорий гиперграфовым программам было универсальным, нам нужно показать, что *любая* гиперграфовая программа в соответствующем классе может быть закодирована запросом и теорией соответствующих типов. Каждое такое утверждение доказывается отдельной конструкцией, эти доказательства можно найти в [85, 23, 22].

Гиперграфовые программы	Классы схем/программ
$\mathsf{HGP} = \mathsf{HGP}_3$	$\mathsf{NP}/\mathrm{poly}$
HGP_2	$\mathsf{coNBP} = \mathsf{coNL}/\mathrm{poly}$
HGP^{path}	$\mathsf{NBP} = \mathsf{NL}/\mathrm{poly}$
HGP^{tree}	SAC^1
$\mathsf{HGP}_2^{tree} = \mathsf{HGP}_2^{path}$	$\mathsf{AC}^0_{3,\mathrm{AND}}$

Таблица 7.2: Выразительная способность гиперграфовых программ.

Замечание 7.3. *Отметим, что подход с гиперграфовыми программами работает не во всех упомянутых нами постановках задач. А именно, нижние оценки в [56] получены существенно другой конструкцией, и это важно. Дело в том, что гиперграфы, соответствующие запросам и теориям, построенным в этой работе, имеют экспоненциальное число ребер. Однако, подход с гиперграфами дает оптимальные результаты во всех остальных рассматриваемых постановках.*

7.4 Гиперграфовые программы: сложность

Мы обсудили, что гиперграфовые программы можно кодировать в запросах и теориях. Теперь нам нужно показать, что есть трудные функции, вычислимые гиперграфовыми программами. Для этого мы установим вычислительную силу гиперграфовых программ разных типов в терминах других моделей вычисления. Тогда существование трудных функций, вычислимых гиперграфовыми программами, будет следовать из известных результатов в теории сложности вычислений.

Мы приводим результаты о сложности гиперграфовых программ в таблице 7.2.

В левом столбце таблицы мы перечисляем классы гиперграфовых программ, а в правом — эквивалентный класс булевых схем или ветвящихся программ. Все результаты также переносятся на монотонный случай.

Обратим внимание, что для второй строки таблицы известно, что в немонотонном случае $\mathsf{NL}/\mathrm{poly} = \mathsf{coNL}/\mathrm{poly}$ [124, 77]. Однако, в монотонном случае это равенство не выполняется (см. [58]). Так что мы предпочли оставить coNL в таблице.

Вместе с рассуждениями двух предыдущих разделов, результаты этой таблицы позволяют заполнить таблицу 7.1 и доказать нижние оценки на размеры преобразований для рассматриваемых видов теорий и запросов. Отметим только, что неоптимальным получается переход от гиперграфовых программ к запросам и теориям в случае теорий глубины 1 и линейных и древовидных запросов. Здесь переходе мы теряем глубину 1 в схеме.

Ниже мы приводим доказательства всех результатов в таблице 7.2.

7.4.1 Произвольные гиперграфовые программы HGP

В этом разделе мы приводим доказательство следующей теоремы.

Теорема 7.2. *Выполняются следующие равенства* $\mathsf{HGP} = \mathsf{HGP}_3 = \mathsf{NP}/poly$. *Такие же равенства выполняется и в монотонном случае.*

Доказательство. Мы проведем доказательство в общем случае, и будет видно, что то же самое доказательство работает и в монотонном случае.

Очевидно, $\mathsf{HGP}_3 \subseteq \mathsf{HGP}$.

Далее, покажем, что $\mathsf{HGP} \subseteq \mathsf{NP}/\mathrm{poly}$. Рассмотрим гиперграфовую программу размера m с переменными $\vec{x}$. Мы построим схему $C(\vec{x}, \vec{y})$ размера $\mathrm{poly}(m)$, удовлетворяющую (1.1), для функции f, вычисляемой гиперграфовой программой. Ее $\vec{x}$-переменные, — это в точности переменные программы, а переменные сертификата $\vec{y}$ соответствуют гиперребрам программы. Схема C выдает 1 на

$(\vec{x}, \vec{y})$ тогда и только тогда, когда семейство $\{e \mid y_e = 1\}$ гиперребер в гиперграфе образует непересекающееся семейство гиперребер, покрывающее все вершины, метки которых принимают значение 0 при означивании вектором $\vec{x}$. Нетрудно построить полиномиальную схему, проверяющую это свойство. Действительно, для каждой пары пересекающихся гиперребер (e, e') достаточно вычислить $\neg y_e \vee \neg y_{e'}$, и для каждой вершины v гиперграфа с меткой t, содержащейся в гиперребрах $e_1, \ldots, e_k$, достаточно вычислить $t \vee y_{e_1} \vee \cdots \vee y_{e_k}$. После этого остается посчитать AND этих дизъюнкций. Легко видеть, что эта конструкция работает и в монотонном случае (заметим, что применение отрицаний к $\vec{y}$-переменным в монотонном варианте $\mathsf{NP}/\mathrm{poly}$ разрешается).

Теперь мы покажем, что $\mathsf{NP}/\mathrm{poly} \subseteq \mathsf{HGP}_3$. Рассмотрим функцию $f \in \mathsf{NP}/\mathrm{poly}$ и рассмотрим схему $C(\vec{x}, \vec{y})$, удовлетворяющую (1.1). Пусть $g_1, \ldots, g_s$ — элементы схемы C (включая переменные $\vec{x}$ и $\vec{y}$), и g_s — выходной элемент схемы. Мы построим гиперграфовую программу степени $\leqslant 3$, вычисляющую f, полиномиального размера от размера C. Для каждого i мы добавляем в программу вершину g_i с меткой 0 и пару гиперребер $\bar{e}_{g_i}$ и e_{g_i}, в которые мы включаем g_i. Никакие другие гиперребра не содержат вершину g_i, так что либо $\bar{e}_{g_i}$, либо e_{g_i} должно присутствовать в покрытии нулей гиперграфовой программы. Интуитивно, если элемент схемы g_i принимает значение 1, то e_{g_i} будет лежать в покрытии, иначе в покрытии будет лежать $\bar{e}_{g_i}$. Чтобы гарантировать это свойство для входных переменных x_i, мы добавляем в e_{x_i} новую вершину v_i, помеченную $\neg x_i$, и добавляем в $\bar{e}_{x_i}$ новую вершину u_i, помеченную x_i. Для элементов g_i, не являющихся переменными, мы рассматриваем три случая.

— Если $g_i = \neg g_j$, то мы добавляем вершину, помеченную 1, в e_{g_i} и e_{g_j}, и добавляем вершину, помеченную 1, в $\bar{e}_{g_i}$ и $\bar{e}_{g_j}$. Ясно, что это гарантирует, что если e_{g_j} лежит в покрытии, то $\bar{e}_{g_i}$ также должно лежать в покрытии, а если $\bar{e}_{g_j}$ лежит в покрытии, то e_{g_i} также должно лежать в покрытии.

— Если $g_i = g_j \vee g_{j'}$, то мы добавляем вершину, помеченную 1, в e_{g_j} и $\bar{e}_{g_i}$, и добавляем вершину, помеченную 1, в $e_{g_{j'}}$ и $\bar{e}_{g_i}$. Это гарантирует, что если e_{g_j} или $e_{g_{j'}}$ лежат в покрытии, то $\bar{e}_{g_i}$ не может лежать в покрытии, а значит, e_{g_i} должно лежать в покрытии. Далее, мы добавляем вершины h_j и $h_{j'}$, помеченные 1, в $\bar{e}_{g_j}$ и $\bar{e}_{g_{j'}}$ соответственно и вершину w_i, помеченную 0, в $\bar{e}_{g_i}$; наконец, мы добавляем гиперребра $\{h_j, w_i\}$ и $\{h_{j'}, w_i\}$. Если одно из гиперребер $\bar{e}_{g_j}$ и $\bar{e}_{g_{j'}}$ не лежит в покрытии, то мы покроем w_i соответствующим ребром $\{h_j, w_i\}$ или $\{h_{j'}, w_i\}$. Иначе нам придется покрывать ее гиперребром $\bar{e}_{g_i}$. Это гарантирует нужное нам свойство в этом случае.

— Если $g_i = g_j \wedge g_{j'}$, мы используем двойственную конструкцию.

Наконец, мы добавляем еще одну вершину, помеченную 0, в e_{g_s} для выходного элемента g_s схемы C. Это добавляет ограничение, что гиперребро e_{g_s} должно лежать в покрытии, что означает, что схема выдает 1. Индукцией по числу элементов схемы несложно показать, что для всякого $\vec{x}$ существует $\vec{y}$, такой что $C(\vec{x}, \vec{y}) = 1$, тогда и только тогда, когда построенная гиперграфовая программа выдает 1 на $\vec{x}$.

Для монотонного случая мы удаляем вершины, помеченные $\neg x_i$. Легко увидеть, что на входе $\vec{x}$ существует покрытие всех нулей в получившейся программе тогда и только тогда, когда существуют $\vec{y}$ и $\vec{x}' \leqslant \vec{x}$ с $C(\vec{x}', \vec{y}) = 1$. В силу монотонности C по $\vec{x}$ это означает, что существует покрытие всех нулей тогда и только тогда, когда существует $\vec{y}$, такой что $C(\vec{x}, \vec{y}) = 1$. ■

7.4.2 Гиперграфовые программы степени 2

В этом разделе мы докажем следующую теорему.

Теорема 7.3. *Выполняется равенство* $\mathsf{HGP}_2 = \mathsf{coNL}/poly$. *Такое же равенство верно и для монотонного случая.*

Доказательство. Начнем со включения $\mathsf{coNL/poly} \subseteq \mathsf{HGP}^2$. Пусть $\neg f$ вычисляется недетерминированной ветвящейся программой B. Мы построим гиперграфовую программу P, вычисляющую f, степени 2 и полиномиального размера от размера B. Для всякого ребра e в B добавим в гиперграфовую программу P две вершины e^0 и e^1, соответствующие началу и концу e соответственно. Вершина e^0 помечена отрицанием метки e в B, а e^1 помечена единицей. Для каждого ребра e в B, добавим в P гиперребро $\{e^0, e^1\}$. Такие гиперребра будем называть e-гиперребрами. Для всякой вершины v в B, кроме s и t, добавим в P гиперребро, состоящее из всех вершин e^1 для ребер e, входящих в v, и всех вершин e^0 для ребер e, исходящих из v. Такие гиперребра будем называть v-гиперребрами. Мы также добавляем в P вершину w с меткой 0 и гиперребро $\bar{e}_w$, состоящее из w, всех вершин e^1 для ребер e в B, ведущих в t. Мы утверждаем, что P вычисляет f. Действительно, если при заданном $\vec{x}$ в B нет пути из s в t, то следующее непересекающееся семейство гиперребер покрывает все вершины с нулевыми метками: все e-гиперребра, для ребер e, достижимых из s и с меткой 1 в B, все v-гиперребра для v недостижимых из s, а также гиперребро $\bar{e}_w$. В другую сторону, если при заданном $\vec{x}$ в B есть путь из s в t, то для всякого ребра e этого пути можно последовательно доказать, что соответствующие e-гиперребра должны входить в покрытие. А тогда никакое покрытие не может покрыть w, метка которой равна 0.

Теперь докажем, что $\mathsf{HGP}_2 \subseteq \mathsf{coNL/poly}$. Сначала покажем, что по гиперграфовой программе степени 2 можно построить эквивалентную программу, степени всех вершин в которой равны 2. Рассмотрим гиперграфовую программу P степени 2, вычисляющую f. Мы дополняем гиперграф тремя вершинами x, y и z, помеченными метками 1, 0 и 0 соответственно, и тремя гиперребрами $e_1 = \{v_1, \ldots, v_l, x, y\}$, $e_2 = \{v_1, \ldots, v_k, x, z\}$ и $e_3 = \{y, z\}$, где $v_1, \ldots, v_k$ — это вершины степени 0, а $v_{k+1}, \ldots, v_l$ — вершины степени 1.

Легко видеть, что каждое покрытие нулевых меток должно содержать e_3 и не может содержать e_1 и e_2. Действительно, y и z обе должны быть покрыты.

Однако, гиперребра e_1 и e_2 пересекаются и не могут быть взяты в покрытие одновременно. Так что y и z должны быть покрыты гиперребром e_3, а e_1 и e_2 не могут попасть в покрытие, поскольку пересекаются с e_3. После решения вопроса с гиперребрами e_1, e_2 и e_3 мы остаемся с изначальным гиперграфом.

Пусть f вычисляется гиперграфовой программой P с гиперребрами $e_1, \ldots, e_k$, в которой все степени вершин равны 2. Сначала мы дадим описание всех покрытий нулей непересекающимися гиперребрами в терминах графов, основываясь на графе следований [11]. Для всякого гиперребра e_i, рассмотрим булеву переменную u_i и с каждым входным набором $\vec{x}$ сопоставим следующий набор $\Phi_{\vec{x}}$ дизъюнктов. Для каждой пары i, j мы включаем дизъюнкт $\neg u_i \vee \neg u_j$, если $e_i \cap e_j \neq \emptyset$, а также дизъюнкт $u_i \vee u_j$, если есть $v \in e_i \cap e_j$, метка которой равна нулю при данном $\vec{x}$.

Неформально, первое означает, что пересекающиеся гиперребра не могут быть выбраны в покрытие одновременно, а второе означает, что все нулевые метки должны быть покрыты. Нетрудно видеть, что покрытия всех нулевых меток соответствуют выполняющим наборам для $\Phi_{\vec{x}}$. Пусть $C_{\vec{x}} = (V, E_{\vec{x}})$ — *граф следований* для $\Phi_{\vec{x}}$, то есть ориентированный граф с литералами $\Phi_{\vec{x}}$ в качестве вершин $V = \left\{u_i, \bar{u}_i \mid 1 \leqslant i \leqslant k\right\}$ и со следующим множеством ребер. Мы проводим ребро $(u_i, \bar{u}_j)$, если $\neg u_i \vee \neg u_j$ входит в $\Phi_{\vec{x}}$, и мы проводим ребро $(\bar{u}_i, u_j)$, если $u_i \vee u_j$ входит в $\Phi_{\vec{x}}$. То есть, ребра графа соответствуют следованиям из нашего набора дизъюнктов, например, дизъюнкт $\neg u_i \vee \neg u_j$ в $\Phi_{\vec{x}}$ влечет две импликации: $u_i \to \neg u_j$ и $u_j \to \neg u_i$, так что мы добавляем два соответствующих ребра. Аналогично для дизъюнков $u_i \vee u_j$.

По доказанному в [11, Теорема 1], $\Phi_{\vec{x}}$ выполнимо тогда и только тогда, когда в построенном графе нет (ориентированных) циклов, проходящих через некоторые вершины u_i и $\bar{u}_i$.

Теперь закодируем графы $C_{\vec{x}}$ для всех наборов $\vec{x}$ в одном размеченном графе C. Вершинами C являются вершины u_i и $\bar{u}_i$ для $1 \leqslant i \leqslant k$, а также дополни-

тельные вершины w_{ij}^v для $1 \leqslant i, j \leqslant k$ и $v \in e_i \cap e_j$. Ребрами C являются ребра $(u_i, \bar{u}_j)$ для $e_i \cap e_j \neq \emptyset$ и ребра $(\bar{u}_i, w_{ij}^v)$ и (w_{ij}^v, u_j) для каждого v в $e_i \cap e_j \neq \emptyset$.

Ребра вида $(u_i, \bar{u}_j)$ и $(\bar{u}_i, w_{ij}^v)$ помечены единицей, а ребра вида (w_{ij}^v, u_j) имеют метку, равную отрицанию метки v в P. Интуитивно, мы размножили ребра второго типа в $C_{\vec{x}}$, чтобы сделать отдельный путь для каждого v в пересечении. Нетрудно видеть, что в $C_{\vec{x}}$ есть цикл, проходящий через u_i и $\bar{u}_i$ тогда и только тогда, когда в C есть оба пути из $\bar{u}_i$ в u_i и из u_i в $\bar{u}_i$, проходящие по ребрам с метками равными 1 при фиксированном $\vec{x}$.

Теперь мы готовы построить ветвящуюся программу B. Она будет содержать две вершины s и t, а также для всякого гиперребра e_i в P мы добавим в B две копии C_i^0 и C_i^1 графа C с дополнительными ребрами из s в $\bar{u}_i$ в графе C_i^0, из u_i в графе C_i^0 в u_i в графе C_i^1 и из $\bar{u}_i$ в графе C_i^1 в t. Все метки дополнительных ребер равны 1. Мы получаем, что на наборе $\vec{x}$ есть путь из s в t тогда и только тогда, когда $C_{\vec{x}}$ содержит цикл через u_i и $\bar{u}_i$ для некоторого гиперребра e_i в P. Таким образом, B вычисляет $\neg f$, что и требовалось.

Нетрудно видеть, что все конструкции переносятся на монотонный случай: по монотонной ветвящейся программе для f мы получаем монотонную гиперграфовую программу для f^* и наоборот. ■

7.4.3 Линейные HGP

Теорема 7.4. *Выполняется следующее равенство* $\mathsf{HGP}^{path} = \mathsf{NL}/poly$. *Аналогичное утверждение верно и для монотонного случая.*

Доказательство. Рассмотрим линейную гиперграфовую программу P с вершинами $v_1, \ldots, v_n$ (в таком порядке). Все гиперребра P имеют вид $[v_i, v_{i+m}] = \{v_i, \ldots, v_{i+m}\}$ для некоторых $1 \leqslant i \leqslant n$ и $m \geqslant 0$. Добавим две новые вершины v_0 и v_{n+1} в P с метками 0 и добавим в P два дополнительных гиперребра $s = \{v_0\}$ и $t = \{v_{n+1}\}$. Ясно, что получившаяся программа эквивалентна изначальной.

Теперь построим ветвящуюся программу B, эквивалентную P. Вершинами P будут гиперребра P, и мы соединяем ребром гиперребра $e_i = [v_{i_1}, v_{i_2}]$ и $e_j = [v_{j_1}, v_{j_2}]$ тогда и только тогда, когда $i_2 < j_1$; меткой этого ребра будет конъюнкция меток всех вершин P с номерами большими i_2 и меньшими j_1 (временно разрешим использовать конъюнкции литералов в качестве меток). Нетрудно видеть, что для данного набора входных переменных есть путь из s в t в B тогда и только тогда, когда есть покрытие нулевых меток в P. Чтобы избавиться от конъюнкций в метках, просто заменим каждое ребро в B на цепочку ребер и расставим литералы из конъюнкции по меткам этих новых ребер.

В обратную сторону, пусть функция f вычисляется ветвящейся программой B с ориентированным графом с вершинами $V = \{v_1, \ldots, v_n\}$ и ребрами $E = \{e_1, \ldots, e_m\}$, где $s = v_1$ и $t = v_n$. Без ограничения общности будет считать, что в B есть петля на вершине t с меткой 1. Тогда, если существует пусть из s в t с метками, равными 1, то также существует и путь с тем же свойством длины $n - 1$.

Построим линейную гиперграфовую программу P для f. Ее вершины будут разбиты на n вершинных блоков $VB^1, \ldots, VB^n$ и $n - 1$ реберный блок $EB^1, \ldots, EB^{n-1}$. Каждый вершинный блок содержит по две вершины $v_j^k, \bar{v}_j^k$ для каждой вершины $v_j \in V$, а каждый реберный блок содержит по две вершины $e_i^k, \bar{e}_i^k$ для каждого ребра $e_i \in E$:

$$VB^k = v_1^k, \bar{v}_1^k, v_2^k, \bar{v}_2^k, \ldots, v_n^k, \bar{v}_n^k \qquad \text{и} \qquad EB^k = e_1^k, \bar{e}_1^k, e_2^k, \bar{e}_2^k, \ldots, e_m^k, \bar{e}_m^k.$$

Чтобы построить путь, лежащий в основе гиперграфовой программы, мы записываем вершинные и реберные блоки поочередно следующим образом: $VB^1, EB^1, VB^2, EB^2, \ldots, EB^{n-1}, VB^n$, и затем соединяем соседние вершины ребрами. Добавим в нашу программу следующие гиперребра:

$$h_i^k = [\bar{v}_j^k, e_i^k] \quad \text{и} \quad g_i^k = (\bar{e}_i^k, v_{j'}^{k+1}], \qquad \text{для } e_i = (v_j, v_{j'}) \in E \ \text{ и } \ 1 \leqslant k < n,$$

где через $[a, b]$ мы обозначаем множество вершин между a и b, включая a и b, а через $(a, b]$ мы обозначаем множество вершин между a и b, не включая a, но включая b. Мы дополнительно добавляем гиперребра $s = \{v_1^1\}$ и $t = \{\bar{v}_n^n\}$.

Вершины P вида v_i^k и $\bar{v}_i^k$ помечены меткой 0, вершины вида e_i^k также помечены меткой 0, а вершины $\bar{e}_i^k$ помечены меткой e_i из B.

Заметим, что размер гиперграфовой программы квадратичен по размеру ветвящейся программы.

Покажем, что построенная программа P вычисляет f. Действительно, если $f(\vec{x}) = 1$, то существует путь $e_{i_1}, \ldots, e_{i_{n-1}}$ из v_1 в v_n с метками равными 1. Тогда $\{s, t\} \cup \{h_{i_k}^k, g_{i_k}^k \mid 1 \leqslant k < n\}$ является покрытием всех нулевых меток в P. В обратную сторону, если E' является покрытием нулевых меток в P, то они обязаны содержать ровно по одной паре гиперребер $h_{i_k}^k$ и $g_{i_k}^k$ для всякого k с $1 \leqslant k < n$, и соответствующая последовательность ребер $e_{i_1}, \ldots, e_{i_{n-1}}$ определяет путь из v_1 в v_n. А поскольку E' не покрывает вершины $\bar{e}_{i_k}^k$ для $1 \leqslant k < n$, то их метки должны быть равны 1.

Легко видеть, что доказательство проходит и в монотонном случае. ■

7.4.4 Древесные HGP

Теорема 7.5. *Выполняется следующее равенство* $\mathsf{HGP}^{tree} = \mathsf{SAC}^1$. *То же самое верно и для монотонного случая.*

Весь этот раздел посвящен доказательству этой теоремы. Вновь мы приведем доказательство для общего случая, и будет легко понять, что то же самое доказательство работает и для монотонного случая.

Прежде чем переходить к доказательству, введем необходимые обозначения, касающиеся деревьев. Пусть Tr — дерево, и $v_1, \ldots, v_k$ — некоторые его вершины. Через $\langle v_1, \ldots, v_k \rangle$ мы обозначаем *интервал* с концами в $v_1, \ldots, v_k$: поддерево Tr, состоящее из объединения всех путей между всеми парами вершин v_i, v_j.

Мы начнем с доказательства $\mathsf{SAC}^1 \subseteq \mathsf{HGP}^{tree}$. Рассмотрим схему C с полуограниченной входной степенью размера s и глубины не больше $\log s$. Обозначим через $g_1, \ldots, g_s$ элементы схемы (включая входные элементы), где g_s — выходной элемент. Определим $\wedge$-глубину g_i в C как максимальное число $\wedge$-элементов (включая сам элемент g_i) на пути из g_i к входным переменным.

Обозначим через S_i множество всех $\wedge$-элементов схемы $\wedge$-глубины i. Заметим, что поскольку глубина C не больше $\log s$, мы имеем, что $\wedge$-глубина всех элементов также не больше $\log s$. Для всякого $\wedge$-элемента g_i схемы мы различаем его первый и второй входы. Мы обозначаем через $\mathsf{Left}(g_i)$ подсхему, вычисляющую первый вход g_i, то есть подсхему, состоящую из первого входа g_j элемента g_i и всех элементов, из которых есть путь в g_j. Аналогично мы обозначаем через $\mathsf{Right}(g_i)$ подсхему, вычисляющую второй вход g_i.

Лемма 7.1. *Всякая схема C полуограниченной входной степени размера s и глубины d эквивалентна схеме полуограниченной входной степени размера $2^d s$ и глубины d, такой что для всякого i*

$$\left(\bigcup_{g \in S_i} \mathsf{Left}(g)\right) \bigcap \left(\bigcup_{g \in S_i} \mathsf{Right}(g)\right) = \emptyset.$$

Доказательство этой леммы достаточно стандартно, мы включаем его для полноты изложения.

Доказательство. Мы покажем индукцией по j, что можно перестроить схему таким образом, что свойство выполняется для всех $i \leqslant j$, глубина схемы не меняется, а размер увеличивается не более чем в 2^j раз.

Рассмотрим все $\wedge$-элементы в S_j и рассмотрим подсхему $\bigcup_{g \in S_j} \mathsf{Left}(g)$. Построим отдельную копию C' этой подсхемы и подставим выходы этой схемы вместо первых входов в $\wedge$-элементы в S_j. Это увеличивает размер схемы не более чем в два раза и гарантирует выполнение свойства для S_j. Теперь для обеих схем C' и $\bigcup_{g \in S_j} \mathsf{Right}(g)$ воспользуемся предположением индукции (заме-

тим, что схемы не пересекаются). Размер обеих схем увеличится не более чем в 2^{j-1} раз, и свойство для S_i при $i < j$ будет выполнено. ■

Мы можем предполагать без ограничения общности, что схема C удовлетворяет свойству из леммы 7.1.

Перейдем к построению HGP^{tree}. Мы начнем с построения дерева Tr и затем определим гиперграфовую программу на этом дереве. Для всякого элемента g_i в C, мы заводим две вершины v_i, u_i и располагаем все эти вершины в виде дерева от выхода схемы к входам. Мы строим дерево индуктивно от корня к листьям. Сначала мы размещаем вершины, соответствующие элементам максимальной $\wedge$-глубины d, в виде пути. Вершины упорядочиваются согласно порядку элементов в C: чем больше номер элемента, тем ближе соответствующие вершины к корню дерева. В каждой паре вершин v-вершина ближе к корню, чем u-вершина. Далее, мы разветвляем дерево на две ветки в последней u-вершине и сопоставляем подсхему $\bigcup_{g \in S_d} \mathsf{Left}(g)$ с левой веткой, а подсхему из всех остальных элементов — с правой веткой. Мы повторяем процедуру для каждой из подсхем. В результате мы получаем дерево, число вершин которого равно $2s$. Наконец, мы удаляем вершину v_s. Таким образом, корнем дерева является вершина u_s.

Перейдем к построению гиперграфовой программы, основанной на этом дереве. Для этого нам нужно определить гипердерева программы. Для всякого $i \neq s$ мы заводим гипердерево $\langle v_i, u_i \rangle$. Для всякого $\wedge$-элемента g_i с $g_i = g_j \wedge g_k$ мы добавляем гипердерево $\langle u_i, v_j, v_k \rangle$. Для всякого $\vee$-gэлемента $g_i = g_{k_1} \vee \ldots \vee g_{k_l}$ мы добавляем гипердерево $\langle u_i, v_{k_1} \rangle, \ldots, \langle u_i, v_{k_l} \rangle$.

Для входных элементов мы помечаем их u-вершины соответствующими литералами (напомним, что в схеме C отрицания применяются только ко входам, так что в схеме нет элементов NOT). Мы помечаем все остальные вершины дерева меткой 0.

Ясно, что описанная конструкция дает древесную гиперграфовую программу полиномиального размера от размера схемы C, и конструкция сохраняет монотонность. Для завершения доказательства первого включения нам нужно показать, что построенная программа вычисляет ту же функцию, что и схема. Мы доказываем это в следующей лемме.

Лемма 7.2. *Для данного входа $\vec{x}$ и всякого i элемент g_i выдает* 1 *тогда и только тогда, когда поддерево с корнем в u_i может быть покрыто (то есть, существует непересекающееся семейство гиперребер, лежащих внутри поддерева и покрывающих все нули в поддереве).*

Доказательство. Мы доказываем утверждение индукцией по i. Для входных элементов утверждение очевидно.

Пусть g_i — $\wedge$-элемент. Тогда, если он выдает 1, то оба его входа выдают 1. Мы покрываем оба поддерева, соответствующих входам (по предположению индукции), и добавляем гиперребро $\langle u_i, v_j, v_k\rangle$. Это покрывает поддерево с корнем в u_i. В другую сторону, единственный способ покрыть вершину u_i — это использовать гиперребро $\langle u_i, v_j, v_k\rangle$, а тогда и оба поддерева с корнями в u_j и u_k должны быть покрыты. Тогда, по предположению индукции, и g_j, и g_k выдают 1, а значит, и g_i выдает 1.

Если g_i — $\vee$-элемент и он выдает 1, то существует вход g_{k_j} элемента g_i, который выдает 1. По предположению индукции существует покрытие поддерева с корнем в u_{k_j}, добавим к нему гиперребро $\langle u_i, v_{k_j}\rangle$. Все остальные вершины поддерева с корнем в u_i можно покрыть гиперребрами вида $\langle v_p, u_p\rangle$. В другую сторону, u_i может быть покрыто только одним из гиперребер вида $\langle u_i, v_{k_j}\rangle$. Тогда для дерева с корнем в u_{k_j} также должно быть покрытие. По предположению индукции g_{k_j} выдает 1, а значит, g_i выдает 1. ■

Теперь перейдем к доказательству включения $\mathsf{HGP}^{tree} \subseteq \mathsf{SAC}^1$. Пусть P — древесная гиперграфовая программа размера s, обозначим через Tr соответствующее ей дерево. Мы построим булеву схему полуограниченной входной

степени, размера полиномиального по s и глубины $O(\log s)$. Сначала мы опишем идею конструкции, а затем перейдем к детальному построению.

Во-первых, мы переформулируем задачу в более удобной форме: вместо покрытия всех нулей среди вершин гиперграфа мы хотим рассматривать разбиения множества всех вершин (независимо от их меток) на непересекающиеся гиперребра. Чтобы перейти к этой постановке задачи, для всякой вершины v дерева добавим одноточечное гиперребро $\{v\}$. Теперь метки на вершинах говорят нам, какие гиперребра мы можем использовать. Более формально, мы заводим метки гиперребер. Изначальные гиперребра помечены 1, а новые гиперребра помечены метками соответствующих вершин. Нетрудно видеть, что существует покрытие всех нулей изначальными гиперребрами тогда и только тогда, когда существует разбиение вершин на гиперребра, метки которых принимают значения 1 в новом гиперграфе. В дальнейшем мы будем рассматривать постановку с разбиением вершин.

Идея конструкции состоит в обобщении стандартного алгоритма для достижимости в ориентированных графах. А именно, мы рассмотрим поддеревья данного дерева и будем вычислять рекурсивно, существуют ли разбиения поддеревьев. Рекурсия работает следующим образом: ясно, что поддерево может быть разбито тогда и только тогда, когда либо множество его вершин совпадает с гиперребром с меткой 1, либо его можно разбить на два поддерева, каждое из которых может быть разбито. Таким образом, мы можем последовательно вычислять для все больших и больших деревьев, можно ли их разбить на гиперребра, и в конце дойдем до всего дерева Tr. Основная проблема, которую нам нужно преодолеть в этом подходе, это что в дереве Tr может быть экспоненциально много поддеревьев. Мы справляемся с этой проблемой, ограничивая вычисления некоторым классом поддеревьев, к описанию которого мы переходим.

Удаление пары ребер e_1, e_2 из Tr разбивает дерево на три поддерева. *Поддеревом между* e_1 *и* e_2 мы называем то из этих трех поддеревьев, которое имеет

общие вершины и с e_1, и с e_2. Определим отношение $\mathsf{Reach}(e_1, e_2)$ равным 1, если поддерево между e_1 и e_2 может быть разбито, и равным нулю 0 иначе. Аналогично мы можем рассмотреть *поддерево между ребром e и листом l* нашего дерева: удалим ребро e и возьмем то из двух получившихся поддеревьев, которое содержит l. Мы определяем $\mathsf{Reach}(e, l)$ аналогично. Поддерево между листьями l_1 и l_2 — это все дерево Tr. $\mathsf{Reach}(l_1, l_2) = 1$ тогда и только тогда, когда Tr может быть разбито.

Мы будем рекурсивно вычислять отношение Reach для пар входов до тех пор, пока не вычислим его для пары листьев. Заметим, что мы на самом деле будем вычислять Reach не для всех пар входов, и будем рассуждать более аккуратно.

Замечание 7.4. *Если дерево* Tr *является путем, то это построение полностью соответствует задаче достижимости для ориентированных ациклических графов. Хорошо известно, что эта задача является* NL*-полной. Наш анализ показывает, что когда мы обобщаем эту задачу до деревьев, она становится* SAC^1*-полной.*

Прежде чем переходить к вычислению Reach, нам нужно проделать предварительную техническую работу.

Вершина дерева Tr называет *точкой ветвления*, если ее степень не меньше 3. *Ветвью* дерева Tr называется поддерево, состоящее из такого пути между двумя точками ветвления или листьями, который не содержит других точек ветвления.

Нам потребуется следующая техническая лемма о структуре древесных гиперграфовых программ.

Лемма 7.3. *Для всякой древесной гиперграфовой программы H с соответствующим деревом* Tr *существует эквивалентная древесная гиперграфовая программа H' с соответствующим деревом* Tr'*, такая что каждое гиперребро*

H' содержит не более одной точки ветвления Tr'*, и размер H' не превышает $p(|H|)$ для некоторого многочлена p.*

Доказательство. Пусть $h_1, \ldots, h_l$ — гиперребра H, содержащие не меньше двух точек ветвления. Пусть $bp_1, \ldots, bp_l$ — число точек ветвления в них. Мы докажем лемму индукцией по $bp = \sum_i bp_i$. База соответствует случаю $bp = 0$.

Для шага индукции рассмотрим h_1, и пусть v — одна из точек ветвления Tr в h_1. Обозначим через $e_1, \ldots, e_k$ ребра, смежные с v в Tr. На каждом e_i введем две дополнительные вершины v_{i1}, v_{i2}, где вершина v_{i1} ближе к v, и пометим их нулями. Разобьем h_1 на $k+1$ непересекающихся гиперребер по ребрам $\{v_{i1}, v_{i2}\}$ и заменим h этими новыми гиперребрами. Добавим гиперребра $\{v_{i1}, v_{i2}\}$ для всех i. Нетрудно видеть, что для произвольных значений переменных существует покрытие всех нулей в изначальном гиперграфе тогда и только тогда, когда существует покрытие всех нулей в новом гиперграфе. Ясно, что bp уменьшается во время этой процедуры. Наконец, нетрудно видеть, что размер гиперграфовой программы не увеличивается существенно во время этой процедуры. ■

Таким образом, мы можем предполагать, что всякое гиперребро гиперграфа содержит не больше одной точки ветвления.

Теперь мы готовы начать описание вычисления отношения Reach. Вычисление происходит в два этапа: сначала мы вычисляем это отношение для всех пар входов (ребер и листьев) на каждой ветке дерева отдельно, а затем мы вычисляем отношение для входов с разных веток. Мы докажем, что оба этапа можно вычислить с помощью схемы в SAC^1.

Вычисление для веток аналогично вычислению для задачи достижимости в ориентированных графах. Мы вводим аналог матрицы смежности B. Это квадратная матрица, строки и столбцы которой помечены входами Reach для этой ветки (ребрами и листьями). Обозначим через $b_1, \ldots, b_k$ упорядоченный список ребер и листьев ветки. Мы записываем 1 в ячейку (b_i, b_j) матрицы тогда и только тогда, когда либо $i = j$, либо $i \leqslant j$ и множество вершин поддерева

между b_i и b_j совпадает с одним из гиперребер. Все остальные ячейки матрицы мы полагаем равными 0. Ясно, что значения ячеек матрицы задаются входами схемы. Далее мы последовательно $\lceil \log_2 k \rceil$ раз применяем булево возведение в квадрат к матрице B. В результате мы получаем матрицу $B^{2^{\lceil \log_2 k \rceil}}$. Стандартные рассуждения показывают, что ячейка (b_i, b_j) этой матрицы для $i \leqslant j$ равна 1 тогда и только тогда, когда поддерево между b_i и b_j может быть разбито на гиперребра.

Заметим, что каждое булево возведение в степень требует $\vee$-элементов неограниченной входной степени и $\wedge$-элементов входной степени 2. Поскольку мы применям эту операцию логарифмическое число раз, получившаяся схема является SAC^1-схемой.

Первый этап вычисления был достаточно стандартным, но второй требует некоторой аккуратности.

Рассмотрим дерево Br, вершинами которого являются точки ветвления и листья изначального дерева Tr, а ребрами которого являются ветви Tr. В Br каждая вершина является либо листом, либо точкой ветвления. Мы будем рассматривать поддеревья дерева Br.

Мы опишем процесс расщепления дерева Br в меньшие поддеревья, не пересекающиеся по ребрам. В конце процесса все поддеревья будут отдельными ребрами. Выведем следующую базовую операцию. Предположим, что мы уже построили поддерево Br', рассмотрим его вершину $v \in \mathrm{Br}'$ и предположим, что из нее выходит k ребер $e_1, \ldots, e_k$ внутри Br', $e_i = \{v, v_i\}$. Разобьем вершину v на k вершин и соединим каждое ребро $e_1, \ldots, e_k$ с отдельной вершиной. Получившееся множество деревьев будем называть *расщеплением* Br' в вершине v. Будем обозначать эти новые деревья через $\mathrm{Br}_1, \ldots, \mathrm{Br}_k$. Для упрощения обозначений мы будем обозначать копии вершины v в каждом из новых поддеревьев снова через v.

Для поддерева Br' дерева Br мы называем его вершину *граничной вершиной*, если у нее есть сосед в Br вне Br'. Ребра Br', смежные с граничными верши-

нами, мы будем называть *граничными ребрами* Br'. *Степенью* поддерева Br' называется число его граничных вершин. Заметим, что единственное поддерево Br степени 0 — это само дерево Br.

Следующая лемма позволяет применять нашу базовую операцию расщепления эффективно.

Лемма 7.4. *Рассмотрим поддерево* Br' *с* m *ребрами. Если его степень* $\leqslant 1$*, то существует* $v \in \mathrm{Br}'$*, расщепляющая его в поддеревья, не пересекающиеся по ребрам, в каждом из которых не более* $m/2+1$ *ребер, и степень каждого из которых не больше* 2*. Если степень* Br' *равна* 2*, то существует* $v \in \mathrm{Br}'$*, расщепляющая его в поддеревья, в каждом из которых не больше* $m/2+1$ *ребер и степень каждого из которых не больше* 2*, а также, возможно, в еще одно поддерево с менее чем* m *ребрами и степени* 1*.*

Доказательство. Если Br' степени $\leqslant 1$, рассмотрим произвольную вершину v_1 и поддеревья, в которые эта вершина разбивает Br'. Если среди них существует поддерево Br_1 с больше чем $m/2+1$ ребрами, то рассмотрим (единственную) вершину v_2 в этом поддереве, соседнюю с v_1. Если мы расщепим Br' в v_2, то это расщепление будет состоять из дерева $(\mathrm{Br}' \setminus \mathrm{Br}_1) \cup \{v_1, v_2\}$ и других деревьев, лежащих внутри Br_1. Таким образом, $(\mathrm{Br}' \setminus \mathrm{Br}_1) \cup \{v_1, v_2\}$ будет размера не больше $m/2$, а остальные поддеревья будут размера меньше, чем $|\mathrm{Br}_1|$ (под размером дерева мы здесь понимаем число ребер в нем). Таким образом, размер самого большого поддерева уменьшится, и мы будем повторять процесс до тех пор, пока размер самого большого поддерева не станет не больше $m/2+1$.

Если Br' имеет степень 2, рассмотрим его граничные точки b_1 и b_2. Мы повторяем тот же процесс, начиная из точки $v_1 = b_1$. Как только в этом процессе текущая вершина v пытается покинуть путь между b_1 и b_2, мы останавливаемся (не покидая путь). Для этой вершины v нетрудно видеть, что все получающиеся деревья будут степени не больше 2. И единственное дерево, которое возможно имеет размер больше $m/2+1$, имеет степень 1. ■

С помощью этой леммы мы можем организовать процесс расщепления следующим образом. Мы начинаем с расщепления $\{\mathrm{Br}\}$, состоящего из самого дерева Br, и последовательно расщепляем каждое из текущих деревьев в меньшие. То есть, на каждом шаге мы повторяем описанную процедуру для каждого из текущих поддеревьев отдельно. Заметим, что через каждые два шага размер самого большого поддерева уменьшается в два раза. Так что через $O(\log s)$ шагов мы получим расщепление, состоящее из отдельных ребер.

Схема, которую мы построим, рассматривает описанное расщепление дерева в обратном порядке. То есть, мы начинаем с поддеревьев, состоящих из отдельных ребер. Затем на каждом шаге мы соединяем некоторые из них. В конце мы получаем все дерево.

Интуиция состоит в том, что вместе с построением поддерева Br' из ребер, мы вычисляем отношение Reach для соответствующего поддерева Tr.

Теперь мы готовы описать схему. Мы уже вычислили отношение Reach для каждой ветви, то есть для изначального разбиения Br. Далее схема вычисляет отношение Reach для более крупных поддеревьев Br, следуя процессу, описанному выше, однако мы вычисляем отношение только для входов на граничных ветвях поддеревьев. Более точно, предположим, что мы склеиваем поддеревья $\mathrm{Br}_1, \ldots, \mathrm{Br}_k$ в вершине v и получаем дерево Br'. Рассмотрим случай, когда два из деревьев $\mathrm{Br}_1, \ldots, \mathrm{Br}_k$ имеют степень 2. Другой случай полностью аналогичен. Для простоты обозначений будем считать, что деревья Br_1 и Br_2 имеют степень 2. Обозначим через b, b' граничные ребра Br' и через $b_1, \ldots, b_k$ граничные ребра $\mathrm{Br}_1, \ldots, \mathrm{Br}_k$, смежные с v соответственно.

Нетрудно видеть, что для всех входов c в b и c' в b' верно

$$\mathsf{Reach}(c, c') = \bigvee_{h \ni v} \left(\mathsf{Reach}(c, e_1) \wedge \mathsf{Reach}(c', e_2) \wedge \bigwedge_{i=3}^{k} \mathsf{Reach}(e_i, l_i) \wedge l(h) \right), \quad (7.5)$$

где h пробегает все гиперребра нашего гиперграфа, лежащие в Br и содержащие v, $e_1, \ldots, e_k$ — граничные ребра h, лежащие в ветвях $b_1, \ldots, b_k$ соответственно, для всякого i l_i — это лист Br_i и $l(h)$ — метка гиперребра h.

В конце мы доходим до всего дерева Br, и, в частности, вычисляем отношение Reach для двух листьев Tr. Это является выходом схемы.

Мы описали схему, вычисляющую нашу функцию. Легко видеть, что монотонность сохраняется. Также нетрудно понять, что размер схемы ограничен полиномом от s. Остается лишь показать, что эту схему можно реализовать так, что ее глубина равна $O(\log s)$. Это нетривиально, поскольку нам нужно указать, как вычислять большие AND в формуле (7.5), чтобы глубина была логарифмической. Для этого мы докажем следующую лемму.

Лемма 7.5. *Пусть отношение* Reach *для каждой ветки уже вычислено. Тогда отношение* Reach *для поддерева* Br' *с* m *ребрами, построенного на шаге* i*, может быть вычислено схемой* $\wedge$*-глубины не больше* $\log m + i$.

Доказательство. Доказательство проходит по индукции. Пусть для построения Br' мы склеиваем поддеревья $\mathrm{Br}_1, \ldots, \mathrm{Br}_k$ размеров $m_1, \ldots, m_k$ соответственно (размер измеряется числом ребер). Заметим, что $m = m_1 + \ldots + m_k$.

По предположению индукции мы можем вычислить отношение Reach для каждого поддерева Br_j схемой $\wedge$-глубины $\log m_j + i - 1$.

Рассмотрим k-буквенный алфавит $A = \{a_1, \ldots, a_k\}$ и сопоставим каждой букве a_j вероятность m_j/m. Хорошо известно, что существует префиксный двоичный код для этого алфавита, такой что каждая буква a_j кодируется словом длины $\lceil \log(m/m_j) \rceil$ [39]. Это кодирование можно представить корневым двоичным деревом, листья которого помечены буквами A, и длина пути из корня в лист, помеченный a_j, равна $\lceil \log(m/m_j) \rceil$. Сопоставив функцию AND каждой внутренней вершине дерева, мы получим вычисление конъюнкции в формуле выше. Глубина этого вычисления равна максимуму по j выражения

$$\log m_j + (i-1) + \lceil \log(m/m_j) \rceil \leqslant \log m_j + (i-1) + \log(m/m_j) + 1 = \log m + i.$$

■

Из этой леммы и из того факта, что вычисление заканчивается после $O(\log s)$ шагов, мы получаем, что суммарная $\wedge$-глубина схемы равна $O(\log s)$, а значит, суммарная глубина схемы также равна $O(\log s)$. Это завершает доказательство теоремы 7.5.

7.4.5 Древесные HGP степени 2

Теорема 7.6. *Выполняются следующие равенства* $\mathsf{HGP}_2^{tree} = \mathsf{HGP}_2^{path} = \mathsf{AC}^0_{3,\mathrm{AND}}$. *То же самое верно в монотонном случае.*

Доказательство. Ясно, что $\mathsf{HGP}_2^{path} \subseteq \mathsf{HGP}_2^{tree}$.

Докажем включение $\mathsf{HGP}_2^{tree} \subseteq \mathsf{AC}^0_{3,\mathrm{AND}}$. Рассмотрим древесную гиперграфовую программу P степени 2. Во-первых, заметим, что мы можем предполагать, что нет гиперребер e, e' в P, таких что $e \subseteq e'$. Действительно, если такая пара гиперребер есть, то все вершины в e не покрыты никакими другими гиперребрами, и если мы удалим их из програмы вместе с e, получившаяся программа будет эквивалентна изначальной.

Теперь рассмотрим следующий граф D. Его вершины — это гиперребра P. Две вершины соединены, если соответствующие гиперребра пересекаются. Нетрудно видеть, что D является лесом. Пометим ребро $\{e_1, e_2\}$ в D конъюнкцией меток вершин в $e_1 \cap e_2$. Пометим вершину e в D конъюнкцией меток вершин P, лежащих только в e. Если не существует таких вершин, то метка e равна 1.

Множества гиперребер P соответствуют множествам вершин D, и непересекающиеся гиперребра соответствуют не соединенным вершинам D. Нетрудно видеть, что для произвольного входа непересекающееся покрытие всех нулей в P соответствует независимому множеству I в D, покрывающему все нули в вершинах, и такому что каждое ребро с меткой равной нулю имеет один из концов в I.

Мы утверждаем, что не существует независимого множества I в D тогда и только тогда, когда существует путь $e_0, e_1, \ldots, e_k$ в D с нечетным k (в частности, годится $k = 1$), такой что e_0 и e_k помечены 0, и «четные» ребра $\{e_{i-1}, e_i\}$ с четным i помечены 0.

Легко видеть, что если такой путь существует, то не существует требуемого независимого множества I в D. Действительно, мы должны включить e_0 и e_k в I. Ребро $\{e_1, e_2\}$, помеченное нулем, вынуждает нас включить e_2 в I (e_1 смежно с e_0 и не может быть включено в I), дальше ребро $\{e_3, e_4\}$ вынуждает нас включить e_4 в I и так далее. В конце мы должны будем включить e_{k-1} в I, а поскольку e_k тоже лежит в I, это приводит к противоречию с независимостью I.

В другую сторону, предположим, что не существует таких путей. Тогда мы можем построить требуемое независимое множество I. Добавим в I все вершины, метки которых равны 0. Если существует тройка последовательных вершин e, e_1, e_2 в D, такая что e уже лежит в I, и ребро $\{e_1, e_2\}$ помечено нулем, мы добавляем e_2 в I. Заметим, что если мы добавляем какую-то вершину e' в I в этом процессе, это означает, что существует путь $e = e_0, e_1, \ldots, e_k = e'$ с четным k, такой что вершина e помечена нулем, и каждое ребро $\{e_{i-1}, e_i\}$ для четного i в этом пути помечено нулем.

В этом процессе мы не добавим две соединенные вершины e и e' графа D в I, поскольку тогда объединение описанных выше путей для этих двух вершин дало бы путь нечетной длины с концами, помеченными нулями, и с каждым вторым ребром, помеченным нулем. Это прямо противоречит нашему предположению.

Если у нас все еще остаются ребра, помеченные нулем в D без концов в I, добавим любой конец такого ребра в I и повторим процедуру выше. Это также не приводит к паре соединенных вершин в I. Действительно, если в результате мы добавим в I вершину e_1, соединенную с вершиной e, которая была добавлена в I на одном из предыдущих шагов, то существует ребро $\{e_2, e_1\}$,

помеченное нулем (которое было причиной добавления e_1 в I), и это означает, что мы должны были добавить e_2 в I на одном из предыдущих шагов.

Повторяя этот процесс, мы получаем независимое множество I, покрывающее все вершины и ребра с метками 0.

Таким образом, утверждение доказано. Это означает, что существует требуемое независимое множество I в D тогда и только тогда, когда для всех пар вершин e и e' в D с нечетным расстоянием между ними (обозначим путь между ними через $e = e_0, e_1, \ldots, e_k = e'$) одна из следующих меток равна 1: метка e, метка e', метки всех $\{e_{i-1}, e_i\}$ с четным i.

Наконец, это свойство несложно вычислить элементом AND, примененным к элементам OR, примененным к элементам AND от меток гиперграфовой программы. На верхнем уровне у нас будет AND по всем парам вершин D с нечетным расстоянием. Дальше у нас будет OR по всем меткам, перечисленным выше. Наконец, каждая метка является конъюнкцией литералов — меток гиперграфовой программы.

Остается доказать включение $\mathsf{AC}^0_{3,\mathrm{AND}} \subseteq \mathsf{HGP}_2^{path}$. Рассмотрим схему C в $\mathsf{AC}^0_{3,\mathrm{AND}}$. Мы покажем, что она может быть вычислена линейной гиперграфовой программой степени 2.

Обозначим элементы OR в C через $g_1, \ldots, g_k$. То есть, C выдает $g_1 \wedge \ldots \wedge g_k$. Обозначим входы g_i через $g_{i,1}, \ldots, g_{i,l_i}$ (каждый $g_{i,j}$ является функцией AND от литералов).

Для удобства мы построим линейную гиперграфовую программу H, в которой метки будут конъюнкциями литералов. Легко видеть, что эти программы эквивалентны обычным линейным гиперграфовым программам. В нашей гиперграфовой программе будут следующие вершины (в таком порядке):

$$h_{1,0}, h_{1,1}, \ldots, h_{1,2l_1+1}, h_{1,2l_1+2}, h_{2,0}, \ldots, h_{2,2l_2+2}, \ldots, h_{k,2l_k+2}.$$

Для каждой пары (i,j), где $j \leqslant 2l_i + 1$, мы заводим гиперребро $e_{i,j} = \{h_{i,j}, h_{i,j+1}\}$.

Вершины $h_{i,0}$ и $h_{i,2l_i+2}$ в H помечены меткой 0. Мы помечаем вершины $h_{i,j}$ для нечетного j меткой 1, а для четного j — конъюнкцией $g_{i,j}$.

Рассмотрим некоторое i. Аналогично предыдущему анализу мы можем покрыть вершины $h_{i0}, h_{i1}, \ldots, h_{il_i+1}, h_{i,l_i+2}$ тогда и только тогда, когда хотя бы одна метка из $h_{i,0}, h_{i,2} \ldots, h_{i,2l_i+2}$ равна 1. Для различных i соответствующие вершины $h_{i,0}, h_{i,2}, \ldots, h_{i,2l_i+2}$ должны быть покрыты независимо. Таким образом, на каждом входе выход гиперграфовой программы совпадает с выходом схемы. ■

Глава 8

Корни макс-плюс многочленов

В этой главе мы работаем в полукольце над $\mathbb{R}$ или над $\mathbb{Q}$. Если не сказано иное, то результаты выполняются над обоими полукольцами.

8.1 Макс-плюс аналог комбинаторной теоремы о нулях

Для макс-плюс многочлена p обозначим через $\mathsf{Supp}(p)$ его носитель — множество всех $J = (j_1, \dots, j_n)$, таких что моном $\vec{x}^J$ встречается в p.

Рассмотрим два конечных множества $S, R \subseteq \mathbb{R}^n$, таких что $|S| = |R|$. Мы называем пару множеств S и R *невырожденными*, если есть биекция $f\colon S \to R$, такая что $\sum_{x\in S}\langle \vec{x}, f(\vec{x})\rangle$ больше, чем аналогичная сумма для всех остальных биекций из S в R. Здесь $\langle \vec{a}, \vec{b}\rangle$ — стандартное скалярное произведение. Иначе будем говорить, что пара множеств R и S *вырождена*. Заметим, что понятие вырожденности симметрично.

Мы говорим, что макс-плюс многочлен вырождается на данном множестве точек, если все точки множества являются корнями многочлена. Сформулируем сначала общий критерий для существования многочлена, вырождающегося на данном носителе.

Теорема 8.1. *Рассмотрим носитель $S \subseteq \mathbb{N}^n$ и множество точек $R \subseteq \mathbb{R}^n$. Есть три возможных случая.*

(i) Если $|R| < |S|$, то существует многочлен p с носителем в S, вырождающийся на R.

(ii) Если $|R| = |S|$, то многочлен p с носителем в S, вырождающийся на R, существует тогда и только тогда, когда пара множеств S и R вырождена.

(iii) Если $|R| > |S|$, то многочлен p с носителем в S, вырождающийся на R, существует тогда и только тогда, когда для всякого подмножества $R' \subset R$, такого что $|R'| = |S|$, пара многжеств R' и S вырождена.

Замечание 8.1. *Прежде чем переходить к доказательству теоремы отметим, что в теореме 8.1(i) можно утверждать не только существование многочлена p с $\mathsf{Supp}(p) \subseteq S$, но и существование многочлена со свойством $\mathsf{Supp}(p) = S$. Действительно, если некоторые мономы с векторами степеней из S отсутствуют в p, мы можем добавить их с достаточно маленькими коэффициентами, так чтобы значения этих мономов были меньше максимального значения мономов p во всех точках R (напомним, что R конечно).*

Доказательство. Рассмотрим многочлен

$$p(\vec{x}) = \bigoplus_{J \in S} c_J \odot \vec{x}^J$$

с носителем S. Утверждение о том, что точка $\vec{a} \in R$ является корнем p, означает, что максимум в

$$\max_{J \in S} (c_J + \langle J, \vec{a} \rangle)$$

достигается на как минимум двух мономах J_1 и J_2. Заметим, что как только S и R зафиксированы, это выражение представляет собой макс-плюс линейный многочлен с коэффициентами $\{c_J\}_{J \in S}$ многочлена p в качестве переменных, а утверждение означает, что коэффициенты являются корнем этого линейного многочлена.

Утверждение, что все точки R являются корнями p таким образом означает, что коэффициенты p являются корнем системы макс-плюс линейных многочленов с матрицей

$$(\langle J, \vec{a} \rangle)_{J \in S, \vec{a} \in R} \in \mathbb{R}^{|S| \times |R|}.$$

Правило Крамера в макс-плюс алгебре [3, 41, 60, 79] утверждает, что если число строк $|R|$ в такой системе меньше числа столбцов $|S|$, то решение всегда существует. Таким образом, в этом случае всегда есть многочлен с корнями во всех точках R.

Если матрица квадратная, то есть $|R| = |S|$, то известно [3,41,60,79], что решение существует тогда и только тогда, когда макс-плюс определитель матрицы вырожден. Макс-плюс определитель является аналогом классического определителя. Для нашей матрицы он задается выражением

$$\bigoplus_{f\colon S\to R}\left(\bigodot_{J\in S}\langle J, f(J)\rangle\right) = \max_{f\colon S\to R}\left(\sum_{J\in S}\langle J, f(J)\rangle\right),$$

где f пробегает по всем биекциям из S в R. Вырожденность определителя означает, что максимум достигается на не менее чем двух мономах. Это значит, что существуют две биекции $f, g\colon S \to R$ с равными и максимальными суммами $\sum_{J\in S}\langle J, f(J)\rangle = \sum_{J\in S}\langle J, g(J)\rangle$. Заметим, что это в точности означает вырожденность пары множеств S и R.

Если число строк $|R|$ в матрице больше числа столбцов $|S|$ в ней, то известно [3, 41, 60, 79], что система имеет нетривиальный корень тогда и только тогда, когда макс-плюс определитель всякой квадратной подматрицы размера $|S| \times |S|$ вырожден. Это в точности обзначает, что для всякого подмножества $R' \subset R$, такого что $|R'| = |S|$, пара множеств R' и S вырождена. ■

Теперь мы выведем следствия из полученного общего критерия.

Пусть нам дано множество $S \subseteq \mathbb{N}^n$. Пусть также нам дано множество действительных чисел $\{\alpha^i_j\}$ для $i = 1, \ldots, n$, $j \in \mathbb{N}$, и для всякого i верно

$$\alpha^i_0 < \alpha^i_1 < \alpha^i_2 < \ldots.$$

Для $J = (j_1, \ldots, j_n)$ введем обозначение $\vec{\alpha}_J = (\alpha^1_{j_1}, \ldots, \alpha^n_{j_n})$. Рассмотрим множество $R_S = \{\vec{\alpha}_J \mid J \in S\}$.

Мы рассматриваем следующий вопрос. Пусть нам дан многочлен p с носителем $\mathsf{Supp}(p) \subseteq S$. Для каких множеств $S' \subseteq \mathbb{N}^n$ возможно, что p вырождается на $R_{S'}$?

Естественным является случай $S = S'$. Мы доказываем следующую теорему.

Теорема 8.2. *Для всякого S и для всякого нетривиального макс-плюс многочлена p, такого что $\mathsf{Supp}(p) \subseteq S$, существует $\vec{r} \in R_S$, не являющийся корнем p.*

Интересным частным случаем этой теоремы является $S = \{0, 1, \ldots, k\}^n$. Для этого случая теорема утверждает, что всякий невырожденный многочлен с индивидуальными степенями переменных не больше k не вырождается на решетке размера $k + 1$.

Теорема 8.1(i) и теорема 8.2 дают ответ на поставленный нами вопрос в некоторых стандартных и естественных случаях. Отметим, что ситуация здесь оказывается существенно отличной от классического случая. Классический аналог теоремы 8.2 для случая $S = \prod_{i=1}^{n}\{0, 1, \ldots, k_i\}$ является несложным наблюдением. В макс-плюс случае доказательство уже требует определенных усилий. С другой стороны, в классическом случае известно, что для таких S носитель многочлена может быть существенно больше S, и при этом многочлен все еще не будет вырождаться на R_S (см. комбинаторную теорему о нулях [5]). В макс-плюс случае, однако, если мы расширим носитель многочлена даже одним дополнительным мономом, то согласно теореме 8.1(i) вырождающийся многочлен уже будет существовать.

В доказательстве теоремы 8.2 нам потребуется следующая несложная техническая лемма, по существу доказанная в [70, стр. 261]. Для полноты изложения мы приводим доказательство.

Лемма 8.1. *Рассмотрим две неубывающие последовательности действительных чисел $v_1 \leqslant v_2 \leqslant \ldots \leqslant v_l$ и $u_1 \leqslant u_2 \leqslant \ldots \leqslant u_l$. Рассмотрим пере-*

становку $\sigma \in Sym_l$ *на* l*-элементном множестве* $\{1, \dots, l\}$*. Тогда*

$$\sum_i v_i u_i \geqslant \sum_i v_i u_{\sigma(i)}.$$

Более того, неравенство является строгим тогда и только тогда, когда существуют i, j*, такие что* $v_i < v_j$*,* $u_{\sigma(j)} < u_{\sigma(i)}$*.*

Доказательство. Введем обозначение для числа инверсий в σ: $D = |\{(i,j) \mid i < j, \sigma(j) < \sigma(i)\}|$. Мы докажем лемму индукцией по D. Для доказательства шага выберем одну из инверсий (i,j) и переставим $\sigma(i)$ и $\sigma(j)$ местами. Заметим, что при этом мы не добавляем новых инверсий.

Воспользуемся следующим наблюдением: если $a \leqslant b$ и $c \leqslant d$, то

$$bd + ac \geqslant bc + da.$$

Это неравенство выполняется, поскольку оно эквивалентно $(b-a)(d-c) \geqslant 0$.

Заметим также, что это неравенство является строгим тогда и только тогда, когда оба неравенства $a \leqslant b$ и $c \leqslant d$ строгие.

Таким образом, после перестановки i и j сумма в формулировке леммы не уменьшается, и неравенство доказано по индукции.

Докажем вторую часть утверждения леммы. Если есть пара i, j, удовлетворяющая условиям в лемме, просто поменяем i и j местами на первом шаге. Уже при этой перестановке мы получим строгое неравенство. Если же таких пар i, j нет, заметим, что мы также и не добавляем таких пар в процессе, описанном выше, поскольку в нем не добавляются новые инверсии. ■

Доказательство теоремы 8.2. По теореме 8.1 достаточно доказать, что S и R_S невырождены.

Пусть $f\colon S \to R_S$ — биекция, задаваемая равенством $f(J) = \vec{\alpha}_J$. Мы утверждаем, что максимум по всем возможным биекциям g суммы $\sum_{J \in S} \langle J, g(J) \rangle$ достигается на биекции f и только на ней.

Рассмотрим произвольную биекцию $g\colon S \to R_S$. Поскольку $R_S \subseteq \mathbb{R}^n$, удобно ввести обозначение $g(J) = (g_1(J), \ldots, g_n(J))$ и $f(J) = (f_1(J), \ldots, f_n(J))$. Рассмотрим сумму

$$\sum_{J\in S}\langle J, g(J)\rangle = \sum_{J\in S}\sum_{i=1}^{n} j_i g_i(J) = \sum_{i=1}^{n}\sum_{J\in S} j_i g_i(J).$$

Мы докажем, что для всякого i

$$\sum_{J\in S} j_i g_i(J) \leqslant \sum_{J\in S} j_i f_i(J) \tag{8.1}$$

и для хотя бы одного i

$$\sum_{J\in S} j_i g_i(J) < \sum_{J\in S} j_i f_i(J). \tag{8.2}$$

Теорема сразу следует из этих двух неравенств.

Рассмотрим произвольное i и рассмотрим проекции всех точек в множестве S на i-ю координату. Перенумеруем эти проекции в неубывающем порядке:

$$j_{1,1} = \ldots = j_{1,k_1} < j_{2,1} = \ldots = j_{2,k_2} < \ldots < j_{l,1} = \ldots = j_{l,k_l}.$$

Различные точки в S могут иметь одну и ту же i-ю координату, так что мы разбиваем точки на блоки по значению их i-й координаты. По определению R_S, проекция его точек на i-ю координату будет иметь ту же структуру:

$$r_{1,1} = \ldots = r_{1,k_1} < r_{2,1} = \ldots = r_{2,k_2} < \ldots < r_{l,1} = \ldots = r_{l,k_l}.$$

Биекции f и g порождают биекции f' и g' из последовательности $\vec{j}$ в последовательность $\vec{r}$. Более того, f порождает естественную биекцию: $f'(j_{i_1,i_2}) = r_{i_1,i_2}$. Неравенство (8.1) таким образом следует из первой части леммы 8.1.

Для доказательства неравенства (8.2) заметим, что поскольку $g \neq f$, существует $J \in S$, такое что $g(J) \neq \vec{\alpha}_J$. Это означает, что существует i, такое что

$$g_i(J) \neq \alpha^i_{j_i}.$$

Таким образом, для биекции, порожденной g на координате i, мы получаем, что $g'(j_{i_1,i_2}) = r_{i'_1,i'_2}$, где $i_1 \neq i'_1$. Без ограничения общности предположим, что $i_1 < i'_1$ (второй случай симметричен). Рассмотрим подпоследовательность

$$\vec{j'} = j_{i'_1,1}, \ldots, j_{i'_1,k_{i'_1}}, \ldots, j_{l,1}, \ldots, j_{l,k_l}.$$

Поскольку j_{i_1,i_2} отображается под действием g' в последовательность $\vec{j'}$ и g' — биекция, существует j_{i_3,i_4} в $\vec{j'}$, которое отображается вне этой последовательности, то есть $g(j_{i_3,i_4}) = r_{i'_3,i'_4}$, где $i'_3 < i'_1$.

Обозначая $a = j_{i_1,i_2}$ и $b = j_{i_3,i_4}$, мы получаем, что $a < b$, но $g'(a) > g'(b)$. По лемме 8.1 это дает неравенство (8.2). ■

8.2 Макс-плюс аналог леммы Шварца-Зиппеля

Опираясь на результаты предыдущего раздела мы можем доказать аналог леммы Шварца-Зиппеля для макс-плюс многочленов.

Теорема 8.3. *Пусть $S_1, S_2, \ldots, S_n \subseteq \mathbb{R}$, введем обозначение $|S_i| = k_i$. Тогда для всякого $d \leqslant \min_i k_i$ максимальное число корней, которое нетривиальный макс-плюс многочлен p степени не больше 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 частности, из теоремы сразу вытекает следующее следствие.

Следствие 8.2. *Пусть $S \subseteq \mathbb{R}$ — множество размера k. Тогда для всякого $d \leqslant k$ максимальное число корней, которое невырожденный макс-плюс многочлен p степени d может иметь в S^n, равно*

$$k^n - (k - d)^n.$$

В точности такое же утверждение верно для многочленов с индивидуальной степенью по каждой переменной не больше d.

Доказательство теоремы 8.3. Оценка достигается на произведении d линейных многочленов. Действительно, введем обозначение $S_i = \{s_{i,1}, s_{i,2}, \ldots, s_{i,k_i}\}$, где $s_{i,1} > s_{i,2} > \ldots > s_{i,k_i}$. Для $j = 1, \ldots, d$ обозначим через p_j следующий линейный многочлен:

$$p_j(\vec{x}) = (-s_{1,j} \odot x_1) \oplus \ldots \oplus (-s_{i,j} \odot x_i) \oplus \ldots \oplus (-s_{n,j} \odot x_n) \oplus 0.$$

Заметим, что $\vec{a} \in S_1 \times \ldots \times S_n$ является корнем p_j, если для некоторого i верно, что $a_i = s_{i,j}$, и для остальных i верно, что $a_i \leqslant s_{i,j}$.

Рассмотрим многочлен степени d, равный $p(\vec{x}) = \bigodot_{j=1}^{d} p_j(\vec{x})$. Тогда по лемме 1.1 мы получаем, что $\vec{a} \in S_1 \times \ldots \times S_n$ не является корнем p тогда и только тогда, когда для всех i верно $a_i < s_{i,d}$. Так что число не корней многочлена p равно $\prod_{i=1}^{n} (|S_i| - d)$. Это завершает доказательство верхней оценки.

Для доказательства нижней оценки предположим, что существует многочлен p с индивидуальными степенями не больше d, который имеет больше чем $\prod_{i=1}^{n} k_i - \prod_{i=1}^{n} (k_i - d)$ корней в $S_1 \times \ldots \times S_n$. Тогда число его не корней в этом множестве не больше $\prod_{i=1}^{n} (k_i - d) - 1$. Обозначим множество всех его не корней через R.

Рассмотрим семейство всех многочленов индивидуальной степени не больше $k_i - d - 1$ по переменной x_i для каждого i. Тогда их (общий) носитель имеет размер $\prod_{i=1}^{n} (k_i - d)$. Поскольку размер носителя больше R, по теореме 8.1(i) существует многочлен q с таким носителем, который имеет корни во всех точках R.

Тогда по лемме 1.1 многочлен $p \odot q$ имеет корни во всех точках $S_1 \times \ldots \times S_n$, а с другой стороны имеет носитель $\{0, \ldots, k_1 - 1\} \times \ldots \times \{0, \ldots, k_n - 1\}$. Это противоречит теореме 8.2. Следовательно, такого многочлена p не существует и теорема доказана. ■

8.3 Универсальные тестирующие множества

В этом разделе мы исследуем минимальный размер универсальных тестирующих множеств для разреженных макс-плюс многочленов. Оказывается, что в макс-плюс случае есть большая разница между тестирующими множествами над $\mathbb{R}$ и над $\mathbb{Q}$. Так что мы рассматриваем эти два случая отдельно.

Всюду в этом разделе мы обозначаем через n число переменных в многочленах, через k — число мономов в них и через s — число точек в универсальном тестирующем множестве.

8.3.1 Тестирующие множества над $\mathbb{R}$

В этом разделе мы докажем, что минимальный размер s универсального тестирующего множества над $\mathbb{R}$ равен k.

Теорема 8.4. *Для макс-плюс многочленов над $\mathbb{R}$ минимальный размер s универсального тестирующего множества для многочленов с не более чем k мономами равен k.*

Доказательство. Во-первых, заметим, что из теоремы 8.1(i) следует, что для всякого множества из s точек существует многочлен с произвольным носителем размера $k = s+1$, имеющий корни во всех s точках. Так что универсальное тестирующее множество обязано содержать не меньше точек, чем число мономов в многочленах. Отсюда мы получаем неравенство $s \geqslant k$.

Дальше мы доказываем, что $s \leqslant k$. Рассмотрим множество из s точек $S = \{\vec{a}_1, \ldots, \vec{a}_s\} \subseteq \mathbb{R}^n$, таких что все их координаты в совокупности линейно независимы над $\mathbb{Q}$. Предположим, что многочлен p с k мономами имеет корни во всех точках $\vec{a}_1, \ldots, \vec{a}_s$. Мы докажем, что $k \geqslant s+1$. Таким образом мы докажем, что S является универсальным тестирующим множеством для многочленов с $k = s$ мономами.

Обозначим мономы p через $m_1, \ldots, m_k$, где $m_i(\vec{x}) = c_i \odot \vec{x}^{J_i}$. Введем обозначение $p(\vec{a}_j) = \max_i(m_i(\vec{a}_j)) = p_j$. Поскольку a_j — корень, то значение p_j достигается на не менее чем двух мономах.

Заметим, что моном m_i принимает значение p_j в точке $\vec{a}_j$ тогда и только тогда, когда

$$\langle \vec{a}_j, J_i \rangle + c_i = p_j.$$

Рассмотрим двудольный неориентированный граф G. Вершины в левой доле соответствуют мономам p (всего k вершин). Вершины в правой доле соответствуют точкам в S (всего s вершин). Мы соединяем вершину m_i в левой доле с вершиной $\vec{a}_j$ в правой доле тогда и только тогда, когда $m_i(\vec{a_j}) = p_j$.

Заметим, что степень каждой вершины в правой доле не меньше 2 (это в точности означает, что точки являются корнями p).

Теперь докажем, что в графе G нет циклов. Действительно, пусть цикл есть. Для удобства обозначений будем считать, что последовательность вершин этого цикла есть

$$m_1, \vec{a}_1, m_2, \vec{a}_2, \ldots, m_l, \vec{a}_l.$$

Заметим, что поскольку граф двудольный, цикл должен иметь четную длину. В частности, для всех $i = 1, \ldots, l$ мы имеем $m_i(\vec{a_i}) = p_i$, то есть

$$\langle \vec{a}_i, J_i \rangle + c_i = p_i. \tag{8.3}$$

Также для всех $i = 1, \ldots, l$ мы имеем $m_{i+1}(\vec{a_i}) = p_i$ (для удобства обозначений положим здесь $m_{l+1} = m_1$), то есть

$$\langle \vec{a}_i, J_{i+1} \rangle + c_{i+1} = p_i. \tag{8.4}$$

Просуммируем равенства в (8.3) для всех $i = 1, \ldots, l$ и вычтем из результата все равенства в (8.4). Легко видеть, что все c_i и p_i сократятся, и мы получим

$$\langle \vec{a}_1, J_1 \rangle - \langle \vec{a}_1, J_2 \rangle + \langle \vec{a}_2, J_2 \rangle - \langle \vec{a}_2, J_3 \rangle + \ldots + \langle \vec{a}_l, J_l \rangle - \langle \vec{a}_l, J_1 \rangle = 0.$$

Поскольку $J_1 \neq J_2$, мы получили нетривиальную линейную комбинацию координат векторов $\vec{a}_1, \ldots, \vec{a}_l$ с целыми коэффициентами. Поскольку координаты этих векторов линейно независимы над $\mathbb{Q}$, мы получили противоречие. Таким образом, мы доказали, что в G нет циклов.

Следовательно, граф G является лесом (совокупностью нескольких деревьев). Рассмотрим каждое дерево в этом лесу отдельно. Мы докажем, что в каждом дереве T число L вершин левой доли больше числа R вершин правой доли. Действительно, поскольку степень каждой вершины в правой доле не меньше 2, число ребер в T не меньше $2R$. Число вершин в дереве на единицу больше числа ребер. Так что в T не меньше $2R + 1$ вершин. То есть,

$$R + L \geqslant 2R + 1,$$

и следовательно, $L \geqslant R + 1$. Поскольку это выполняется для каждого дерева, суммируя эти неравенства по всем деревьям, мы получаем

$$k \geqslant s + 1.$$

Таким образом, множество S является универсальным тестовым множеством для многочленов с $k = s$ мономами, и теорема доказана. ■

8.3.2 Тестирующее множество над $\mathbb{Q}$

Основное отличие нашей задачи для случая полукольца над $\mathbb{Q}$ по сравнению с полукольцом над $\mathbb{R}$ заключается в том, что теперь точки в универсальном тестовом множестве должны быть рациональными.

В этом разделе мы будем рассматривать несколько более общий объект — макс-плюс многочлены с рациональными (возможно, отрицательными) степенями переменных. Заметим, что это в действительности не сказывается на рассматриваемых нами вопросах: для всякого такого многочлена существует другой многочлен с натуральными степенями с точно таким же множеством корней

и с точно таким же числом мономов. Действительно, пусть p — многочлен с рациональными степенями. Напомним, что

$$p(\vec{x}) = \max(m_1(\vec{x}), \ldots, m_k(\vec{x})), \tag{8.5}$$

где $m_1, \ldots, m_k$ — мономы. Напомним, что каждый моном — это линейная функция над $\vec{x}$. Заметим, что если мы умножим все выражение (8.5) на положительную константу и прибавим одну и ту же линейную форму $m(\vec{x})$ ко всем мономам, мы получим многочлен с тем же самым множеством корней. Следовательно, мы можем избавиться от рациональных степеней в p, просто домножив p на достаточно большое целое число, а затем мы можем избавиться от отрицательных степеней, прибавив к p линейную форму m с достаточно большими коэффициентами.

Таким образом, в этом разделе мы будем рассматривать многочлены с рациональными степенями.

Нам будет удобно формулировать результаты этого раздела в следующих обозначениях. Обозначим через $k(s, n)$ минимальное число, такое что для всякого множества S из s точек в $\mathbb{Q}^n$ существует макс-плюс многочлен от n переменных с не более чем $k(s, n)$ мономами с корнями во всех точках S. Заметим, что универсальное тестирующее множество размера s для многочленов с k мономами существует тогда и только тогда, когда $k < k(s, n)$. Таким образом, мы можем легко получить оценки размера универсального тестирующего множества из оценок на $k(s, n)$.

Мы начнем со следующей верхней оценки на $k(s, n)$.

Теорема 8.5. *Верно неравенство* $k(s, n) \leqslant \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$.

Эквивалентно, верно следующее неравенство для размера универсальноого тестирующего множества: $s \geqslant \frac{(k-1)(n+1)+1}{2}$.

Заметим, что уже этот результат показывает различие между универсальными тестирующими множествами над $\mathbb{R}$ и над $\mathbb{Q}$.

Доказательство. Заметим, что два утверждения в теореме эквивалентны. Действительно, по определению $k(s,n)$ первое утверждение равносильно неравенству $k < \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$, где s — размер минимального тестового множества для многочленов с k мономами. Легко видеть, что это неравенство верно тогда и только тогда, когда $s > (k-1)(n+1)/2$. Минимальное целое s, для которого это неравенство верно, — это $s = \lceil \frac{(k-1)(n+1)+1}{2} \rceil$. Таким образом, неравенство эквивалентно $s \geqslant \frac{(k-1)(n+1)+1}{2}$. Нам остается доказать только первое утверждение теоремы.

Мы покажем, что для любого множества $S = \{\vec{a}_1, \ldots, \vec{a}_s\} \subseteq \mathbb{Q}^n$ размера s существует нетривиальный многочлен с не более чем $k = \lceil \frac{2s}{(n+1)} \rceil + 1$ мономами и с корнями во всех точках S. Из этого вытекает неравенство в теореме.

В этом доказательстве мы будем использовать следующие стандартные факты о (классических) афинных функциях над $\mathbb{Q}^n$.

Утверждение. *Пусть π — это $(n-1)$-мерная гиперплоскость в $\mathbb{Q}^n$. Пусть P_1 — конечное множество точек в одном из двух (открытых) полупространств относительно π и P_2 — конечное множество точек в другом (открытом) полупространстве. Пусть C_1 и C_2 — некоторые константы. Тогда верны следующие утверждения.*

1. *Если $\vec{a}_1, \ldots, \vec{a}_n \in \pi$ — точки в общем положении на π (то есть, эти точки не лежат в $(n-2)$-мерном аффинном пространстве) и $p_1, \ldots, p_n$ — некоторые константы в $\mathbb{Q}$, то существует аффинная функция f на $\mathbb{Q}^n$, такая что $f(\vec{a}_i) = p_i$ для всех i, $f(\vec{x}) > C_1$ для всех $\vec{x} \in P_1$ и $f(\vec{x}) < C_2$ для всех $\vec{x} \in P_2$.*

2. *Если g — аффинная функция на $\mathbb{Q}^n$, то существует другая аффинная функция f на $\mathbb{Q}^n$, такая что $f(\vec{x}) = g(\vec{x})$ для всех $\vec{x} \in \pi$, $f(\vec{x}) > C_1$ для всех $\vec{x} \in P_1$ и $f(\vec{x}) < C_2$ для всех $\vec{x} \in P_2$.*

Доказательство теоремы проводится индукцией по s. Базой является случай $s = 0$. В этом случае одного монома достаточно (и необходимо, поскольку мы требуем, чтобы многочлен был нетривиальным).

Рассмотрим выпуклую оболочку точек в S. Рассмотрим грань P максимальной размерности в этой выпуклой оболочке. Если выпуклая оболочка S имеет размерность n, то P имеет размерность $(n-1)$, а если оболочка S имеет размерность меньше n, мы берем в качестве P саму выпуклую оболочку S. Для удобства обозначений мы предполагаем, что точки S, принадлежащие P — это $\vec{a}_1, \ldots, \vec{a}_l$. Рассмотрим ($(n-1)$-мерную) гиперплоскость π, проходящую через $\vec{a}_1, \ldots, \vec{a}_l$. Поскольку P — это грань выпуклой оболочки S, все точки в $S' = \{\vec{a}_{l+1}, \ldots, \vec{a}_s\}$ лежат в одном (открытом) полупространстве относительно π (если S имеет размерность меньше n, то $l = s$).

Применяя предположение индукции, мы получаем многочлен $p'(\vec{x}) = \max_i m'_i(\vec{x})$, который имеет корни во всех точках S'. Для $j = 1, \ldots, l$ введем обозначение $p_j = p'(\vec{a}_j) = \max_i m'_i(\vec{a}_j)$.

Рассмотрим три случая: P содержит все точки S; P содержит не все точки S и $l \leqslant n$; P содержит не все точки S и $l > n$.

Если P содержит все точки S, то многочлен p' получен из базы индукции и состоит из одного монома m'_1. Напомним, что моном — это просто аффинная функция на $\mathbb{Q}^n$. Рассмотрим новый моном $m(\vec{x})$, такой что $m(\vec{x}) = m'_1(\vec{x})$ на гиперплоскости π, но $m(\vec{b}) \neq m'_1(\vec{b})$ для некоторого $\vec{b} \notin \pi$. Тогда многочлен $p = p' \oplus m$ имеет корни во всех точках гиперплоскости π и, таким образом, во всех точках S. Этот многочлен содержит $2 \leqslant \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$ мономов.

Если P содержит не все точки S, то размерность P равна $n-1$ (действительно, иначе P не является гранью максимальной размерности).

Если дополнительно верно, что $l \leqslant n$, мы получаем, что $l = n$. Следовательно, $\vec{a}_1, \ldots, \vec{a}_n$ — точки в общем положении в π. Тогда по утверждению выше мы можем выбрать новый моном m, такой что $m(\vec{a}_j) = p_j$ для всех $j = 1, \ldots, l$ и

$m(\vec{a}_j) < p'(\vec{a}_j)$ для всех $j > l$. Тогда многочлен $p = p' \oplus m$ имеет корни во всех точках S. Этот многочлен содержит $1 + \left\lceil \frac{2(s-n)}{(n+1)} \right\rceil + 1 \leqslant \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$ мономов.

Наконец, если $l \geqslant n+1$, положим $p_0 = \max_{j \leqslant l} p_j$. Применяя утверждение выше, рассмотрим пару новых различных мономов m_1 и m_2, таких что $m_1(\vec{x}) = m_2(\vec{x}) = p_0$ для всех $\vec{x} \in \pi$ и $m_1(\vec{a}_j), m_2(\vec{a}_j) < p'(\vec{a}_j)$ для всех $j > l$. Тогда многочлен $p = p' \oplus m_1 \oplus m_2$ имеет корни во всех точках S. Этот многочлен содержит не больше $2 + \left\lceil \frac{2(s-n-1)}{(n+1)} \right\rceil + 1 = \left\lceil \frac{2s}{(n+1)} \right\rceil + 1$ мономов.

Во всех трех случаях мы построили многочлен с требуемым количеством мономов. ■

В доказательстве предыдущей теоремы возможно некоторое улучшение параметров. Например, для $n = 2$ мы можем доказать следующее.

Теорема 8.6. *Для $n = 2$ верно $k(s, 2) \leqslant \left\lceil \frac{s}{2} \right\rceil + 1$. Для размера минимального универсального тестирующего множества для многочленов двух переменных верно следующее неравенство: $s \geqslant 2(k-1) + 1$.*

Доказательство. Доказательство эквивалентности двух утверждений теоремы аналогично доказательству похожего утверждения для теоремы 8.5.

Для доказательства первого утверждения мы используем тот же подход, что и в доказательстве теоремы 8.5. Мы проводим такой же разбор случаев на шаге индукции. Заметим, что первые два случая переносятся полностью.

Так что нам остается лишь разобрать случай, в котором $l > 2$ и P содержит не все точки S. Существует прямая π в $\mathbb{Q}^2$, содержащая точки $\vec{a}_1, \ldots, \vec{a}_l$, и такая что все точки в $S \setminus \{\vec{a}_1, \ldots, \vec{a}_l\}$ лежат в одной полуплоскости относительно π. Рассмотрим среди точек $S \setminus \{\vec{a}_1, \ldots, \vec{a}_l\}$ ближайшую к прямой π. Проведем прямую π' параллельную π через эту точку. Если на π' лежит несколько точек S, рассмотрим ту, которая не лежит между какими-то двумя другими. Для простоты обозначений пусть это точка $\vec{a}_{l+1}$. Обозначим множество оставшихся точек через $S' = \{\vec{a}_{l+2}, \ldots, \vec{a}_s\}$ и применим к S' предположение индукции. Как и раньше положим $p_j = p'(\vec{a}_j)$.

Рассмотрим новый моном m_1 (напомним, что мономы, это просто аффинные функции на $\mathbb{Q}^2$), такой что $m_1(\vec{a}_{l+1}) = p_{l+1}$, $m_1(\vec{a}_j) \leqslant p_j$ для всех $\vec{a}_j \in S \cap \pi'$, $m_1(\vec{a}_j) \leqslant p_j$ для всех $\vec{a}_j \in S' \setminus \pi$ и $m_1(\vec{a}_j) \geqslant p_j$ для всех $j \leqslant l$. Заметим, что это возможно по утверждению выше, поскольку $\vec{a}_1, \ldots, \vec{a}_l$ и $S' \setminus \pi$ лежат в разных полуплоскостях относительно π'. Наконец, выберем еще один новый моном m_2, такой что $m_1(\vec{x}) = m_2(\vec{x})$ для всех $\vec{x} \in \pi$ и $m_2(\vec{a}_j) \leqslant p_j$ для всех $j > l$. Тогда многочлен $p = p' \oplus m_1 \oplus m_2$ имеет корни во всех точках S. Этот многочлен содержит не больше чем

$$2 + \left\lceil \frac{s-4}{2} \right\rceil + 1 = \left\lceil \frac{s}{2} \right\rceil + 1$$

мономов. ■

Ниже мы увидим, что эта оценка точна.

Теперь перейдем к нижним оценкам на $k(s, n)$. Мы докажем следующую оценку.

Теорема 8.7. *Верно неравенство* $k(s, n) \geqslant \left\lceil \frac{s}{n+1} \right\rceil$.

Эквивалентно, верно следующее неравенство для размера универсальноого тестового множества над $\mathbb{Q}$*:* $s \leqslant k(n+1) + 1$.

Доказательство. Заметим, что два утверждения теоремы эквиваленты. Действительно, по определению $k(s, n)$ первое утверждение эквивалентно тому, что для всякого k и s, если $k < \left\lceil \frac{s}{n+1} \right\rceil$, то существует тестовое множество размера s для многочленов с не более чем k мономами. Это неравенство можно переписать как $s \geqslant k(n+1) + 1$. Тогда утверждение эквивалентно тому, что минимальный размер тестового множества s для многочленов с не более чем k мономами удовлетворяет неравенству $s \leqslant k(n+1) + 1$.

Дальше мы доказываем первое утверждение теоремы. В рамках этого доказательства мы временно перейдем к многочленам над $\mathbb{R}$. Также здесь мы будем допускать действительные степени многочленов. Пусть для всякого множества

$S = \{\vec{a}_1, \ldots, \vec{a}_s\} \in \mathbb{R}^n$ существует многочлен с k мономами, имеющий корни во всех s точках.

Множество всех наборов $\vec{a}_1, \ldots, \vec{a}_s$ из s точек в $\mathbb{R}^n$ образует sn-мерное пространство над $\mathbb{R}$. Пусть многочлен p с мономами $m_1, \ldots, m_k$ имеет корни во всех точках $\vec{a}_1, \ldots, \vec{a}_s$. Это означает, что для всякой точки $\vec{a}_j$ есть два монома, значения которых в этой точке равны. *Конфигурацией* мы назовем сопоставление каждой точке $\vec{a}_j$ пары мономов m_{i_1}, m_{i_2} и координаты l, таких что $m_{i_1}(\vec{a}_j) = m_{i_2}(\vec{a}_j)$ и степень x_l в m_{i_1} больше степени x_l в m_{i_2} как минимум на 1 (это нужно, чтобы гарантировать, что m_{i_1} и m_{i_2} — различные мономы). Всякая конфигурация задается множеством наборов (j, i_1, i_2, l), где $1 \leqslant j \leqslant s$, $1 \leqslant i_1, i_2 \leqslant k$ и $1 \leqslant l \leqslant n$, так что различных конфигураций конечно.

Рассмотрим $(sn + k(n + 1))$-мерное пространство, задаваемое наборами $\vec{a}_1, \ldots, \vec{a}_s$ и $J_1, c_1, \ldots, J_k, c_k$, где J_i — вектор степеней монома m_i и c_i — свободный член этого монома. Для всякой конфигурации мы можем рассмотреть полуалгебраическое множество (множество, заданное конечной булевой комбинацией алгебраических уравнений и неравенств), заданное равенствами $m_{i_1}(\vec{a}_j) = m_{i_2}(\vec{a}_j)$ и неравенствами $J_{i_1,l} - J_{i_2,l} \geqslant 1$ для всех наборов (j, i_1, i_2, l) в конфигурации. По нашему предположению всякая точка $(\vec{a}_1, \ldots, \vec{a}_s)$ лежит в проекции одного из этих полуалгебраических множеств.

Заметим, что во всех точках каждое из этих полуалгебраических множеств имеет размерность не больше $k(n + 1) + s(n - 1)$. Действительно, мы можем рассмотреть следующее множество локальных координат. Мы включаем в это множество все координаты из $J_1, c_1, \ldots, J_k, c_k$ (их $k(n+1)$). Для всякого a_j мы можем рассмотреть соответствующий набор (j, i_1, i_2, l) и включить в множество локальных координат все координаты a_j, кроме l-й координаты. Заметим, что l-я координата может быть выражена через остальные с помощью равенства $m_{i_1}(\vec{a}_j) = m_{i_2}(\vec{a}_j)$, благодаря неравенству $J_{i_1,l} - J_{i_2,l} \geqslant 1$.

Таким образом, всякое полуалгебраическое множество имеет размерность не больше $k(n + 1) - s(n - 1)$. По теореме Тарского проекция полуалгебраическо-

го множества также является полуалгебраическим множеством, и размерность при взятии проекции не возрастает (см., напр., [15]). Так что по нашему предположению мы можем покрыть все точки $(\vec{a}_1, \ldots, \vec{a}_s)$ в sn-мерном пространстве конечным числом множеств размерности не больше $k(n+1) - s(n-1)$. Если между размерностями выполнено неравенство

$$k(n+1) + s(n-1) < sn,$$

то это невозможно, а значит, есть набор точек S (над $\mathbb{R}$), такой что всякий многочлен p с не более чем k мономами имеет не корень в S. Нам осталось доказать, что существует набор S и над $\mathbb{Q}$, обладающий тем же свойством.

Для этого рассмотрим наши полуалгебраические множества в координатах $\vec{a}_1, \ldots, \vec{a}_s$ и рассмотрим их замыкания. Они также являются полуалгебраическими множествами и их размерность также не больше $k(n+1) + s(n-1)$. Так что дополнение их объединения в $\mathbb{R}^{sn}$ (которое не пусто благодаря неравенству между размерностями) является открытым множеством и содержит каждую точку $(\vec{a}_1, \ldots, \vec{a}_s)$ вместе с окрестностью. Остается заметить, что эта окрестность содержит точку с рациональными координатами. ■

Дальше мы докажем точную оценку для случая $n = 2$.

Пусть для некоторого множества точек $S = \{\vec{a}_1, \ldots, \vec{a}_s\} \subseteq \mathbb{Q}^n$ существует многочлен p с мономами $m_1, \ldots, m_k$, имеющий корни во всех точках S.

Напомним, что график p в $(n+1)$-мерном пространстве — это кусочно-линейная функция. Всякий линейный фрагмент является многогранником и соответствует моному, а корнями многочлена являются точки негладкости функции, то есть точки на гранях многогранников. Рассмотрим множество всех корней p в $\mathbb{Q}^n$. Они разделяют пространство $\mathbb{Q}^n$ на не более чем k выпуклых (возможно, неограниченных) многогранника. Всякий многогранник соответствует одному из мономов m и состоит из всех точек $\vec{a} \in \mathbb{Q}^n$, таких что $m(\vec{a}) = p(\vec{a})$. Заметим, что любые два таких многогранника *отделены* плоскостью: если мно-

гогранники соответствуют мономам m_i и m_j, то первый лежит в полупространстве $m_i(\vec{x}) \leqslant m_j(\vec{x})$, а второй лежит в полупространстве $m_i(\vec{x}) \geqslant m_j(\vec{x})$.

Рассмотрим многогранник, соответствующий моному m_i. Рассмотрим все точки из S, лежащие на его границе, и рассмотрим их выпуклую оболочку. Мы получаем меньший (и уже ограниченный) выпуклый многогранник, который мы будем обозначать через P_i.

Таким образом, начав с p, мы получили множество попарно отделимых многогранников $P_1, \ldots, P_k$ с вершинами в S, не содержащими точек S в своих внутренностях (здесь мы рассматриваем многогранники в n-мерном пространстве и их n-мерные внутренности, то есть $\vec{a}$ лежит во внутренности, если его n-мерная ϵ-окрестность лежит в многограннике для достаточно маленького $\epsilon > 0$; так что возможно такое, что некоторые многогранники имеют пустую внутренность). Утверждение, что p имеет корни во всех точках S означает, что всякая точка S принадлежит как минимум двум из многогранников $P_1, \ldots, P_k$.

Этим анализом мотивируется следующее определение. *Двойным покрытием* ограниченными выпуклыми многогранниками данного множества S из s точек в n-мерном пространстве называется семейство многогранников $P_1, \ldots, P_k$, такое что они попарно отделены, и каждая точка в S лежит на границе как минимум двух многогранников (если многогранник лежит в $(n-1)$-мерном подпространстве, его граница совпадает со всем многогранником). Здесь мы говорим, что многогранники P и Q *отделены*, если существует гиперплоскость π, такая что P и Q лежат в разных замкнутых полупространствах относительно π. В частности, P и Q могут пересекаться только по точкам π, а значит, только по своим границам. *Размером* покрытия называется число k многогранников в нем. Обозначим через $k_2(s, n)$ минимальное число многогранников, достаточное для двойного покрытия любых s точек в n мерном пространстве. Из анализа выше сразу вытекает неравенство $k(s, n) \geqslant k_2(s, n)$ для всех s и n: из многочлена мы можем изготовить двойное покрытие многогранниками того же размера.

Эта связь с покрытиями многогранниками позволяет нам найти точное значение размера минимального универсального тестирующего множества для случая $n = 2$.

Теорема 8.8. *Верны неравенства* $k(s, 2) \geqslant k_2(s, 2) \geqslant \left\lceil \frac{s}{2} \right\rceil + 1$.

Следовательно, для $n = 2$ *размер минимального универсального тестирующего множества равен* $s = 2k - 1$.

Оставшаяся часть этого раздела посвящена доказательству теоремы 8.8.

Вторая часть теоремы сразу вытекает из первой части и теоремы 8.6.

Так что остается доказать, что $k_2(s, 2) \geqslant \left\lceil \frac{s}{2} \right\rceil + 1$.

В качестве универсального тестирующего множества из s точек в $\mathbb{Q}^2$ мы возьмем множество вершин произвольного выпуклого многоугольника M.

Предположим, что есть двойное покрытие вершин M с помощью k выпуклых многоугольников. Среди этих многоугольников будем разделять множество E тех, которые являются ребрами M, и множество T остальных многоугольников. Введем обозначения $|E| = k_1$ и $|T| = k_2$, так что $k = k_1 + k_2$. Обозначим через W суммарное количество вершин во всех многоугольниках в T.

Мы докажем следующую лемму.

Лемма 8.3. *Для* $s \geqslant 2$ *верно* $W \leqslant s + 2k_2 - 2$.

Но сначала покажем, почему этой леммы достаточно для завершения доказательства нижней оценки на $k_2(s, 2)$.

Заметим, что всякий многоугольник в E имеет две вершины. Так что суммарное количество вершин во всех многоугольниках в E равно $2k_1$. Суммарное количество вершин во всех многоугольниках в T по определению равно W. Каждая вершина в M должна быть вершиной как минимум двух многоугольников в E и T. Так что суммарное количество вершин во всех многоугольниках в E и T не меньше $2s$. Таким образом, мы получаем, что

$$2s \leqslant 2k_1 + W \leqslant 2k_1 + s + 2k_2 - 2,$$

где второе неравенство вытекает из леммы 8.3. Из этого мы получаем

$$k = k_1 + k_2 \geqslant \frac{s}{2} + 1.$$

Поскольку k — целое, мы получаем $k \geqslant \left\lceil \frac{s}{2} \right\rceil + 1$, что и требовалось для завершения доказательства теоремы.

Таким образом, нам остается доказать лемму.

Доказательство леммы 8.3. Доказательство проходит индукцией по s.

Базой является случай $s = 2$ (вырожденный многоугольник). Тогда $T = \emptyset$, $k_2 = 0$, $W = 0$, и неравенство верно.

Рассмотрим $s \geqslant 3$. Если $k_2 = 0$, то $W = 0$, и неравенство очевидно верно. Предположим, что $k_2 \geqslant 1$ и выберем произвольный многоугольник P из T. Обозначим через r количество вершин в P. Тогда P разбивает остальную часть M на r отдельных выпуклых многоугольников (возможно, вырожденных, то есть содержащих лишь 2 вершины) $M_1 \ldots, M_r$. Обозначим число вершин в них через $s_1, \ldots, s_r$ соответственно. Заметим, что

$$s_1 + \ldots + s_r = s + r. \tag{8.6}$$

Предположим, что многоугольники $M_1, \ldots, M_r$ содержат $t_1, \ldots, t_r$ многоугольников из T соответственно. Обозначим множества этих многоугольников соответственно через $T_1, \ldots, T_r$. Тогда

$$t_1 + \ldots + t_r = k_2 - 1. \tag{8.7}$$

Обозначим через W_i суммарное число вершин в многоугольниках из T_i для $1 \leqslant i \leqslant r$. Тогда

$$W_1 + \ldots + W_r = W - r. \tag{8.8}$$

По предположению индукции для всякого M_i верно следующее неравенство:

$$W_i \leqslant s_i + 2t_i - 2. \tag{8.9}$$

Суммируя неравенства (8.9) для всех $i = 1, \ldots, r$ и применяя (8.6)-(8.8), получаем, что

$$W - r \leqslant (s + r) + 2(k_2 - 1) - 2r,$$

то есть

$$W \leqslant s + 2k_2 - 2,$$

и лемма доказана. ■

Глава 9

Мин-плюс линейные системы

9.1 Циклические игры

В этом разделе мы определим циклические игры, которые потребуются нам в этой главе.

Циклическая игра задается задается двудольным ориентированным графом $G = (V, E)$ с долями V_1 и V_2, некоторой фиксированной начальной вершиной $v \in V$ и функцией $w\colon E \to \mathbb{R}$, приписывающей веса ребрам графа G (см. рисунок 9.1). В начале игры в начальную вершину v помещается фишка. На каждом шаге один из двух игроков перемещает фишку в другую вершину графа вдоль ребра. Более точно, каждый ход устроен следующим образом. Если фишка находится в некоторой вершине $u \in V_1$, то первый игрок (Алиса) передвигает ее в любую вершину w, такую что $(u, w) \in E$. Если, с другой стороны, $u \in V_2$, то второй игрок (Боб) передвигает ее в любую вершину w, такую что $(u, w) \in E$. Игра продолжается бесконечно, и партия в игре описывается последовательностью вершин $v_0, v_1, v_2, \ldots$, по которым прошла фишка. Заметим, что $v_0 = v$. Первый игрок выигрывает, если

$$\liminf_{n\to\infty} \frac{1}{t} \sum_{i=1}^{t} w(v_{i-1}, v_i) > 0. \tag{9.1}$$

Если предел равен нулю, то объявляется ничья. Иначе выигрывает второй игрок. С циклической игрой связана задача определения победителя в этой игре, то есть определение игрока, у которого есть выигрышная стратегия (в алгоритмической задаче мы считаем, что веса на ребрах целые или рациональные).

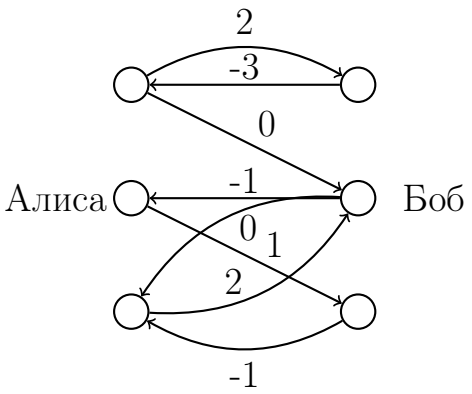


Рисунок 9.1: Пример циклической игры.

В игре на рисунке 9.1, если игра начинается в левой верхней вершине, то Алисе не выгодно ходить в правую верхнюю вершину, потому что Боб переведет фишку обратно и в совокупности наберет на одно очко больше. Если Алиса пойдет в среднюю вершину справа, то нетрудно видеть, что она выиграет при любой игре Боба. Так что в этой игре побеждает Алиса.

Циклические игры активно изучаются в теории сложности вычислений (см. подробнее в [86]). В частности, известно, что у игроков есть оптимальные позиционные стратегии, то есть стратегии, зависящие только от текущего положения фишки, но не от истории предыдущих ходов. Из этого в частности следует, что для целых весов на ребрах оптимальное значение в игре (значение предела в (9.1), которого при правильной игре могут достичь оба игрока) является рациональным числом со знаменателем, полиномиальным от числа вершин в G. Также отсюда несложно выводится, что задача определения победителя в циклических играх лежит в $\mathsf{NP} \cap \mathsf{coNP}$ (в качестве сертификатов можно взять выигрышные стратегии игроков). Лежит ли эта задача в P, является важным открытым вопросом. Известно, что задача определения победителя в циклических играх эквивалентна задаче разрешимости систем линейных мин-плюс неравенств.

9.2 Мин-плюс многочлены и мин-плюс уравнения

В этом разделе мы покажем, что есть тесная связь между множествами корней мин-плюс многочленов и множествами решений мин-плюс уравнений. Эта связь устанавливается для многочленов произвольной степени, но также переносится и на линейные многочлены. В частности, из этой связи мы выведем результат о том, что задача проверки разрешимости мин-плюс линейных систем многочленов эквивалентна задаче о циклических играх.

Мы начнем со следующего наблюдения о связи между системами мин-плюс уравнений и мин-плюс неравенств.

Лемма 9.1. *Для любой системы мин-плюс уравнений F существует система мин-плюс неравенств G от того же множества переменных, той же степени и с тем же множеством решений.*

Для любой системы мин-плюс неравенств G существует система мин-плюс уравнений F от того же множества переменных, той же степени и с тем же множеством решений.

Для любой линейной системы мин-плюс уравнений $A \odot \vec{x} = B \odot \vec{x}$ существует линейная система мин-плюс неравенств $C \odot \vec{x} \geqslant D \odot \vec{x}$ с тем же множеством решений.

Для любой линейной системы мин-плюс неравенств $C \odot \vec{x} \geqslant D \odot \vec{x}$ существует линейная система мин-плюс уравнений $A \odot \vec{x} = B \odot \vec{x}$ с тем же множеством решений.

Все перечисленные утверждения верны над полукольцами без ∞ и с ∞. Во всех утверждениях новые системы можно построить по старым за полиномиальное время.

Доказательство. Начнем с перехода от уравнений к неравенствам. Рассмотрим произвольное мин-плюс уравнение $f(x) = g(x)$. Нетрудно видеть, что оно

эквивалентно паре неравенств $f(x) \geqslant g(x)$ и $g(x) \geqslant f(x)$. Сделав такую замену для каждого уравнения в системе, мы получаем эквивалентную систему неравенств. Легко видеть, что все условия леммы выполняются.

В другую сторону, рассмотрим произвольное мин-плюс неравенство $L_1(x) \geqslant L_2(x)$. Нетрудно видеть, что оно эквивалентно мин-плюс уравнению $\min(L_1(x), L_2(x)) = L_2(x)$. Сделав такую замену для каждого неравенства в системе, мы получаем эквивалентную систему уравнений. Легко видеть, что все условия леммы выполняются.

Также легко видеть, что эти конструкции работают и для линейных систем. Ясно, что описанные конструкции эффективны. ■

Перейдем к доказательству связи между мин-плюс многочленами и мин-плюс уравнениями. Начнем с перехода от многочленов к уравнениям.

Лемма 9.2. *Если задана система мин-плюс многочленов, мы можем построить систему мин-плюс уравнений над тем же множеством переменных, с тем же множеством корней и той же степени. Новую системы можно построить по старой за полиномиальное время.*

Доказательство. Пусть T — некоторая система мин-плюс многочленов. Для всякого многочлена $f \in T$ мы построим систему мин-плюс уравнений над тем же множеством переменных, эквивалентную f.

Пусть

$$f = \min\{l_1, l_2, \ldots, l_m\}, \tag{9.2}$$

где l_i — мин-плюс мономы.

Нетрудно видеть, что минимум в (9.2) достигается как минимум дважды тогда и только тогда, когда для всех $i = 1, \ldots, m$ верно

$$\begin{aligned} &\min\{l_1, ..., l_{i-1}, l_i, l_{i+1}, ..., l_m\} = \\ &\min\{l_1, ..., l_{i-1}, l_{i+1}, ..., l_m\}. \end{aligned} \tag{9.3}$$

Таким образом, эти уравнения задают эквивалентную систему мин-плюс уравнений. Чтобы получить мин-плюс систему уравнений, эквивалентную всей системе многочленов, мы просто объединяем приведенные системы для всех многочленов в T.

Это работает над полукольцами с без ∞ и с ∞. Ясно, что конструкция эффективна. ■

Мы также можем доказать аналогичный результат для линейных систем.

Лемма 9.3. *Над полукольцами без ∞ и с ∞ для любой линейной системы мин-плюс многочленов $A \odot \vec{x}$ мы можем построить линейную мин-плюс систему уравнений $B \odot \vec{x} = C \odot \vec{x}$ с тем же множеством корней. Эта система может быть найдена по системе многочленов за полиномиальное время.*

Доказательство. Для случая полуколец с бесконечностью мы можем просто воспользоваться леммой 9.2.

Для случая полуколец без бесконечности возникает дополнительная трудность, что мы дополнительно требуем, чтобы все переменные присутствовали в линейной системе с конечным коэффициентом. Чтобы преодолеть эту трудность, мы просто используем вместо (9.3) равенство

$$\min\{l_1, ..., l_{i-1}, l_i, l_{i+1}, ..., l_m\} =$$
$$\min\{l_1, ..., l_{i-1}, l_i + \epsilon, l_{i+1}, ..., l_m\},$$

для произвольного положительного ϵ.

В этом равенстве для линейного случая сохраняются все переменные, в отличие от равенства (9.3). При этом это равенство эквивалентно (9.3). ■

Теперь перейдем к преобразованию систем уравнений в системы многочленов. В эту сторону у нас нет такой простой взаимосвязи, но тем не менее мы можем доказать следующую лемму.

Лемма 9.4. *Над $\mathbb{R}$ для любой системы мин-плюс уравнений F от n переменных существует система мин-плюс многочленов T от $2n$ переменных той*

же степени и инъективное линейное отображение $H\colon \mathbb{R}^n \to \mathbb{R}^{2n}$*, такие что образ множества решений* F *под действием* H *совпадает с множеством корней* T*. То же самое верно для остальных полуколец. Эта конструкция эффективна и может быть вычислена за полиномиальное время.*

Доказательство. Сначала для данной системы мин-плюс уравнений F мы построим соответствующую систему многочленов T, а затем докажем требуемое утверждение о связи между F и T.

Обозначим переменные в F через $(x_1, \ldots, x_n)$. Система мин-плюс многочленов T для каждой переменной x_i системы F будет содержать две переменные x_i и x'_i, то есть переменными T являются $(x_1, \ldots, x_n, x'_1, \ldots, x'_n)$.

Система T состоит из следующих многочленов.

1. Для всякого $i = 1, \ldots, n$ мы добавляем в T многочлен

$$x_i \oplus x'_i. \tag{9.4}$$

2. Пусть $(\min_j m_j(\vec{x}), \min_p l_p(\vec{x}))$ — произвольное уравнение в F. Для всякого p мы добавляем в T мин-плюс многочлен

$$\min\left(m_1(\vec{x}), m_1(\vec{x}'), \ldots, m_k(\vec{x}), m_k(\vec{x}'), l_p(\vec{x})\right). \tag{9.5}$$

   Для всякого j мы добавляем в T мин-плюс многочлен

$$\min\left(l_1(\vec{x}), l_1(\vec{x}'), \ldots, l_t(\vec{x}), l_t(\vec{x}'), m_j(\vec{x})\right). \tag{9.6}$$

   Будем называть мономы $m_1, \ldots, m_k$ в этих многочленах m-мономами, а мономы $l_1, \ldots, l_t$ будем называть l-мономами.

Это завершает построение T. Легко видеть, что это построение эффективно. Заметим, что максимальная степень многочленов в T равна максимальной степени уравнений в F.

Теперь перейдем к доказательству взаимосвязи между F и T.

Положим $H(\vec{a}) = (\vec{a}, \vec{a})$ для всех $\vec{a}$. Ясно, что H — инъективное линейное отображение.

Заметим, что входной набор является корнем многочлена $x_i \oplus x'_i$ в T тогда и только тогда, когда $x_i = x'_i$. Следовательно, все корни T лежат в образе H.

Если есть решение $\vec{a}$ системы F, то нетрудно видеть, что его образ $(\vec{a}, \vec{a})$ под действием H является корнем многочленов вида (9.5) и (9.6) в T. Действительно, поскольку $\min_j m_j(\vec{a}) = \min_p l_p(\vec{a})$, то существует j, такое что $m_j(\vec{a}) = \min_p l_p(\vec{a})$. Тогда минимум в соответствующих многочленах (9.5) будет достигаться на мономах $m_j(\vec{x})$ и $m_j(\vec{x}')$. Симметричное рассуждение работает для многочленов вида (9.6).

В обратную сторону, если есть корень T, как мы уже заметили, он должен иметь форму$(\vec{a}, \vec{a})$. Тогда нетрудно видеть, что для каждого мин-плюс уравнения в F верно $\min_j m_j(\vec{a}) = \min_p l_p(\vec{a})$. Действительно, поскольку для соответствующих мин-плюс многочленов (9.5) мы имеем корень, верно, что $\min_j m_j(\vec{a}) \leqslant \min_p l_p(\vec{a})$. С другой стороны, многочлены (9.6) гарантируют, что

$$\min_j m_j(\vec{a}) \geqslant \min_p l_p(\vec{a}).$$

Доказательство работает для все полуколец, как с ∞, так и без. ■

В частности, мы доказали, что множества корней систем мин-плюс многочленов и множества решений систем мин-плюс уравнений топологически эквивалентны.

Для случая линейных систем у нас снова возникнет техническая трудность для случая полуколец без ∞, состоящая в том, что мы требуем, чтобы в матрицах все ячейки были конечны. Для преодоления этой трудности мы докажем следующую вспомогательную лемму.

Лемма 9.5. *Пусть $k \leqslant n$, рассмотрим вектор $\vec{a} = (a_1, \ldots, a_k) \in \mathbb{R}^k$. Тогда для любого $C \in \mathbb{R}$ существует система мин-плюс линейных многочленов $A \in \mathbb{R}^{m \times n}$, где $m = n - k + 1$, такая что*

- *для всякого $i \in [m]$ и всякого $j \in [k]$ верно, что $a_{ij} = a_j$;*
- *для всякого $i \in [m]$ и всякого $j \in [n] \setminus [k]$ верно, что $a_{ij} \geqslant C$;*
- *для всякого решения A и всякой строки системы минимум достигается дважды в $\vec{a}$-части строки.*

То же самое выполняется для всех остальных полуколец.

Доказательство. Для доказательства леммы мы сначала определим несколько мин-плюс линейных многочленов. Система A будет состоять из всех них. Во-первых, рассмотрим многочлен с таким вектором коэффициентов

$$l_0 = (\vec{a}, C+1, \ldots, C+1),$$

где $l_0 \in \mathbb{R}^n$. Дальше, для всякого $i = k+1, \ldots, n$ положим

$$l_i = l_0 - e_i = (\vec{a}, C+1, \ldots, C, \ldots, C+1),$$

где $e_i \in \mathbb{R}^n$ — вектор с единицей на позиции i и нулями в остальных координатах. Положим A равной системе, состоящей из уравнений $l_0, l_{k+1}, \ldots, l_n$.

Для удобства, мы выписываем пример системы A с $n = 6$, $k = 3$, $\vec{a} = (1, 2, 3)$ и $C = 9$:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 10 & 10 & 10 \\ 1 & 2 & 3 & 9 & 10 & 10 \\ 1 & 2 & 3 & 10 & 9 & 10 \\ 1 & 2 & 3 & 10 & 10 & 9 \end{array}\right).$$

Предположим противное, что A имеет корень, такой что в некоторой строке l_i есть всего один минимум в $\vec{a}$-части. Это означает, что в этой строке есть минимум в столбце j, таком что $k+1 \leqslant j \leqslant n$. Если $j - k \neq i$, рассмотрим строку l_j. Легко видеть, что в этой строке будет ровно один минимум (в столбце j), что дает противоречие. Таким образом, минимум в строке l_i вне $\vec{a}$-части может

быть расположен только в столбце $i + k$ (эта ячейка соответствует одной из ячеек с числом 9 в примере выше), в частности $i \neq 0$. Но поскольку минимум в строке достигается дважды, должен быть еще хотя бы один минимум в $\vec{a}$-части l_i. То есть, есть ровно один минимум в $\vec{a}$-части строки l_i и еще один минимум в столбце $i+k$. Теперь рассмотрим строку l_0. Нетрудно видеть, что в этой строке тогда будет ровно один минимум, что дает противоречие.

Видно, что рассуждение проходит над любым полукольцом. ■

Мы будем говорить, что множества S и T векторов размерности n являются C-эквивалентными для некоторого числа $C > 0$, если $S \cap \mathbb{R}_{\leqslant C} = T \cap \mathbb{R}_{\leqslant C}$, где через $\mathbb{R}_{\leqslant C}$ мы обозначаем множество векторов, все координаты которых по абсолютному значению не больше C.

Лемма 9.6. *Для случая полукольца $\mathbb{R}$ для всякой системы мин-плюс уравнений $A \odot \vec{x} = B \odot \vec{x}$ от n переменных и для всякого C' существует система мин-плюс многочленов $D \odot \vec{x}$ от $2n$ переменных и инъективное линейное отображение $H\colon \mathbb{R}^n \to \mathbb{R}^{2n}$, такие что все корни системы $D \odot \vec{x}$ лежат в $Im(H)$, а также образ множества решений системы (A, B) под действием H C'-эквивалентен множеству корней системы $D \odot \vec{x}$.*

Для случая полукольца $\mathbb{R}_\infty$ для всякой системы мин-плюс уравнений $A \odot \vec{x} = B \odot \vec{x}$ от n переменных существует система мин-плюс многочленов $D \odot \vec{x}$ от $2n$ переменных и инъективное линейное отображение $H\colon \mathbb{R}^n_\infty \to \mathbb{R}^{2n}_\infty$, такие что все корни системы $D \odot \vec{x}$ лежат в $Im(H)$, а образ множества решений системы (A, B) под действием H совпадает с множеством корней системы $D \odot \vec{x}$.

Аналогичные утверждения верны и для остальных полуколец. При этом конструкции эффективны.

Доказательство. Для случая полукольца $\mathbb{R}_\infty$ мы можем просто воспользоваться результатом леммы 9.4.

Для случая полукольца $\mathbb{R}$ нам нужно решить проблему, что при применении леммы 9.4 мы получаем многочлены, в которых присутствуют не все переменные.

Для того чтобы решить эту проблему, для каждого многочлена из конструкции в доказательстве леммы 9.4, в котором присутствуют не все переменные, мы заменяем этот многочлен на систему по лемме 9.5 с $C = 2C'$ так, чтобы в получившихся многочленах присутствовали все переменные. Заметим, что такую замену нужно делать только для многочленов вида (9.4).

Проверим теперь, что получающаяся система удовлетворяет всем необходимым условиям.

Заметим, что система, построенная нами для многочлена $x_i \oplus x'_i$, гарантирует, что в любом корне системы с матрицей D верно, что $x_i = x'_i$. Следовательно, все корни D лежат в образе H.

Если есть решение $\vec{a}$ системы $A \odot \vec{x} = B \odot \vec{x}$ в $\mathbb{R}_{\leqslant C}$, то аналогично доказательству леммы 9.4, его образ $(\vec{a}, \vec{a})$ под действием H является корнем многочленов вида (9.5) и (9.6) в T. Также в силу ограничения на абсолютные значения координат вектора $\vec{a}$, вектор $(\vec{a}, \vec{a})$ также будет корнем многочленов, добавленных для многочленов вида (9.4).

В обратную сторону, если есть корень T, как мы уже заметили, он должен иметь форму$(\vec{a}, \vec{a})$. Доказательство того, что вектор $\vec{a}$ является решением $A \odot \vec{x} = B \odot \vec{x}$ полностью аналогично доказательству леммы 9.4.

Ясно, что рассуждения проходят и для других полуколец, а также, что конструкция эффективна. ■

Из полученных результатов для линейных систем мы можем вывести результаты о сложности задачи разрешимости для мин-плюс линейных систем многочленов.

Определение 9.1. *В задаче* TropSolv *на вход подается матрица* $A \in \mathbb{Z}^{m\times n}$ *(или из* $\mathbb{Q}^{m\times n}$*). Требуется определить, есть ли у соответствующей мин-плюс системы линейных многочленов решение.*

Аналогично определяется задача над $\mathbb{Z}_\infty$ *или* $\mathbb{Q}_\infty$*. Мы обозначаем ее через* TropSolv_∞.

Следствие 9.7. *Задачи* TropSolv *и* TropSolv_∞ *полиномиально эквивалентны задаче о циклических играх.*

Доказательство. Как мы указывали, разрешимость систем линейных мин-плюс неравенств полиномиально эквивалентна задаче о циклических играх. По лемме 9.1 то же самое можно утверждать о задачах разрешимости систем линейных мин-плюс уравнений.

В силу леммы 1.2, если для линейной системы есть решение, то есть решение с координатами, ограниченными полиномом от размера коэффициентов в системе. Тогда леммы 9.3 и 9.6 дают нам полиномиальную эквивалентность задач разрешимости для мин-плюс линейных систем уравнения и мин-плюс линейных систем многочленов. Это завершает доказательство. ■

9.3 Комбинаторное описание размерности множества корней

В нашем анализе будет удобно использовать следующее определение.

Определение 9.2. *Пусть* A *– матрица размера* $m \times n$ *над* $\mathbb{R}$*. Мы связываем с ней таблицу* A^* *того же размера* $m \times n$*, в которой мы помещаем* $*$ *в ячейку* (i, j) *тогда и только тогда, когда* $a_{ij} = \min_k a_{ik}$*, и мы оставляем ячейку пустой в противном случае.*

Таблица A^* отражает важные для нас свойства линейной мин-плюс системы многочленов с матрицей A. Например, вектор $x = (x_1, \ldots, x_n)$ является корнем

системы $A \odot \vec{x}$ тогда и только тогда, когда в каждой строке таблицы $(\{a_{ij} + x_j\}_{ij})^*$ есть не меньше двух звездочек.

Ниже мы дадим комбинаторное описание локальной размерности (в данной точке) множества корней системы в терминах таблицы A^*. Для этого мы будем использовать следующую блочно-треугольную форму матрицы (которая существует тогда и только тогда, когда таблица, соответствующая матрице, содержит не меньше двух звездочек в каждой строке).

Определение 9.3. *Блочно-треугольной формой размера d матрицы A называется разбиение множества строк A на подмножества $R_1, R_2, \ldots, R_d$ (некоторые множества R_i могу быть пустыми) и разбиение множества столбцов A на непустые подмножества $C_1, \ldots, C_d$ со следующими свойствами (см. рисунок 9.2):*

1. *для всякого i всякая строка в R_i содержит не меньше двух звездочек в столбцах C_i в A^*;*

2. *если $1 \leqslant i < j \leqslant d$, то строки в R_i не содержат звездочек в столбцах C_j в A^*.*

Например, для таблицы

$$\left(\begin{array}{c|c|c|c|c} * & & & * & \\ * & & * & & \\ & * & & * & * \end{array}\right)$$

существует блочно-треугольная форма размера 2 с $C_1 = \{1, 3, 4\}, C_2 = \{2, 5\}, R_1 = \{1, 2\}, R_2 = \{3\}$. Есть и другая блочно-треугольная форма размера 2 с $C_1 = \{1, 2, 3, 4\}, C_2 = \{5\}, R_1 = \{1, 2, 3\}, R_2 = \emptyset$. Нетрудно видеть, что для этой таблицы нет блочно-треугольной формы размера 3.

Нас интересует блочно-треугольная форма матрицы с максимально возможным размером d. Сделаем несколько наблюдений о структуре блочно-треугольной формы максимального размера.

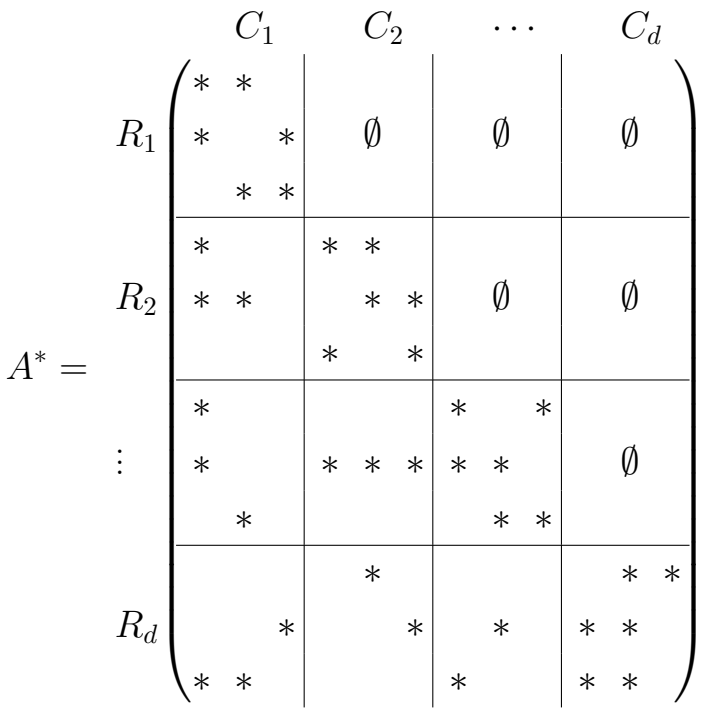


Рисунок 9.2: Блочно-треугольная форма.

— Без ограничения общности пары (C_i, R_i) с пустыми R_i можно перенести в начало списка, переставляя одинаковым образом список C_i и список R_i.

— Можно предполагать, что для пар с пустыми R_i верно, что $|C_i| = 1$. Действительно, если $|C_i| > 1$, мы можем разбить это множество на несколько множеств размера 1, и размер только увеличится.

Теперь мы готовы дать комбинаторное описание размерности множества корней системы.

Теорема 9.1. *Пусть нулевой вектор является корнем линейной мин-плюс системы многочленов с матрицей A над $\mathbb{R}$. Тогда локальная проективная размерность системы A в нулевой точке равна максимальному d, такому что существует блочно-треугольная форма для A размера $d + 1$.*

То же самое верно и для других полуколец.

Ясно, что случай произвольного корня сводится к случаю нулевого корня (можно рассмотреть матрицу $A_{\vec{x}}$, определенную в главе 1).

Для доказательства теоремы мы докажем следующую техническую лемму.

Лемма 9.8. *Во всяком конусе размерности k в пространстве $\mathbb{R}^n$ существует вектор с не менее чем k различными координатами.*

Доказательство леммы 9.8. Рассмотрим некоторое множество линейно независимых векторов $f^1, f^2, \ldots, f^k$ в конусе.

Для всякой координаты i этих векторов $f^1, \ldots, f^k$ рассмотрим набор $f_i = (f_i^1, \ldots, f_i^k)$ всех i-х координат векторов в этом наборе. Заметим, что $a = |\{f_1, f_2, \ldots, f_n\}| \geqslant k$, то есть, число различных векторов среди f_i не меньше k. Действительно, если число различных наборов f_i меньше k, мы можем рассмотреть векторное уравнение $\sum_i c_i f^i = \vec{0}$ для $c_i \in \mathbb{R}$ как линейную систему от переменных $c_1, \ldots, c_k$. Эта система имеет меньше k уравнений, и значит, имеет ненулевое решение. Это означает, что $f^1, \ldots, f^k$ линейно зависимы, что дает противоречие.

Далее, умножая все вектора f^j на положительное число, мы можем предполагать, что если $|f_i^j - f_{i'}^{j'}|$ не равно нулю, то оно не меньше 2. Обозначим $C = \max_{i,j,i',j'} |f_i^j - f_{i'}^{j'}|$.

Теперь мы можем рассмотреть вектор

$$f' = \sum_{j=1}^{k} C^{2j-2} f^j.$$

Мы утверждаем, что число различных координат f' не меньше k. Для этого мы докажем, что если $f_i \neq f_{i'}$, то $f_i' \neq f_{i'}'$. Действительно, пусть это не так. Тогда

$$\sum_{j=1}^{k} C^{2j-2}(f_i^j - f_{i'}^j) = 0. \tag{9.7}$$

Рассмотрим максимальное j, такое что $f_i^j - f_{i'}^j \neq 0$. Тогда соответствующий член в (9.7) больше C^{2j-2} по абсолютному значению. С другой стороны, каждый предыдущий член l не больше C^{2l-1}. Поскольку

$$C^{2j-2} > \sum_{l=1}^{2j-3} C^l$$

для $C \geqslant 2$, сумма в (9.7) не может быть равна нулю. Получаем противоречие. ■

Доказательство теоремы 9.1. Мы можем предполагать, что минимум в каждой строке A равен 0 (мы можем прибавить одно и то же число ко всем элементам строки), а положительные по абсолютному значению не меньше 1 (можно умножить ячейки на большое положительное число).

Обозначим через $d+1$ размер максимальной блочно-треугольной формы, и обозначим локальную проективную размерность множества корней в нулевом решении через $\dim A$.

Нетрудно видеть, что $\dim A \geqslant d$. Действительно, рассмотрим блочно-треугольную форму размера $d+1$ и возьмем в качестве базиса в множестве корней характеристические векторы множеств $\cup_{j \geqslant i} C_j$ для $i = 2, \ldots, d+1$, взятые с отрицанием. Легко видеть, что всякая точка конуса, порожденного этими векторами, достаточно близкая к нулевому вектору, является корнем системы.

Остается доказать, что $\dim A \leqslant d$. Рассмотрим многогранник (над $\mathbb{R}^n$) размерности $k = \dim A + 1$ в множестве корней, содержащий нулевую точку. Мы можем ограничиться рассмотрением конуса той же размерности с вершиной в нуле и такого, что окрестность вершины, пересеченная с конусом, лежит в этом многограннике. По лемме 9.8 мы можем найти вектор f' в этом конусе с $a \geqslant k$ различными координатами. Поделив вектор на достаточно большое число, мы можем гарантировать, что он лежит в множестве корней, и что все его координаты не больше 1 по абсолютному значению. Поскольку множество корней замкнуто относительно сдвига на вектор $c \cdot \vec{1} = (c, \ldots, c)$, мы можем также предполагать, что координаты f' неположительны. Перенумеруем координаты f' в возрастающем порядке: $b_1 < \ldots < b_a \leqslant 0$.

Обозначим через B_j для $j \in [a]$ множество координат f' со значением не больше b_j, то есть $B_j = \{l \in [n] \mid f'_l \leqslant b_j\}$. Заметим, что $B_1 \subset B_2 \subset \ldots \subset B_a$.

Утверждение. *Для всякого j и всякой строки l столбцы в B_j содержат в l либо ноль звездочек, либо не меньше двух звездочек в таблице A^*.*

Доказательство утверждения. Доказательство проходит индукцией по j.

Для базы индукции рассмотрим множество B_1. Заметим, что столбцы в B_1 — это в точности столбцы с минимальными координатами f'. Предположим, что существует звездочка в строке l в столбце из B_1. Прибавим к каждому столбцу i матрицы A i-ю координату f' (напомним, она неположительна). Поскольку f' — корень, получившаяся матрица должна иметь не меньше двух звездочек в строке l. Но звездочка в столбце из B_1 имеет значение b_1, а оно минимально возможное среди всех координат в строке l. Таким образом, должна быть еще одна координата с таким же значением, которая может быть только в столбцах из B_1, и может быть только звездочкой A. Таким образом, столбцы из B_1 содержат не меньше двух звездочек в строке l.

Для шага индукции предположим, что мы уже доказали утверждение для B_{j-1} и рассмотрим множество B_j. Если строка l содержит две звездочки в B_{j-1}, то она также содержит две звездочки в B_j. Таким образом, мы можем предполагать, что срока l не содержит звездочек в B_{j-1}. Предположим, что есть звездочка в B_j. Как и раньше, добавим координаты f' к соответствующим столбцам A. Поскольку в B_{j-1} звездочек нет, все соответствующие координаты в строке l в этих столбцах не меньше 1 (напомним, что координаты f' меньше 1). Звездочка в координате B_j имеет значение b_j, и это минимально возможное значение координаты. Поскольку f' — корень, должна быть еще одна координата с тем же значением, и это может быть только координата из B_j и при этом только изначальная звездочка в A. Таким образом, в B_j есть как минимум две звездочки в строке l. ■

Теперь мы готовы описать множества строк и столбцов, соответствующие требуемой блочно-треугольной форме. Размер этой формы будет равен a. В качестве множества C_{a-i+1} мы берем $B_i \setminus B_{i-1}$ (заметим, что C_{a-i+1} непусты).

Выбор R_i простой: мы берем все строки, которые имеют не меньше двух звездочек в C_i и не имеют звездочек в $C_{i+1}, \ldots, C_k$.

Свойства блочно-треугольной формы следуют из конструкции. Нам только нужно проверить, что каждая строка лежит в каком-то R_i. Рассмотрим произвольную строку l и положим i равным минимальному числу, такому что B_i содержит звездочку в строке l. По доказанному утверждению эта звездочка не уникальна, а в силу выбора B_i в строке l и столбцах из B_{i-1} звездочек нет. Мы полагаем $l \in R_{a-i+1}$.

Также нетрудно видеть, что то же рассуждение работает и для линейных систем с ∞: мы можем игнорировать бесконечные координаты рассматриваемого решения, а бесконечные ячейки матрицы не сказываются на доказательстве. То есть, для решения $x \in \mathbb{Z}_\infty$ мы удаляем из матрицы A_x все столбцы, в которых координата x бесконечна, и обозначаем получившуюся матрицу через $\widetilde{A}_x$. Рассмотрим соответствующую таблицу $\widetilde{A}^*_x$. Нетрудно видеть, что строки, состоящие из бесконечностей, не влияют на максимальный размер блочно-треугольной формы. Заметим, что бесконечности в других строках не могут быть звездочками в $\widetilde{A}^*_x$ в окрестности x, а значит, если мы заменим их на достаточно большие числа, ни локальная размерность, ни блочно-треугольная форма максимального размера не изменятся. ■

Почти без изменений рассуждение работает и для линейных мин-плюс систем уравнений $A \odot x = B \odot x$. Здесь мы рассматриваем совмещенную матрицу $D = \left(\begin{array}{c|c} A & B \end{array} \right)$ и также рассматриваем таблицу D^*. Блочно-треугольной формой размера d здесь мы называем разбиение $R_1, R_2, \ldots, R_d$, где некоторые множества R_i могут быть пусты, и разбиение $C_1, \ldots, C_d$ множества $\{1, \ldots, n\}$, где все C_i непусты. С каждым множеством C_i мы сопоставляем столбцы в A-части матрицы D с соответствующими номерами и столбцы в B-части матрицы D с теми же номерами. Разбиение должно удовлетворять следующим свойствам:

1. для всякого i каждая строка в R_i содержит не менее одной звездочки в столбцах с номерами C_i в A-части матрицы D и не менее одной звездочки в столбцах с номерами C_i в B-части матрицы D;

2. если $1 \leqslant i < j \leqslant d$, то строки R_i не содержат звездочек в столбцах с номерами C_j в обеих частях таблицы D^*.

Аналог теоремы 9.1 доказывается с очевидными изменениями доказательства выше.

9.4 Задача о подсчете размерности множества решений мин-плюс систем NP-полна

В этом разделе мы докажем NP-полноту следующих задач.

Определение 9.4. *В задаче* TropDim *на вход подается матрица* $A \in \mathbb{Z}^{m\times n}$ *(или в* $\mathbb{Q}^{m\times n}$*) и целое число* $k \in \mathbb{N}$*. Требуется определить, верно ли, что размерность множества решений соответствующей мин-плюс системы линейных многочленов не меньше* k*.*

Аналогично определяется задача над $\mathbb{Z}_\infty$ *или* $\mathbb{Q}_\infty$*. Мы обозначаем ее через* TropDim_∞*.*

Прежде чем переходить к результатам о полноте, докажем следующую техническую лемму.

Лемма 9.9. *Пусть дана линейная мин-плюс система многочленов с матрицей* A *с* n *переменными, ячейки матрицы неотрицательны и по абсолютному значению не превышают* M*. Тогда максимальная размерность множества корней системы достигается на точке со всеми конечными координатами, не превышающими* $(M+1)n$*.*

Доказательство. Мы видели в теореме 9.1, что размерность множества решений в данной точке зависит только от таблицы звездочек в этой точке. По данной таблице звездочек рассмотрим граф, вершинами которого являются звездочки в таблице, и две звездочки соединены ребром, если они находятся в одном столбце или в одной строке. Будем называть этот граф *графом звездочек*. Мы говорим, что два столбца связаны, если есть две звездочки в этих столбцах, которые связаны путем в графе звездочек. Заметим, что если есть некоторый путь в графе звездочек между двумя вершинами, то есть и путь длины не больше $2n$ (n шагов по строкам и n шагов по столбцам). Если все столбцы связаны, то для каждой пары координат решения есть путь длины не больше $2n$, соединяющий два соответствующих столбца. Нетрудно видеть, что для каждой пары последовательных координат решения в этом пути разность между этими координатами не больше M (по абсолютному значению).

Если не все столбцы связаны, то есть несколько связных компонент. Рассмотрим одну из них и будем уменьшать значения всех координат в этой компоненте решения на одно и то же число, пока не появится новая звездочка в этом множестве столбцов. Легко видеть, что эта звездочка соединяет две компоненты связности. После этого мы обратно увеличиваем все координаты, которые только что уменьшали на 1. Тогда на месте новой звездочки мы получаем ячейку, которая на 1 больше, чем ячейки, соответствующие звездочкам в этой строке. Вместо звездочки мы помещаем в эту ячейку символ «$\circ$» и с этого момента рассматриваем граф на звездочках и кругах. Уменьшая компоненты одну за другой таким же образом и добавляя новые $\circ$-ячейки, мы получаем связный граф. Применяя рассуждение для связных графов мы получаем требуемую верхнюю оценку $(M+1)n$. ■

Лемма 9.10. TropDim $\in$ NP *и* TropDim$_\infty \in$ NP.

Доказательство. В качестве сертификата неравенства $\dim A \geqslant k$ мы можем взять корень x, в котором локальная размерность не меньше k вместе с блочно-

треугольной формой матрицы $A_x = \{a_{ij} + x_j\}_{i,j}$ размера не меньше $k+1$ (см. теорему 9.1). По лемме 9.9 существует необходимое решение с достаточно маленькими координатами. Нетрудно проверить за полиномиальное время, что данный вектор является решением, и что данное разбиение строк и столбцов действительно задает блочно-треугольную форму нужного размера.

То же самое доказательство работает для $\textsc{TropDim}_\infty$. ■

Чтобы доказать NP-трудность, мы построим полиномиальное сведение задачи VertexCover о вершинном покрытии к нашей задаче.

Определение 9.5. VertexCover*: по данному неориентированному G и натуральному параметру k решить, есть ли в G вершинное покрытие размера не больше k, то есть, есть ли подмножество K множества вершин G размера не больше k, такое что для всякого ребра G хотя бы один его конец лежит в K.*

Пусть n — число вершин в G, а m — число ребер в G. Мы сделаем следующие дополнительные предположения о графе G и k:

1. G связен;
2. $k \leqslant 2n/3$.

С этими дополнительными ограничениями задача о вершинном покрытии остается NP-полной (это следует из стандартного доказательства полноты этой задачи [50]).

Теорема 9.2. *Задача* TropDim *является* NP*-полной.*

Доказательство. Принадлежность классу NP уже доказана, так что остается доказать только NP-трудность.

По данному графу G мы построим матрицу A, задающую линейную минплюс систему многочленов. Матрица A будет иметь $(n+1)$ столбцов, m строк,

и все ее ячейки будут равны 0 или 1, то есть $A \in \{0,1\}^{m\times(n+1)}$. Нулевой вектор будет корнем соответствующей A системы многочленов и глобальный максимум размерности множества решений будет достигаться на этом корне.

Перейдем к построению матрицы A. Первый столбец A состоит из нулей (а значит, первый столбец A^* состоит из звездочек). Всем остальным столбцам сопоставлены вершины G, а строкам — ребра G. Ячейку (e, v) мы полагаем равной 0 тогда и только тогда, когда v является одним из концов e. То есть, строка для ребра $e = \{v, u\}$ будет выглядеть так:

$$
\begin{array}{c}
 \\ e
\end{array}
\begin{array}{c}
\begin{array}{ccccccccccc}
 & & & & v & & & & u & & \\
\end{array} \\
\left(\begin{array}{c|ccc|c|ccc|c|ccc}
0 & & & & & & & & & & \\
0 & & & & & & & & & & \\
\vdots & & & & & & & & & & \\
0 & 1 & \ldots & 1 & 0 & 1 & \ldots & 1 & 0 & 1 & \ldots & 1 \\
\vdots & & & & & & & & & & \\
0 & & & & & & & & & &
\end{array}\right)
\end{array}
$$

В частности, это означает, что каждая строка A содержит ровно 3 нуля и один из них лежит в первом столбце.

Теперь рассмотрим нулевой корень системы с матрицей A. Мы докажем, что локальная размерность множества корней в этой точке не меньше $n - k$ тогда и только тогда, когда для G есть вершинное покрытие размера k. Здесь мы рассматриваем проективную размерность.

Сначала рассмотрим вершинное покрытие $V_1 \subseteq V$ графа G с $|V_1| = k$. Рассмотрим множество столбцов V_1 в A вместе с первым столбцом. Нетрудно видеть, что это множество столбцов содержит не меньше двух нулей в каждой строке: один в первом столбце и второй в V_1, поскольку V_1 является вершинным покрытием. Следовательно, мы можем увеличить координаты решения во всех остальных столбцах, и размерность пространства решений не меньше $n - k$.

Теперь предположим, что размерность множества корней равна $n-d$. Следовательно, есть блочно-треугольная форма A размера $n-d+1$ (по теореме 9.1), рассмотрим такую форму. Рассмотрим множество C_i, содержащее первый столбец A. Мы утверждаем, что для всех $j \neq i$ множества R_j пусты. Действительно, предположим, что R_j непусто для некоторого $j \neq i$. Во-первых, заметим, что $j > i$, иначе у нас будет звездочка над диагональными блоками в блочно-треугольной форме. Рассмотрим максимальное j с непустым R_j. Нетрудно показать, что C_j содержит все столбцы, кроме первого. Действительно, если C_j соответствует собственному подмножеству множества всех вершин графа G, то, в силу связности G, существуют вершины v, u, такие что $v \in C_j$, $u \notin C_j$ и есть ребро $\{v, u\}$ в G. Это ребро очевидно не лежит в R_j, но оно также не может лежать в R_k с $k < j$, иначе вновь мы бы получили звездочку над диагональными блоками в блочно-треугольной форме. Таким образом, C_j содержит все столбцы, кроме первого. Но тогда размер этой блочно-треугольной формы равен 2, при этом мы знаем, что размер блочно-треугольная формы большего размера (напомним, что размер интересующего нас вершинного покрытия в задаче о вершинном покрытии не больше $2n/3$). Таким образом, мы доказали, что для всех $j \neq i$ множества R_j пусты, и таким образом, мы можем считать $i = n - d + 1$.

Итак, мы получили, что блочно-треугольная форма имеет следующую структуру. Множества $R_1, \ldots, R_{n-d}$ пусты, $|C_1| = \ldots = |C_{n-d}| = 1$, $|C_{n-d+1}| = d + 1$ и $R_{n-d+1} = \{1, \ldots, m\}$. Также мы знаем, что первый столбец лежит в C_{n-d+1}. Легко видеть, что множество всех остальных столбцов в C_{n-d+1} образует вершинное покрытие, а значит $k \leqslant d$.

Остается лишь доказать, что максимальная размерность в множестве корней достигается в нулевом корне системы A. Рассмотрим произвольное решение x системы с матрицей A. Поскольку мы работаем в проективном пространстве,

мы можем предполагать, что $x_1 = 0$. Это означает, что первый столбец матрицы

$$B = \{a_{ij} + x_j\}_{i,j} \tag{9.8}$$

такой же, как в A.

Утверждение. *Для всех $j = 1, \ldots, n$ мы можем предполагать, что $x_j \geqslant 0$.*

Доказательство утверждения. Предположим от противного, что $\alpha = \min_j x_j < 0$. Положим $C_1 = \{j \mid x_j = \alpha\}$. Множество столбцов C_1 соответствует некоторому множеству $V_1 \subseteq V$ вершин графа G (заметим, что $1 \notin C_1$). Рассмотрим два случая.

Случай 1. $V_1 \neq V$. Поскольку G связен, существует ребро e с одним концом в V_1 и другим концом в $V \setminus V_1$. Рассмотрим строку матрицы (9.8), соответствующую e. Нетрудно видеть, что в одной ячейке этой строки у нас значение α, а во всех остальных — значения больше α. Таким образом, эта строка в таблице B^* содержит одну звездочку, и мы получаем противоречие.

Случай 2. $V_1 = V$. Тогда мы можем получить B, уменьшив все столбцы A (кроме первого) на одно и то же число. Тогда у нас ровно две звездочки в каждой строке B^*. А поскольку граф связен, максимальная блочно-треугольная форма в этом случае будет иметь размер 2: первый столбец с пустым множеством строк и все остальные столбцы с множеством всех строк. Таком образом, размерность множества решений в этой точке равна лишь 1, что меньше, чем для нулевого решения. ■

Теперь рассмотрим столбец j, такой что $x_j > 0$. Легко видеть, что все ячейки матрицы B в этом столбце больше нуля. Поскольку первый столбец состоит из нулей, мы получаем, что в столбце j в B^* нет звездочек. Таким образом, несложно описать, чем таблица B^* отличается от A^*: мы просто удаляем все звездочки в A^* из столбцов j, таких что $x_j > 0$. Остается только показать,

что максимальный размер блочно-треугольной формы для A не меньше максимального размера блочно-треугольной формы для B. Для этого рассмотрим блочно-треугольную форму для B максимального размера. Заметим, что каждый столбец j, такой что $x_j > 0$, должен составлять отдельное множество C_i с пустым множеством R_i, и заметим, что мы можем предполагать, что все эти множества находятся в начале списка всех C_i. Рассмотрим ту же систему множеств C_i и R_i для матрицы A. Легко видеть, что эта система является блочно-треугольной формой и для этой матрицы. Таким образом, максимальный размер блочно-треугольной формы для A может быть только больше, чем для B, а значит, размерность множества корней достигает максимума на нулевом корне. ■

Как следствие мы получаем следующий результат.

Следствие 9.11. *Задача* TropDim$_\infty$ *является* NP*-полной.*

Доказательство. Принадлежность NP была доказана в лемме 9.10.

Для доказательства полноты достаточно доказать сведение TropDim $\leqslant_p$ TropDim$_\infty$.

Пусть нам дана мин-плюс линейная система над полукольцом без бесконечности, например, $\mathbb{Q}$. Рассмотрим ту же систему, как систему над полукольцом с бесконечностью $\mathbb{Q}_\infty$. Если у системы есть корень над $\mathbb{Q}$, он же является корнем и над $\mathbb{Q}_\infty$, и размерность множества корней в этой точке над $\mathbb{Q}_\infty$ будет такая же. В обратную сторону, если есть корень над $\mathbb{Q}_\infty$, то есть возможно содержащий бесконечные координаты, то мы можем заменить эти координаты на достаточно большие конечные числа. Мы получим корень над $\mathbb{Q}$ с той же локальной размерностью множества корней. ■

Результаты этого раздела могут быть легко распространены на случай линейных мин-плюс систем уравнений.

Теорема 9.3. *Задача проверки по данной линейной мин-плюс системе уравнений и данному натуральному k, имеет ли множество корней размерность не меньше k, является* NP*-полной.*

Доказательство. Действительно, аналоги лемм 9.9 и 9.10 можно доказать таким же образом. Для полноты заметим, что лемма 9.3 дает полиномиальное сведение из TropDim и TropDim_∞. ■

9.5 Линейная двойственность в мин-плюс алгебре

9.5.1 Формулировки результатов

Результаты этого раздела верны для всех рассматриваемых нами полуколец, мы приведем формулировки для $\mathbb{R}$ и $\mathbb{R}_\infty$.

Мы докажем следующие результаты о линейной двойственность для линейных систем мин-плюс неравенств.

Лемма 9.12. *Пусть $A, B \in \mathbb{R}_\infty^{m\times n}$ — две матрицы.*

(i) Для любого множества $S \subseteq \{1, \ldots, n\}$ верно ровно одно из следующих двух утверждений.

1. *Существует решение системы $A \odot \vec{x} \leqslant B \odot \vec{x}$ с конечными координатами x_i для $i \in S$.*
2. *Существует решение транспонированной системы $B^T \odot \vec{y} < A^T \odot \vec{y}$, такое что для некоторого $i \in S$ i-я координата вектора $B^T \odot \vec{y}$ конечна.*

(ii) Для любого множества $S \subseteq \{1, \ldots, n\}$ верно ровно одно из следующих двух утверждений.

1. *Существует решение системы* $A \odot \vec{x} \leqslant B \odot \vec{x}$, *такое что для некоторого* $i \in S$ *координата* x_i *конечна.*

2. *Существует решение системы* $B^T \odot \vec{y} < A^T \odot \vec{y}$, *такое что* i*-я координата вектора* $B^T \odot \vec{y}$ *конечна для всех* $i \in S$.

Напомним, что мы здесь допускаем, что обе части строго неравенства могут равняться бесконечности.

Доказательство этой леммы будет дано в разделе 9.5.2. Оно основано на связи мин-плюс линейных систем неравенств с циклическими играми, установленной в [4].

Как несложное следствие этой леммы мы получаем следующую простую формулировку линейной двойственности для линейных мин-плюс систем неравенств.

Следствие 9.13. *(i) Для двух матриц* $A, B \in \mathbb{R}^{m\times n}$ *верно ровно одно из двух следующих утверждений.*

1. *Существует решение системы* $A \odot \vec{x} \leqslant B \odot \vec{x}$ *над* $\mathbb{R}$.

2. *Существует решение системы* $B^T \odot \vec{y} < A^T \odot \vec{y}$ *над* $\mathbb{R}$.

(ii) Для двух матриц $A, B \in \mathbb{R}_\infty^{m\times n}$ *верно ровно одно из двух следующих утверждений.*

1. *Существует решение* $\vec{x} \neq (\infty, \ldots, \infty)$ *системы* $A \odot \vec{x} \leqslant B \odot \vec{x}$.

2. *Существует конечное решение системы* $B^T \odot \vec{y} < A^T \odot \vec{y}$.

(iii) Для двух матриц $A, B \in \mathbb{R}_\infty^{m\times n}$ *верно ровно одно из двух следующих утверждений.*

1. *Существует конечное решение системы* $A \odot \vec{x} \leqslant B \odot \vec{x}$.

2. *Существует решение* $\vec{y} \neq (\infty, \ldots, \infty)$ *системы* $B^T \odot \vec{y} < A^T \odot \vec{y}$.

Поскольку это следствие вытекает из леммы 9.12 почти мгновенно, мы приводим доказательство сразу.

Доказательство. Для матриц $A, B \in \mathbb{R}^{m\times n}$ с конечными ячейками мы можем использовать лемму 9.12(i) с $S = \{1, \ldots, n\}$. Тогда первое утверждение леммы 9.12(i) совпадает с первым утверждением следствия 9.13(i). Второе утверждение леммы 9.12(i) эквивалентно второму утверждению следствия 9.13(i). Действительно, если есть конечное решение системы $B^T \odot \vec{y} < A^T \odot \vec{y}$, то ясно, что для этого $\vec{y}$ все координаты вектора $B^T \odot \vec{y}$ конечны. В другую сторону, если есть решение $\vec{y}$, такое что $B^T \odot \vec{y}$ имеет конечную координату, то вектор $\vec{y}$ сам должен иметь конечную координату. Поскольку все ячейки A и B конечны, то все координаты $A^T \odot \vec{y}$ и $B^T \odot \vec{y}$ конечны. Если в векторе $\vec{y}$ есть бесконечные координаты, мы можем заменить их на достаточно большие конечные числа так, чтобы векторы $A^T \odot \vec{y}$ и $B^T \odot \vec{y}$ не изменились. Получившийся вектор является конечным решением системы $B^T \odot \vec{y} < A^T \odot \vec{y}$.

Для доказательства следствия 9.13(ii) положим $S = \{1, \ldots, n\}$ и применим лемму 9.12(ii). Первое утверждение леммы 9.12(ii) эквивалентно первому утверждению следствия 9.13(ii). Чтобы увидеть, что эквивалентны также вторые утверждения в лемме 9.12(ii) и в следствии 9.13(ii), заметим, что если для некоторого $\vec{y}$ все координаты $B^T \odot \vec{y}$ конечны, то мы можем считать, что все координаты $\vec{y}$ также конечны. Действительно, если в $\vec{y}$ есть бесконечные координаты, мы можем просто заменить их на достаточно большие числа без изменения значения вектора $B^T \odot \vec{y}$.

Последняя часть следствия доказывается аналогично, полагая $S = \{1, \ldots, n\}$ и применяя лемму 9.12(i). ■

Мы докажем близкий результат о двойственности линейных систем многочленов.

Лемма 9.14. *Пусть $A \in \mathbb{R}_\infty^{m\times n}$ — матрица.*

(i) Для любого множества $S \subseteq \{1, \ldots, n\}$ верно ровно одно из следующих двух утверждений.

1. *Существует корень системы $A \odot \vec{x}$ с конечными координатами x_i для $i \in S$.*
2. *Существует $\vec{z}$, такое что в каждой строке $A^T \odot \vec{z}$ минимум достигается один раз или равен ∞, для любых двух строк с конечным минимумами (единственные) минимумы достигаются в разных столбцах, и для некоторого $i \in S$ i-я координата $A^T \odot \vec{z}$ конечна.*

(ii) Для любого множества $S \subseteq \{1, \ldots, n\}$ верно ровно одно из следующих двух утверждений.

1. *Существует корень $A \odot \vec{x}$, такой что для некоторого $i \in S$ координата x_i конечна.*
2. *Существует $\vec{z}$, такое что в каждой строке $A^T \odot \vec{z}$ минимум достигается один раз или равен ∞, для любых двух строк с конечным минимумами (единственные) минимумы достигаются в разных столбцах, и i-е координаты $A^T \odot \vec{z}$ конечны для всех $i \in S$.*

Этот результат можно доказать или сведением из результата для линейных мин-плюс систем неравенств, или через анализ в духе [60]. Мы приводим доказательство через сведение от линейных мин-плюс систем неравенств в разделе 9.5.3.

Как и в случае систем неравенств, здесь мы можем получить следующее следствие.

Следствие 9.15. *(i) Для матрицы $A \in \mathbb{R}^{m \times n}$ верно ровно одно из двух следующих утверждений.*

1. *Существует решение системы $A \odot \vec{x}$ над $\mathbb{R}$.*

2. *Существует $\vec{z} \in \mathbb{R}^m$, такой что в каждой строке $A^T \odot \vec{z}$ минимум достигается только один раз, и в любых двух строках минимумы достигаются в разных столбцах.*

(ii) Для матрицы $A \in \mathbb{R}_\infty^{m \times n}$ верно ровно одно из двух следующих утверждений.

1. *Существует решение $\vec{x} \neq (\infty, \ldots, \infty)$ системы $A \odot \vec{x}$.*
2. *Существует конечное $\vec{z}$, такое что в каждой строке $A^T \odot \vec{z}$ минимум достигается только один раз, и в любых двух строках минимумы достигаются в разных столбцах.*

(iii) Для матрицы $A \in \mathbb{R}_\infty^{m \times n}$ верно ровно одно из двух следующих утверждений.

1. *Существует конечное решение $A \odot \vec{x}$.*
2. *Существует $\vec{z} \neq (\infty, \ldots, \infty)$, такое что в каждой строке $A^T \odot \vec{z}$ минимум достигается только один раз или равен ∞, и для любых двух строк с конечным минимум их минимумы достигаются в разных столбцах.*

Доказательство этого следствия полностью аналогично доказательству следствия 9.13.

9.5.2 Линейная двойственность для систем неравенств

В этом разделе мы доказываем лемму 9.12 о двойственности для линейных мин-плюс систем неравенств.

Доказательство леммы основано на интерпретации мин-плюс систем линейных неравенств в терминах циклических игр. Более точно, по данной системе можно построить циклическую игру G, такую что разрешимость системы соответствует наличию выигрышной стратегии для одного из игроков. Эта связь

между мин-плюс системами линейных неравенств и циклическими играми была установлена в [4]. Опишем эту взаимосвязь, а затем на ее основе докажем лемму 9.12.

По данным матрицам $A, B \in \mathbb{R}_\infty^{m\times n}$ мы можем построить следующую циклическую игру G. Рассмотрим ориентированный двудольный граф с вершинами $r_1, \ldots, r_m$ в левой доле и вершинами $c_1, \ldots, c_n$ в правой доле. Вершины левой доли соответствуют строкам матриц A и B, а вершины в правой доле — столбцам матриц. Из каждой вершины r_i мы проводим ребро в вершину c_j, помеченное $-a_{ij}$. Из каждой вершины c_j мы проводим ребро в вершину r_i, помеченное b_{ij}. Мы будем обозначать метку ребра (v, u) через $w(v, u)$. То есть, $w(r_i, c_j) = -a_{ij}$ и $w(c_j, r_i) = b_{ij}$. Игроков в этой игре мы называем игроком-строкой и игроком-столбцом. Если фишка находится в какой-то вершине r_i, то игрок-столбец передвигает ее в любую из вершин c_j (игрок-столбец выбирает столбец). Если, наоборот, фишка расположена в какой-то вершине c_j, то игрок-строка передвигает ее в любую из вершин r_i (игрок-строка выбирает строку). Игрок-столбец стремиться максимизировать сумму в (9.1), то есть выигрывает, если предел положителен. Если некоторые ячейки матриц A, B бесконечны, мы предполагаем, что этих ребер в графе просто нет, и соответственно, игроки не могут передвигать фишку вдоль них. Эквивалентно, можно считать, что у нас есть ребра, помеченные бесконечностью, и игрок, который по ним переходит, немедленно проигрывает.

Заметим, что если все ячейки матриц конечны, то игра проходит на полном двудольном ориентированном графе, и легко видеть, что победитель в игре не зависит от стартовой позиции.

В случае матриц с ячейками из $\mathbb{R}_\infty$ ситуация иная. Для построенной игры G верны следующие свойства, по существу доказанные в [4] (см. также изложение в [63]).

Лемма 9.16. *Существует конечное решение системы $A \odot \vec{x} \leqslant B \odot \vec{x}$ тогда и только тогда, когда игрок-столбец имеет непроигрышную стратегию, начиная из любой начальной позиции.*

Существует решение $\vec{x} \neq (\infty, \ldots, \infty)$ системы $A \odot \vec{x} \leqslant B \odot \vec{x}$ тогда и только тогда, когда игрок-столбец имеет непроигрышную стратегию, начиная из какой-то начальной позиции.

Существует решение системы $A \odot \vec{x} \leqslant B \odot \vec{x}$ с конечной координатой x_i тогда и только тогда, когда игрок столбец имеет непроигрышную стратегию, начиная из позиции c_i.

Существует решение системы $A \odot \vec{x} \leqslant B \odot \vec{x}$, такое что j-я координата $A \odot \vec{x}$ конечна тогда и только тогда, когда игрок столбец имеет непроигрышную стратегию, начиная из позиции r_j.

Следующее наблюдение является основным шагом к доказательству линейной двойственности для мин-плюс систем.

Лемма 9.17. *Существует конечное решение системы $A \odot \vec{x} < B \odot \vec{x}$ тогда и только тогда, когда игрок-столбец имеет выигрышную стратегию, начиная из какой-то начальной позиции.*

Существует решение $\vec{x} \neq (\infty, \ldots, \infty)$ системы $A \odot \vec{x} < B \odot \vec{x}$ тогда и только тогда, когда игрок-столбец имеет выигрышную стратегию, начиная из какой-то начальной позиции.

Существует решение системы $A \odot \vec{x} < B \odot \vec{x}$ с конечной координатой x_i тогда и только тогда, когда игрок столбец имеет выигрышную стратегию, начиная из позиции c_i.

Существует решение системы $A \odot \vec{x} < B \odot \vec{x}$, такое что j-я координата $A \odot \vec{x}$ конечна тогда и только тогда, когда игрок столбец имеет выигрышную стратегию, начиная из позиции r_j.

Доказательство. Пусть есть решение $\vec{x}$ системы $A \odot \vec{x} < B \odot \vec{x}$. Тогда для достаточно маленького положительного ϵ существует решение системы $A \odot \vec{x} \leqslant$

$(B-\epsilon)\odot\vec{x}$, в которой мы вычитаем ϵ из каждой ячейки B. Тогда по лемме 9.16 существует непроигрышная стратегия для игрока-столбца в циклической игре G', соответствующей системе $A\odot\vec{x}\leqslant(B-\epsilon)\odot\vec{x}$. Пусть игрок-столбец применяет ту же стратегию в игре G, соответствующей системе $A\odot\vec{x}<B\odot\vec{x}$. Тогда в любой партии после k ходов сумма в (9.1) будет на $k\epsilon$ больше суммы для аналогичной партии в игре G'. Если в игре G' для некоторой партии предел был неотрицателен, то в G он будет положителен. Следовательно, в игре G игрок-столбец имеет выигрышную стратегию.

В другую сторону, предположим, что игрок столбец имеет выигрышную стратегию. Тогда, если мы для небольшого ϵ заменим в графе все метки b_{ij} на $b_{ij}-\epsilon$, то игрок-столбец все еще будет иметь выигрышную стратегию, которая в частности будет непроигрышной. Следовательно, по лемме 9.16 мы получаем, что есть решение $\vec{x}$ системы $A\odot\vec{x}\leqslant(B-\epsilon)\odot\vec{x}$, в которой мы вычитаем ϵ из каждой ячейки B. Ясно, что этот же $\vec{x}$ является решением и $A\odot\vec{x}<B\odot\vec{x}$.

Эти соответствия доказывают все четыре утверждения леммы. ■

Теперь для завершения доказательства леммы 9.12 остается лишь воспользоваться двойственностью для циклических игр. Для этого заметим, что в игре G либо игрок-столбец имеет выигрышную стратегию при начале игры из некоторой позиции, либо игрок-строка имеет непроигрышную стратегию при начале игры из той же позиции. Также заметим, что если вместе с игрой G, соответствующей мин-плюс линейной системе неравенств $A\odot\vec{x}\leqslant B\odot\vec{x}$, мы рассмотрим игру G', соответствующую мин-плюс линейной системе неравенств $B^T\odot\vec{y}\leqslant A^T\odot\vec{y}$, то игры G и G' отличаются лишь сменой ролей игроков.

9.5.3 Линейная двойственность для систем многочленов

Пусть нам дана система мин-плюс линейных многочленов $A\odot\vec{x}$ для $A\in\mathbb{R}^{m\times n}$, и нас интересует, есть ли у нее корень. Во-первых, известно, что если число переменных больше числа многочленов, то корень всегда есть [41]. Так

что мы можем предполагать, что $m \geqslant n$. Далее, заметим, что если мы прибавим одно и то же число ко всем ячейкам в каком-то столбце A, то свойство разрешимости не изменится. Одно простое препятствие к тому, чтобы система $A \odot \vec{x}$ не имела корней, состоит в том, что мы можем прибавить некоторые числа ко всем столбцам A и, возможно, переставить строки и столбцы так, чтобы минимумы в первых n строках получившейся матрицы были уникальны в каждой из строк и достигались в ячейках $(1,1),(2,2),\ldots,(n,n)$. Нетрудно видеть, что если это возможно, то система $A \odot \vec{x}$ не имеет корней [41]. Оказывается, что это единственное препятствие. Мы приводим доказательсто ниже. Отметим, что доказательство также можно извлечь из анализа [60, 79].

Доказательство леммы 9.14. Для данного произведения матрицы на вектор $A \odot \vec{a}$, где $A \in \mathbb{R}_{\infty}^{m \times n}$, удобно определить значение $n_i(A \odot \vec{a})$ для всех $i = 1, \ldots, m$, которое равно номеру столбца, где расположен конечный минимум в строке i (если он вообще конечен). Если минимумов в строке несколько, $n_i(A \odot \vec{a})$ соответствует первому из них. Когда из контекста ясно, о каких матрице и векторе идет речь, мы будем сокращать обозначение до n_i.

Обозначим через C_i для $i = 1, \ldots, n$ матрицу из $\mathbb{R}^{m \times n}$ с ячейками 1 в столбце i и с ячейками 0 в остальных столбцах. Обозначим через R_i для $i = 1, \ldots, n$ матрицу из $\mathbb{R}^{n \times m}$ с ячейками 1 в строке i и с ячейками 0 в остальных строках. Заметим, что $R_i = C_i^T$.

Мы докажем первое утверждение леммы. Второе утверждение доказывается полностью аналогично.

Пусть дана матрица $A \in \mathbb{R}_{\infty}^{m \times n}$, рассмотрим мин-плюс систему линейных многочленов $A \odot \vec{x}$. Как мы видели в доказательстве леммы 9.3, $\vec{x}$ является корнем этой системы тогда и только тогда, когда для для произвольного $\epsilon > 0$

вектор $\vec{x}$ является решением следующей системы неравенств:

$$\begin{pmatrix} A+\epsilon C_1 \\ A+\epsilon C_2 \\ \vdots \\ A+\epsilon C_n \end{pmatrix} \odot \vec{x} \leqslant \begin{pmatrix} A \\ A \\ \vdots \\ A \end{pmatrix} \odot \vec{x}.$$

По лемме 9.12 эта система имеет решение $\vec{x}$ с конечными координатами x_i для $i \in S$ тогда и только тогда, когда система

$$\begin{pmatrix} A^T & A^T & \cdots & A^T \end{pmatrix} \odot \vec{y} < \begin{pmatrix} A^T+\epsilon R_1 & A^T+\epsilon R_2 & \cdots & A^T+\epsilon R_n \end{pmatrix} \odot \vec{y} \tag{9.9}$$

не имеет решения $\vec{y}$, такого что для некоторого $i \in S$ i-я координата

$$\begin{pmatrix} A^T & A^T & \cdots & A^T \end{pmatrix} \odot \vec{y}$$

конечна.

В правой части (9.9) мы получили блочную матрицу с блоками $A^T + \epsilon R_i$.

Остается показать, что система (9.9) имеет решение с указанными свойствами тогда и только тогда, когда существует $\vec{z}$, такой что в каждой строке $A^T \odot \vec{z}$ минимум достигается один раз или равен ∞, для любых двух строк с конечными минимумами эти минимумы достигаются в разных столбцах, и для некоторого $i \in S$ i-я координата $A^T \odot \vec{z}$ конечна. Заметим, что если $\vec{y}$ является решением (9.9), то в каждой строке i, в которой минимум левой части неравенства конечен, верно, что $m(i-1) < n_i \leqslant mi$, то есть n_i лежит в i-м блоке. Действительно, иначе минимум в этой строке в левой части больше либо равен минимума в правой части, поскольку i-е строки левой и правой части отличаются только в i-м блоке. Таким образом, если $\vec{y}$ является решением, то для каждой строки i с конечным минимумом существует столбец $j_i = n_i \pmod m$ в i-м блоке, такой что минимум достигается в этом столбце. Заметим, что для $i_1 \neq i_2$ с конечными минимумами в строках системы верно, что $j_{i_1} \neq j_{i_2}$. Действительно, иначе строки i_1, i_2 и столбцы $n_{i_1} = mi_1 + j_{i_1}, n_{i_2} = mi_2 + j_{i_1}$ составили

бы подсистему

$$\begin{pmatrix} a_{i_1,j_{i_1}} & a_{i_1,j_{i_1}} \\ a_{i_2,j_{i_1}} & a_{i_2,j_{i_1}} \end{pmatrix} \odot \begin{pmatrix} y_{mi_1+j_{i_1}} \\ y_{mi_2+j_{i_1}} \end{pmatrix} < \begin{pmatrix} a_{i_1,j_{i_1}} + \epsilon & a_{i_1,j_{i_1}} \\ a_{i_2,j_{i_1}} & a_{i_2,j_{i_1}} + \epsilon \end{pmatrix} \odot \begin{pmatrix} y_{mi_1+j_{i_1}} \\ y_{mi_2+j_{i_1}} \end{pmatrix}$$

размера 2×2 с конечными $y_{mi_1+j_{i_1}}, y_{mi_2+j_{i_1}}$, что невозможно. Таким образом, столбцы j_i соответствуют различным столбцам матрицы A^T. Рассмотрим систему многочленов

$$A^T \odot \vec{z}$$

и рассмотрим следующий вектор $\vec{z}$. Для всех i с конечным минимумом в строке i положим $z_{j_i} = y_{mi+j_i}$. Положим все остальные координаты $\vec{z}$ равными ∞. Для этого $\vec{z}$ минимум в каждой строке либо бесконечен, либо достигается только один раз, и никакие два минимума в разных строках не лежат в одном столбце. Действительно, если конечный минимум достигается дважды в некоторой строке, то для той же строки (9.9) у нас было бы равенство. Заметим также, что i-я координата вектора

$$\begin{pmatrix} A^T & A^T & \cdots & A^T \end{pmatrix} \odot \vec{y}$$

конечна тогда и только тогда, когда i-я координата вектора $A^T \odot \vec{z}$ конечна.

В другую сторону, пусть у нас есть вектор $\vec{z}$, такой что в каждой строке $A^T \odot \vec{z}$ минимум либо бесконечен, либо достигается один раз, и никакие два минимума в разных строках не лежат в одном столбце. Тогда для каждой строки i с конечным минимумом рассмотрим столбец j_i , в котором этот минимум достигается, и положим $y_{im+j_i} = z_j$. Положим все остальные координаты $\vec{y}$ равными ∞. Тогда для достаточно маленького ϵ мы получим решение (9.9), и i-я координата $A^T \odot \vec{z}$ конечна тогда и только тогда, когда i-я координата

$$\begin{pmatrix} A^T & A^T & \cdots & A^T \end{pmatrix} \odot \vec{y}$$

конечна. ■

Глава 10

Мин-плюс аналоги теоремы Гильберта о нулях

Результаты этой секции выполняются для полуколец $\mathbb{R}$ и $\mathbb{Q}$, а также их вариантов с добавлением бесконечности. Результаты не переносятся на полукольцо $\mathbb{Z}$: в нем не выполняется мин-плюс аналог алгебраической замкнутости.

Приведем формулировку классической теоремы о нулях.

Теорема 10.1 (Эффективная теорема Гильберта о нулях [90]). *Система многочленов $F = \{f_1, \ldots, f_k\}$ от n переменных степени не больше d над $\mathbb{C}$ не имеет общего корня тогда и только тогда, когда существуют многочлены $g_1, \ldots, g_k$, такие что*

$$\sum_i f_i g_i \equiv 1$$

и

$$\max_i deg(f_i g_i) \leqslant 2d^{\min(n,k)}.$$

Отметим, что наивный мин-плюс аналог теоремы о нулях оказывается не верен: пара многочленов $f_1 = 0 \odot x \oplus 0$ и $f_2 = 0 \odot x \oplus 1$ не имеет корня, но любая их мин-плюс алгебраическая комбинация будет содержать непостоянные мономы и будет иметь корень.

В этой главе мы сформулируем и докажем корректный мин-плюс аналог теоремы о нулях.

10.1 Формулировки результатов

Определение 10.1. *Для данной системы мин-плюс многочленов* $F = \{f_1, \ldots, f_k\}$ *от* n *переменных мы определяем ее бесконечную матрицу Макколея* M*. Столбцы* M *соответствуют неотрицательным целочисленным векторам* $I \in \mathbb{Z}_+^n$*, а строки* M *соответствуют парам* (j, J)*, где* $1 \leqslant j \leqslant k$ *и* $J \in \mathbb{Z}_+^n$*. Для данных* I *и* (j, J) *мы полагаем ячейку* $m_{(j,J),I}$ *равной коэффициенту монома* $\vec{x}^I$ *в многочлене* $\vec{x}^J \odot f_j$ *(если такого монома в многочлене нет, мы считаем эту ячейку равной* ∞*). Через* M_N *мы обозначаем конечную подматрицу матрицы* M*, состоящую из всех столбцов* I*, для которых* $|I| = i_1 + \ldots + i_n \leqslant N$*, и из всех строк, все конечные ячейки которых лежат в этих столбцах. Нас будет интересовать мин-плюс линейная система* $M_N \odot \vec{y}$*. Над* $\mathbb{R}_\infty$ *мы рассматриваем неоднородную систему линейных многочленов* $M_N \odot (0, \vec{y})$*. Столбец, соответствующий, постоянному моному, является неоднородным столбцом.*

Для системы мин-плюс уравнений $F = \{(f_1, g_1), \ldots, (f_k, g_k)\}$ *мы аналогично вводим пару матриц* Ml *и* Mr*, соответствующих левым и правым частям уравнений соответственно. Аналогично мы определяем матрицы* Ml_N*,* Mr_N *и соответствующие мин-плюс линейные системы* $Ml_N \odot \vec{y} = Mr_N \odot \vec{y}$*. Аналогично, для случая* $\mathbb{R}_\infty$ *мы рассматриваем неоднородные системы* $Ml_N \odot (0, \vec{y}) = Mr_N \odot (0, \vec{y})$*.*

В [59] были выдвинуты три гипотезы о теореме о нулях для мин-плюс многочленов. Мы формулируем самую сильную из этих гипотез, а именно, гипотезу о сильной теореме о нулях.

Гипотеза ([59]). *Существует функция* N *от* n *и* $\deg(f_i)$ *для* $1 \leqslant i \leqslant k$*, такая что система мин-плюс многочленов* $F = \{f_1, \ldots, f_k\}$ *от* n *переменных имеет общий корень тогда и только тогда, когда соответствующая мин-плюс линейная система с матрицей* M_N *имеет решение.*

Заметим, что классический аналог этого утверждения — это в точности эффективная версия теоремы Гильберта о нулях в двойственной форме (см. подробности в [59]).

В [59] гипотеза была доказана для случая $n = 1$. В этом разделе мы докажем общий случай этой гипотезы.

Теорема 10.2 (Двойственная теорема о нулях для мин-плюс многочленов). *Рассмотрим систему мин-плюс многочленов $F = \{f_1, \ldots, f_k\}$ от n переменных. Обозначим через d_i степень многочлена f_i и положим $d = \max_i d_i$.*

(i) Над полукольцом $\mathbb{R}$ система F имеет корень тогда и только тогда, когда линейная система с матрицей Маколея $M_N \odot \vec{y}$ для

$$N = (n+2)\,(d_1 + \ldots + d_k)$$

имеет корень.

(ii) Над полукольцом $\mathbb{R}_\infty$ система F имеет корень тогда и только тогда, когда неоднородная линейная система с матрицей Маколея $M_N \odot (0, \vec{y})$ для

$$N = poly(n, k, d)\,(4d)^{\min(n,k)}$$

имеет корень.

Заметим, что в одну сторону доказательство теоремы не сложно. Действительно, если система многочленов имеет корень $\vec{a} \in \mathbb{R}^n$, то нетрудно видеть, что есть решение и у $M_N \odot \vec{y}$. Для этого заметим, что координаты y_I вектора $\vec{y}$ соответствуют мономам $\vec{x}^I$, так что можно положить $y_I = \vec{a}^I$. Поскольку каждая строка M_N соответствует многочлену вида $\vec{x}^J \odot f_j(\vec{x})$, и $\vec{a}$ является корнем всякого такого многочлена, мы получаем, что $\vec{y}$ является корнем всех строк M_N. Это же рассуждение проходит и для $\mathbb{R}_\infty$. Таким образом, основной сложностью является доказательство теоремы в другую сторону.

Отметим, что мы также можем рассматривать линейную систему с бесконечной матрицей Маколея $M \odot \vec{y}$. Это корректно, поскольку каждая строка M содержит лишь конечное число конечных ячеек. Как следствие предыдущей теоремы мы выводим бесконечную версию двойственной теоремы о нулях для мин-плюс многочленов.

Следствие 10.1. *Система мин-плюс многочленов $F = \{f_1, \ldots, f_k\}$ от n переменных имеет корень тогда и только тогда, когда линейная система с бесконечной матрицей Маколея M имеет корень. Это утверждение верно для обоих полуколец $\mathbb{R}$ и $\mathbb{R}_\infty$.*

Доказательство в простую сторону полностью аналогично теореме 10.2, а доказательство в сложную сторону легко следует из теоремы 10.2.

Также мы доказываем двойственную теорему о нулях для мин-плюс уравнений.

Теорема 10.3 (Двойственная теорема о нулях для мин-плюс уравнений). *Рассмотрим систему мин-плюс уравнений $F = \{(f_1, g_1), \ldots, (f_k, g_k)\}$ от n переменных. Обозначим через d_i максимальную степень многочленов в уравнении (f_i, g_i) и положим $d = \max_i d_i$.*

(i) Над полукольцом $\mathbb{R}$ система F имеет решение тогда и только тогда, когда линейная система уравнений с матрицами Маколея $Ml_N \odot \vec{y} = Mr_N \odot \vec{y}$ для

$$N = (n+2)\,(d_1 + \ldots + d_k)$$

имеет решение.

(ii) Над полукольцом $\mathbb{R}_\infty$ система F имеет решение тогда и только тогда, когда неоднородная линейная система уравнений с матрицами Маколея $Ml_N \odot (0, \vec{y}) = Mr_N \odot (0, \vec{y})$ для

$$N = poly(n, k, d)\,(4d)^{\min(n,k)}$$

имеет решение.

Как и в случае мин-плюс многочленов, простым следствием является бесконечная версия двойственной теоремы о нулях для мин-плюс уравнений.

Следствие 10.2. *Система мин-плюс уравнений* $F = \{f_1{=}g_1, \ldots, f_k{=}g_k\}$ *от* n *переменных имеет решение тогда и только тогда, когда линейная система уравнений с бесконечными матрицами Маколея* (Ml, Mr) *имеет решение. Это утверждение верно для обоих полуколец* $\mathbb{R}$ *и* $\mathbb{R}_\infty$.

Мы приводим примеры, показывающие, что наши оценки на N в этих теоремах близки к точным. А именно, для полукольца $\mathbb{R}$ для всякого $d > 1$ и всякого n мы строим семейство F из $(n+1)$ мин-плюс многочлена (мин-плюс уравнения) от n переменных и степени d, такое что F не имеет корней, но линейная система многочленов (уравнений) с матрицей Маколея для $N = (d-1)(n-1)$ имеет корень. Для полукольца $\mathbb{R}_\infty$ для всякого $d > 1$ и всякого n мы строим семейство F из $(n+1)$ мин-плюс многочлена (мин-плюс уравнения) от $(n+1)$ переменной и степени d, такое что F не имеет корней, но линейная система многочленов (уравнений) с матрицей Маколея для $N = d^{n-1} - 1$ имеет корень.

Отметим, что эти оценки все же не точны. Разрыв лучше всего виден в случае полукольца $\mathbb{R}$. Предположим для простоты, что $n \approx k$. Тогда наша верхняя оценка дает $N \sim dn^2$, а нижняя оценка дает $N \sim dn$.

Далее мы доказываем теоремы о нулях в более стандартных, прямых (а не двойственных) формах.

Мы начнем с более интуитивно понятной теоремы о нулях для мин-плюс уравнений. Для этого мы введем понятие алгебраической комбинации для мин-плюс уравнений.

Определение 10.2. Алгебраической комбинацией *системы мин-плюс уравнений* $F = \{(f_1, g_1), \ldots, (f_k, g_k)\}$ *называется уравнение* (f, g) *представимое в*

форме

$$(f, g) = \left(\bigoplus_{j=1}^{K} h_j^{(l)}, \bigoplus_{j=1}^{K} h_j^{(r)} \right)$$

для некоторого K*, где для всякого* $1 \leqslant j \leqslant K$ *верно либо* $(h_j^{(l)}, h_j^{(r)}) = (m_j \odot f_{i_j}, m_j \odot g_{i_j})$*, либо* $(h_j^{(l)}, h_j^{(r)}) = (m_j \odot g_{i_j}, m_j \odot f_{i_j})$ *для некоторого монома* m_j *и некоторого* $1 \leqslant i_j \leqslant k$*.*

Теорема 10.4 (Прямая теорема о нулях для мин-плюс уравнений). *Рассмотрим систему мин-плюс уравнений* $F = \{(f_1, g_1), \ldots, (f_k, g_k)\}$ *от* n *переменных. Обозначим через* d_i *максимальную степень многочленов в уравнении* (f_i, g_i) *и положим* $d = \max_i d_i$*.*

(i) Над полукольцом $\mathbb{R}$ *система* F *не имеет решений тогда и только тогда, когда существует алгебраическая комбинация* (f, g) *системы* F *со степенью не больше*

$$N = (n + 2)(d_1 + \ldots + d_k),$$

такая что для каждого монома $m = x_1^{\odot j_1} \odot \ldots \odot x_n^{\odot j_n}$ *его коэффициент в* f *больше его коэффициента в* g*.*

(ii) Над полукольцом $\mathbb{R}_\infty$ *система* F *не имеет решений тогда и только тогда, когда существует алгебраическая комбинация* (f, g) *системы* F *со степенью не больше*

$$N = poly(n, k, d)\,(4d)^{\min(n,k)},$$

такая что для каждого монома $m = x_1^{\odot j_1} \odot \ldots \odot x_n^{\odot j_n}$ *его коэффициент в* f *больше его коэффициента в* g*, и с дополнительным свойством, что постоянный член в* g *конечен.*

Для случая мин-плюс многочленов нам потребуется следующее определение.

Определение 10.3. *Для системы мин-плюс многочленов $F = \{f_1, \ldots, f_k\}$ и мин-плюс мономов $m_1, \ldots, m_K$ алгебраическая комбинация*

$$g = \bigoplus_{j=1}^{K} g_j,$$

где

$$g_j = m_j \odot f_{i_j}, 1 \leqslant j \leqslant K$$

для некоторых мономов m_j и некоторых $1 \leqslant i_j \leqslant k$, называется невырожденной, *если выполняются следующие два условия:*

- *для всякого монома m в g существует (единственное) $1 \leqslant l(m) \leqslant K$, такое что коэффициент m в многочлене $g_{l(m)}$ меньше, чем коэффициент m во всех многочленах g_j для $j \neq l(m)$;*
- *для различных m и m' верно $l(m) \neq l(m')$.*

Проиллюстрируем это понятие на простом примере. Рассмотрим систему мин-плюс многочленов $F = \{f_1, f_2\}$, где $f_1 = 0 \odot x \oplus 0$ и $f_2 = 0 \odot x \oplus 1$. Мы уже обсуждали, что эта система на имеет корней. Теперь заметим, что у этой системы есть невырожденная алгебраическая комбинация. Действительно, рассмотрим $g_1 = \frac{1}{2} \odot f_1$, $g_2 = 0 \odot f_2$ и

$$g = g_1 \oplus g_2 = \frac{1}{2} \odot (0 \odot x \oplus 0) \oplus 0 \odot (0 \odot x \oplus 1) = \left(\frac{1}{2} \odot x \oplus \frac{1}{2}\right) \oplus (0 \odot x \oplus 1).$$

Заметим, что коэффициент постоянного монома минимален только в g_1, а коэффициент монома x минимален только в g_2.

Теперь мы можем сформулировать прямую теорему о нулях для мин-плюс многочленов. Эта теорема, в частности, говорит о том, что в предыдущем примере не случайно нашлась невырожденная алгебраическая комбинация.

Теорема 10.5 (Прямая теорема о нулях для мин-плюс многочленов). *Рассмотрим систему мин-плюс многочленов $F = \{f_1, \ldots, f_k\}$ от n переменных. Обозначим через d_i степень многочлена f_i и положим $d = \max_i d_i$.*

(i) Над полукольцом $\mathbb{R}$ система F не имеет решений тогда и только тогда, когда существует невырожденная алгебраическая комбинация g многочленов в F степени не больше

$$N = (n+2)\left(d_1 + \ldots + d_k\right).$$

(ii) Над полукольцом $\mathbb{R}_\infty$ система F не имеет решений тогда и только тогда, когда существует невырожденная алгебраическая комбинация g многочленов в F степени не больше

$$N = poly(n,k,d)\,(4d)^{\min(n,k)}$$

и с конечным постоянным коэффициентом.

Перейдем к доказательствам результатов этой главы.

10.2 Теоремы о нулях в двойственной форме

Всюду в этом разделе мы предполагаем, что нам дана система мин-плюс многочленов $F = \{f_1, \ldots, f_k\}$ от n переменных $\vec{x} = (x_1, \ldots, x_n)$.

Доказательства теорем 10.2 и 10.3 аналогичны. Мы подробно опишем доказательство теоремы 10.2 (которое будет более интуитивно естественным) и явно укажем, что должно быть изменено в рассуждениях, чтобы получить доказательство теоремы 10.3.

Этот раздел устроен следующим образом. В разделе 10.2.1 мы введем необходимые предварительные понятия и докажем предварительные результаты. В разделах 10.2.2 и 10.2.3 мы приведем доказательства теорем 10.2(i) и 10.3(i). В разделе 10.2.4 мы приведем примеры, иллюстрирующие трудности, которые обходит наше доказательство. В разделе 10.2.5 мы докажем теоремы 10.2(ii) и 10.3(ii). Наконец, в разделе 10.2.6 мы покажем, что верхние оценки в теоремах 10.2 и 10.3 точны.

10.2.1 Предварительные понятия и результаты

Геометрическая интерпретация мин-плюс многочленов. Все функции $\phi\colon \mathbb{Z}^n \to \mathbb{R}$, которые мы рассматриваем в этом разделе, являются частичными, то есть могут быть определены только на некотором подмножестве $\mathsf{Dom}(\phi) \subseteq \mathbb{Z}^n$.

Определение 10.4. *Для двух функций $\phi, \psi\colon \mathbb{Z}^n \to \mathbb{R}$ положим $D = \mathsf{Dom}\,\phi \cap \mathsf{Dom}\,\psi$ и рассмотрим $t \in \mathbb{R}$ (если оно существует), такое что*

1. *для всех $\vec{x} \in D$ верно $\phi(\vec{x}) + t \leqslant \psi(\vec{x})$;*
2. *существует $\vec{x} \in D$, такое что $\phi(\vec{x}) + t = \psi(\vec{x})$.*

Легко видеть, что если t существует, то оно единственно. Мы обозначаем множество точек $\vec{x}$, для которых выполняется свойство 2, через $\mathsf{Sing}(\phi, \psi)$ и называем их сингулярными точками *для пары (ϕ, ψ). Если такое t не существует, мы полагаем $\mathsf{Sing}(\phi, \psi) = \emptyset$. Мы говорим, что ϕ* сингулярно *к ψ, если $|\mathsf{Sing}(\phi, \psi)| \neq 1$.*

Предположим, что в случае непустого D функция $\psi(x) - \phi(x)$ достигает своего минимума на D (это всегда будет верно для функций, которые мы будем рассматривать, но это необязательно верно для случая бесконечного D). Тогда геометрически ϕ сингулярно к ψ, если либо области определения ϕ и ψ не пересекаются, либо мы можем сдвинуть график ϕ в пространстве $\mathbb{R}^{n+1}$ вдоль $(n+1)$-й оси так, чтобы весь график лежал ниже графика ψ и имел с ним не меньше двух общих точек. Для функции ϕ обозначим через $G(\phi)$ график этой функции в $\mathbb{R}^{n+1}$.

Заметим, что понятие сингулярности несимметричное. Может случиться, что ϕ сингулярна к ψ, но ψ не сингулярна к ϕ. Например, рассмотрим $\phi, \psi\colon \mathbb{Z} \to \mathbb{R}$, такие что $\phi(x) = 0$ для всех x, а $\psi(0) = 1$ и $\psi(x) = 0$ для всех $x \neq 0$.

Следующая лемма прямо следует из определения.

Лемма 10.3. *Верно, что* $\vec{x} \in \mathsf{Sing}(\phi, \psi)$ *тогда и только тогда, когда* $\vec{x}$ *минимизирует функцию* $\psi - \phi$ *(на ее области определения). Или, эквивалентно,* $\vec{x} \in \mathsf{Sing}(\phi, \psi)$ *тогда и только тогда, когда для всех* $\vec{y}$ *верно*

$$\phi(\vec{x}) - \phi(\vec{y}) \geqslant \psi(\vec{x}) - \psi(\vec{y}).$$

В этом разделе мы среди прочего будем рассматривать строки матрицы Маколея M_N, решения $M_N \odot \vec{y}$ и коэффициенты многочленов f_i. Все эти объекты являются векторами вида $\vec{a}$, координаты которых проиндексированы элементами $I \in D$ для некоторого $D \subseteq \mathbb{Z}_+^n$, то есть, векторами с целыми неотрицательными координатами. С каждым вектором $\vec{a}$ такого вида мы сопоставляем функцию $\phi_{\vec{a}} \colon \mathbb{Z}^n \to \mathbb{R}$, полагая $\phi_{\vec{a}}(I) = a_I$, если $I \in D$ и $a_I \neq \infty$, и оставляя $\phi_{\vec{a}}(I)$ неопределенным в противном случае. Когда вектор $\vec{a}$ — это вектор коэффициентов многочлена f, мы коротко обозначаем получившуюся функцию через ϕ_f. Если многочлен f — это один из многочленов $f_i \in F$, мы дополнительно упрощаем обозначение соответствующей функции до ϕ_i. Заметим, что по определению M_N, если $\vec{r}$ — строка матрицы M_N, проиндексированная (i, J), то $\phi_{\vec{r}}(I) = \phi_i(I - J)$.

Далее в этом разделе мы используем греческие буквы для функций, представляющих коэффициенты многочленов или строки матрицы Маколея, чтобы было проще отличать их от функций f_i.

Мотивацией для введенного нами понятия сингулярности является то, что оно отражает наличие корня у мин-плюс многочленов.

Лемма 10.4. *Вектор* $\vec{a} = \{a_I\}_{|I| \leqslant N}$ *над* $\mathbb{R}$ *или* $\mathbb{R}_\infty$ *является корнем линейного мин-плюс многочлена* $\min_I\{y_I + r_I\}$, *соответствующего вектору* $\vec{r} = \{r_I\}_{|I| \leqslant N}$, *тогда и только тогда, когда функция* $-\phi_{\vec{a}}$ *сингулярна к* $\phi_{\vec{r}}$.

Доказательство. Рассмотрим произвольный вектор $\vec{r}$ над $\mathbb{R}$ или $\mathbb{R}_\infty$ и соответствующий линейный мин-плюс многочлен. Вектор $\vec{a}$ является корнем этого линейного многочлена, если минимум в $\{\phi_{\vec{a}}(I) + \phi_{\vec{r}}(I)\}_I$ достигается дважды или равен ∞. Этот минимум равен ∞ тогда и только тогда, когда

$\mathsf{Dom}(\phi_{\vec{a}}) \cap \mathsf{Dom}(\phi_{\vec{r}}) = \emptyset$, что означает, что $\mathsf{Sing}(-\phi_{\vec{a}}, \phi_{\vec{r}}) = \emptyset$. Если минимум конечен, положим t равным минимальному числу, такому что $\phi_{\vec{a}}(I) + \phi_{\vec{r}}(I) + t \geqslant 0$ для всех I. Тогда $\phi_{\vec{a}}(I) + \phi_{\vec{r}}(I) + t = 0$ для хотя бы двух различных I. Это означает, что $-\phi_{\vec{a}}(I) - t \leqslant \phi_{\vec{r}}(I)$ и равенство верно на хотя бы двух точках. Таким образом, функция $-\phi_{\vec{a}}$ сингулярна к $\phi_{\vec{r}}$.

Доказательство в другую сторону аналогично. ■

В частности, вектор $\vec{y}$ является решением системы $M_N \odot \vec{y}$ тогда и только тогда, когда $-\phi_{\vec{y}}$ сингулярна ко всем $\phi_{\vec{r}}$, где $\vec{r}$ — строки матрицы M_N.

Существенная разница между полукольцами $\mathbb{R}$ и $\mathbb{R}_\infty$ состоит в том, что над $\mathbb{R}$ верно, что $\mathsf{Dom}\, \phi_{\vec{y}} = \{I |\ |I| \leqslant N\}$.

Теперь пусть $\vec{r}$ — вектор коэффициентов мин-плюс многочлена f, то есть r_I — коэффициент монома $\vec{x}^I$ в f. Тогда корни многочлена f задаются векторами $\vec{x} = (x_1, \ldots, x_n)$. Как мы уже описывали выше, можно такому вектору $\vec{x}$ сопоставить решение для соответствующих строк матрицы Маколея $\vec{y}$ следующим образом:

$$y_I = \vec{x}^I = \sum_j i_j x_j = \langle \vec{x}, I \rangle.$$

То есть вектор решения задается как (классическое) скалярное произведение векторов $\vec{x}$ и I. Таким образом, в этом случае $\phi_{\vec{y}}(I) = \langle \vec{x}, I \rangle$ — частичная линейная функция (заметим, что некоторые координаты x_j вектора $\vec{x}$ могут быть равны бесконечности, и тогда $y_I = \infty$ как только $i_j \neq 0$ для хотя бы одной бесконечной координаты x_j), график которой является частью гиперплоскости в $(n+1)$-мерном пространстве. Заметим, что мы считаем здесь, что $0 \cdot \infty = 0$. Введем обозначение $\chi_{\vec{x}} = -\phi_{\vec{y}}$ и будем говорить, что $\chi_{\vec{x}}$ — *частичная гиперплоскость*. Над $\mathbb{R}$ функция $\chi_{\vec{x}}$ соответствует обычным гиперплоскостям. Таким образом, из леммы 10.4 мы получаем следующий результат.

Лемма 10.5. *Вектор $\vec{x} \in \mathbb{R}_\infty^n$ является корнем f тогда и только тогда, когда частичная гиперплоскость $\chi_{\vec{x}}$ сингулярна к функции ϕ_f.*

В частности, система многочленов F имеет корень над $\mathbb{R}_\infty$ тогда и только тогда, когда существует частичная гиперплоскость, сингулярная к ϕ_i для всех $i = 1, \ldots, k$.

Как следствие мы получаем, что если есть частичная гиперплоскость, сингулярная к ϕ_i для всех $i = 1, \ldots, k$, то она задает решение линейной системы с матрицей M_N. Это повторяет доказательство двойственной теоремы о нулях в простую сторону. Что нам требуется доказать, чтобы доказать теорему в обратную сторону, это то, что если есть некоторая функция, сингулярная ко всем сдвигам всех функций ϕ_i в пределах некоторого симплекса $|I| \leqslant N$, то есть и сингулярная частичная гиперплоскость.

Для доказательства теоремы 10.2 удобно использовать язык многогранников. Мы описываем его в следующем определении.

Определение 10.5. *Чтобы перейти к языку многогранников, для многочлена $f \in F$ рассмотрим график $G(\phi_f) = \{(I, \phi_f(I)) \mid I \in \mathbb{Z}^n,\ \phi_f(I) \neq \infty\}$ функции ϕ_f и вместе с каждой точкой $(I, \phi_f(I))$ рассмотрим все точки (I, t) выше нее, то есть, такие что $t > \phi_f(I)$. Возьмем выпуклую оболочку всех этих точек в $\mathbb{R}^{n+1}$, обозначим полученный многогранник через $P(f)$ и назовем* (расширенным) многогранником Ньютона *для f. Для данной системы F многочленов $f_1, \ldots, f_k$ обозначим эти многогранники через $P_1, \ldots, P_k$. Отметим, что эта конструкция достаточно стандартна [78, 113, 123].* Дном *многогранника $P(f)$ назовем множество точек $\vec{x} = (x_1, \ldots, x_n, x_{n+1}) \in P(f)$, таких что ниже них нет точек $P(f)$, то есть для любого $\epsilon > 0$ верно $(x_1, \ldots, x_n, x_{n+1} - \epsilon) \notin P(f)$. Заметим, что дно $P(f)$ можно рассматривать как график частичной функции на $\mathbb{R}^n$. Будем обозначать сужение этой функции на $\mathbb{Z}^n$ через $\beta_P \colon \mathbb{Z}^n \to \mathbb{R}$. Заметим, что в случае, когда график ϕ_f образует выпуклое множество, новая функция β_P является доопределением функции ϕ_f. Для случая многогранников P_i мы сокращаем обозначение до β_i. Нетрудно увидеть геометрически, что частичная гиперплоскость сингулярна к ϕ_f тогда и только тогда, когда*

она сингулярна к β_P. Это необязательно верно для произвольной функции $\phi_{\vec{a}}$ вместо гиперплоскости.

Замечание 10.1. *Заметим, что в работе [59] гипотеза о двойственной теореме о нулях для мин-плюс многочленов рассматривалась не для изначальной матрицы Маколея, а для матрицы Маколея, в которой уже совершен переход к выпуклым оболочкам для многочленов в F, то есть вместо значений функций ϕ_i строки матрицы Маколея содержали значения функций β_{P_i}. Наше доказательство работает и для этого случая тоже, но мы считаем, что формулировка с оригинальной матрицей Маколея более естественна.*

Замечание 10.2. *Для случая мин-плюс уравнений мы аналогично сопоставляем каждому уравнению $(f_i, g_i) \in F$ функцию ϕ_i. Мы полагаем $\phi_i(I)$ равным минимуму коэффициентов монома $\vec{x}^I$ в f_i и g_i. Дополнительно мы вводим цвета для точек графика $G(\phi_i)$. Если $\phi_i(I)$ равно коэффициенту $\vec{x}^I$ в f_i, то мы красим $(I, \phi_i(I))$ в черный цвет, и если $\phi_i(I)$ равно коэффициенту $\vec{x}^I$ в g_i, мы красим $(I, \phi_i(I))$ в белый цвет. Заметим, что мы разрешаем покрасить одну и ту же точку в два цвета одновременно.*

В определении понятия сингулярности некоторой функции ϕ к ψ мы теперь рассматриваем в качестве ψ раскрашенную функцию. Для того, чтобы ϕ была сингулярной к ψ, мы требуем, чтобы либо сингулярных точек не было, либо было хотя бы по одной сингулярной точке каждого цвета. Заметим, однако, что нас также устроит, если будет одна сингулярная точка, но покрашенная сразу в оба цвета. Аналог леммы 10.4 доказывается аналогично. Заметим, что теперь мы работаем с мин-плюс уравнениями, и, чтобы получить решение, нам нужно, чтобы минимум достигался на мономах в обеих разных частях уравнения. Это напрямую соответствует наличию сингулярных точек обоих цветов. Аналог леммы 10.5 доказывается аналогично.

Многогранники Ньютона P_i вводятся аналогично (в построении многогранников мы игнорируем цвета). Но заметим, что некоторые точки P_i покрашены. В частности, покрашены все вершины.

Выпуклые многогранники. Выпуклый многогранник P в n-мерном пространстве можно задать системой (классических) линейных функций $E_1(\vec{x}), \ldots, E_l(\vec{x}), L_1(\vec{x}), \ldots, L_k(\vec{x})$, где $\vec{x} \in \mathbb{R}^n$: P состоит из точек $\vec{x} \in \mathbb{R}^n$, таких что $E_i(\vec{x}) = 0$ для всех $i = 1, \ldots, l$, и $L_i(\vec{x}) \geqslant 0$ для всех $i = 1, \ldots, k$. Мы предполагаем, что ни одна из форм $L_i(\vec{x})$ не обращается в 0 на множестве $\{\vec{x} \mid \forall i\ E_i(\vec{x}) = 0\}$. Каждая грань многогранника может быть задана непустым множеством $S \subseteq \{1, \ldots, k\}$. Грань, соответствующая S, состоит из точек $\vec{x} \in P$, таких что $L_i(\vec{x}) = 0$ для всех $i \in S$.

Границей многогранника будем называть объединение его граней. Внутренностью $\mathring{P}$ многогранника P будем называть множество его не граничных точек.

Для многогранников P_1 и P_2 мы обозначаем через $P_1 + P_2$ сумму Минковского этих многогранников. Для натурального k мы используем обозначение $kP = P + \ldots + P$, где в правой части равенства k слагаемых. Для n-мерного вектора $\vec{\alpha}$ мы обозначаем через $P + \vec{\alpha}$ сдвиг P на вектор $\vec{\alpha}$. То есть,

$$P + \vec{\alpha} = \{\vec{x} + \vec{\alpha} \mid \vec{x} \in P\}.$$

Гомотетией с центром $\vec{x} \in \mathbb{R}^n$ и коэффициентом $\lambda > 0$ мы называем следующее биективное преобразование $h^\lambda_{\vec{x}}$ пространства $\mathbb{R}^n$: точка $\vec{y} \in \mathbb{R}^n$ отображается в точку $h^\lambda_{\vec{x}}(\vec{y}) = \vec{x} + \lambda(\vec{y} - \vec{x})$. Заметим, что kP — это образ P под действием гомотетии $h^k_{\vec{0}}$. Хорошо известно, что множество сдвигов и гомотетий вместе с операцией композиции образуют группу. В частности, произвольная композиция сдвигов и гомотетий является сдвигом или гомотетией. Ниже мы будем использовать этот факт без дополнительных упоминаний.

Определение 10.6. *Рассмотрим многогранник $P \subseteq \mathbb{R}^n$, множество точек $Q \subseteq \mathbb{R}^n$ и точку $\vec{x}$ на границе P. Мы говорим, что Q* касается *P в $\vec{x}$, если*

1. $Q \subseteq P$;

2. $\vec{x} \in Q$;

3. *если Q содержит точку $\vec{y}$ на границе P, то $\vec{y}$ лежит в какой-то грани P, содержащей $\vec{x}$.*

Ниже мы приведем некоторые факты о структуре выпуклых многогранников, которые нам потребуются в дальнейшем. Хотя эти факты просты и интуитивно понятны, мы приводим доказательства для полноты изложения.

Лемма 10.6. *Пусть P — выпуклый многогранник, и пусть $\vec{x}, \vec{y}, \vec{z}$ — три различные точки в P, лежащие на одной прямой в указанном порядке. Тогда, если $\vec{y}$ лежит в некоторой грани P, то $\vec{x}$ лежит в той же грани P.*

Доказательство. Предположим от противного, что $\vec{y}$ принадлежит некоторой грани, а $\vec{x}$ нет. Тогда есть некоторое неравенство L среди неравенств, задающих P, такое что $L(\vec{x}) > 0$ и $L(\vec{y}) = 0$. Ограничение функции L на прямую, содержащую $\vec{x}$, $\vec{y}$ и $\vec{z}$, является линейной функцией, а значит $L(\vec{z}) < 0$. Следовательно, $\vec{z}$ не лежит в P. Получаем противоречие. ■

Следствие 10.7. *Пусть P — выпуклый многогранник, и пусть $\vec{x}, \vec{y}, \vec{z}, \vec{t}$ — четыре различные точки в P, лежащие на одной прямой в указанном порядке. Тогда $\vec{y}$ лежит в некоторой грани P тогда и только тогда, когда $\vec{z}$ лежит в той же грани.*

Доказательство. Достаточно применить лемму 10.6 к точкам $\vec{y}, \vec{z}, \vec{t}$ и к точкам $\vec{z}, \vec{y}, \vec{x}$. ■

Лемма 10.8. *Пусть P — выпуклый многогранник, и пусть $\vec{x}$ — точка в P. Обозначим через P' образ P под действием $h^{\lambda}_{\vec{x}}$ для $\lambda > 1$. Если P содержит точку на некоторой грани P', то эта грань содержит $\vec{x}$.*

Доказательство. Пусть $\vec{y}$ — точка в P. Тогда точка

$$\vec{z} = h^{\lambda}_{\vec{x}}(\vec{y}) = \vec{x} - \lambda(\vec{y} - \vec{x})$$

лежит в P', и точки $\vec{x}, \vec{y}, \vec{z}$ лежат на одной прямой в указанном порядке. Тогда по лемме 10.6, если $\vec{y}$ лежит в некоторой грани P', то $\vec{x}$ также лежит в этой грани. ■

10.2.2 Объемлющий многогранник

Ключевая идея доказательства теоремы 10.2(i) состоит в том, чтобы рассмотреть большой (расширенный) многогранник Ньютона P_0, «объемлющий» все многогранники $P_1, \ldots, P_k$, соответствующие мин-плюс многочленам $f_1, \ldots, f_k$. Основное свойство P_0, которое мы установим в этом разделе, состоит в том, что для всякой точки $\vec{x}$ на его дне и для всякого i существует сдвиг $P_i + \vec{\alpha}$ многогранника P_i, такой что $P_i + \vec{\alpha}$ касается P_0 в $\vec{x}$ (лемма 10.10). Используя это свойство, в следующем разделе мы докажем, что для решения $\vec{a}$ линейной мин-плюс системы $M_N \odot \vec{y}$ существует сингулярная точка в $\mathsf{Sing}(\vec{a}, \beta_{P_0})$, такая что грань P_0, содержащая точку $(\vec{a}, \beta_{P_0}(\vec{a}))$, задает корень системы F (лемма 10.12).

Оказывается, что в качестве P_0 мы можем взять просто сумму Минковского многогранников $P_1, \ldots, P_k$, умноженную на достаточно большое число. Мы просто полагаем

$$P_0 = (n+2) \cdot (P_1 + \ldots + P_k)\,. \tag{10.1}$$

Чтобы доказать желаемые свойства P_0, нам потребуется следующий общий факт о выпуклых многогранниках.

Лемма 10.9. *Пусть P — n-мерный выпуклый многогранник, и пусть $P' = (n+2)P$. Тогда для всякой точки $\vec{x} \in \mathring{P}'$ существует сдвиг $P + \vec{\alpha}$ многогранника P и гомотетия $h^{n+2}_{\vec{y}}$, отображающая $P + \vec{\alpha}$ в P', со следующими свойствами:*

1. *центр $\vec{y}$ этой гомотетии лежит в $\mathring{P}'$;*

2. $\vec{x}$ является вершиной $P + \vec{\alpha}$.

Нетрудно увидеть, что первое свойство равносильно тому, что $P + \vec{\alpha} \subseteq \mathring{P}'$, однако текущая формулировка леммы будет более удобна для нас.

Основными инструментами в доказательстве этой леммы является теорема Каратеодори, понятие центра масс и гомотетические преобразования.

Доказательство. Мы сначала приведем краткий план доказательства, а затем уже перейдем к полному формальному доказательству. Поскольку точка $\vec{x}$ лежит в P', она лежит в некотором симплексе S', построенном на $n+1$ вершине P'. Для S' мы рассматриваем каждую из его вершин и применяем к S' гомотетию с центром в этой вершине и с коэффициентом $(n+1)/(n+2)$. Получившиеся $(n+1)$ меньших симплексов покрывают весь S' (даже с перекрытием). Так что $\vec{x}$ лежит в одном из них, пусть в том, который задается вершиной v'_1. Затем мы рассматриваем сдвиг $S + \vec{\alpha}$ симплекса S, который в $(n+2)$ раза меньше, чем S', такой что его вершина, соответствующая v'_1, отображается в $\vec{x}$. Тогда $S + \vec{\alpha}$ лежит в S'. Мы можем рассмотреть P' и заметить, что $P + \vec{\alpha}$ лежит в P'.

Теперь мы дадим формальное доказательство, следующее приведенному плану. Поскольку $\vec{x}$ — точка лежащая в выпуклом многограннике P', она лежит в выпуклой оболочке вершин многогранника. По теореме Каратеодори существуют $n+1$ вершин $v'_1, \ldots, v'_{n+1}$ многогранника P', таких что $\vec{x} \in \mathrm{Conv}\{v'_1, \ldots, v'_{n+1}\}$. Обозначим симплекс на этих вершинах через S' и обозначим соответствующие вершины P через $v_1, \ldots, v_{n+1}$.

Пусть $w_1, \ldots w_{n+1}$ — барицентрические координаты $\vec{x}$ относительно $v'_1, \ldots, v'_{n+1}$, то есть $w_i \geqslant 0$ для всех i, $\sum_i w_i = 1$ и

$$\vec{x} = \sum_i w_i v'_i.$$

Без ограничения общности пусть w_1 — максимален среди всех w_i. Тогда $nw_1 \geqslant w_2 + \ldots + w_{n+1}$. Положим

$$v' = \frac{1}{\sum_{i=2}^{n+1} w_i} \sum_{i=2}^{n+1} w_i v'_i.$$

Тогда $v' \in \mathrm{Conv}\{v'_2, \dots v'_{n+1}\}$ и верно соотношение

$$\vec{x} = w_1 v'_1 + \left(\sum_{i=2}^{n+1} w_i\right) v'.$$

Следовательно, точки v'_1, $\vec{x}$ и v' лежат на одной прямой. Более того, $|\vec{x} - v'_1| \leqslant n|v' - \vec{x}| < (n+1)|v' - \vec{x}|$ (заметим, что $|v' - \vec{x}|$ не равно нулю, поскольку w_1 не равен нулю как максимальный вес). Рассмотрим точку $\vec{y}$ на той же прямой между точками $\vec{x}$ и v', такую что $(n+1)|\vec{x} - \vec{y}| = |v'_1 - \vec{x}|$.

Теперь рассмотрим многогранник P и рассмотрим его сдвиг $P + \alpha$, при котором v_1 переводится в $\vec{x}$. Гомотетия $h^{n+2}_{\vec{y}}$ переводит $\vec{x}$ в v'_1, и поскольку $(n+2)P$ и P' равны, образ $P+\alpha$ под действием этой гомотетии совпадает с P'.

Остается лишь заметить, что точки $\vec{x}$, $\vec{y}$, v' лежат на одной прямой в указанном порядке и все лежат в P'. Следовательно, по лемме 10.6, поскольку $\vec{x} \in \mathring{P}'$, мы получаем, что $\vec{y} \in \mathring{P}'$. ■

Замечание 10.3. *Заметим, что лемма 10.9 не верна для $P' = (n+1)P$. Контрпример очень простой: пусть P — стандартный симплекс, то есть выпуклая оболочка точек $\{0, \vec{e}_1, \dots, \vec{e}_n\}$. Тогда $P' = (n+1)P$ — выпуклая оболочка точек $\{\vec{0}, (n+1)\vec{e}_1, \dots, (n+1)\vec{e}_n\}$. Положим $\vec{x}$ равным центру многогранника P', то есть $\vec{x} = \vec{e}_1 + \ldots + \vec{e}_n$. Тогда для того, чтобы $\vec{x}$ был вершиной $P + \vec{\alpha}$, нам придется либо положить $\vec{\alpha} = \vec{e}_1 + \ldots + \vec{e}_n$, либо положить $\vec{\alpha} = \vec{e}_1 + \ldots + \vec{e}_{i-1} + \vec{e}_{i+1} + \ldots + \vec{e}_n$ для некоторого i. В первом случае $\vec{y} = (n+1)(\vec{e}_1 + \ldots + \vec{e}_n)/n$, а во втором — $\vec{y} = (n+1)(\vec{e}_1 + \ldots + \vec{e}_{i-1} + \vec{e}_{i+1} + \ldots + \vec{e}_n)/n$. В обоих случаях $\vec{y}$ лежит на границе P': в первом случае он лежит в выпуклой оболочке $\{\vec{e}_1, \dots, \vec{e}_n\}$, а во втором случае — в выпуклой оболочке $\{\vec{0}, \vec{e}_1, \dots, \vec{e}_{i-1}, \vec{e}_{i+1}, \dots, \vec{e}_n\}$.*

Лемма 10.10. *Для всякой точки $\vec{x}$ на дне P_0 и для всякого P_j существует $\vec{\alpha}$, такое что $P_j + \vec{\alpha}$ касается P_0 в $\vec{x}$.*

Доказательство. Пусть

$$P = P_1 + \ldots + P_k.$$

Тогда $P_0 = (n+2)P$.

Сначала мы покажем, что существует сдвиг P, касающийся P_0 в $\vec{x}$.

Если $\vec{x}$ — вершина P_0, просто заметим, что существует сдвиг $P+\vec{\alpha}'$, лежащий в P_0 и содержащий $\vec{x}$ (поскольку P_0 — сумма Минковского и P — одно из слагаемых, P_0 можно рассматривать как объединение сдвигов P). Поскольку $\vec{x}$ — вершина P_0, она также является вершиной $P + \vec{\alpha}'$. Гомотетия $h_{\vec{x}}^{n+2}$ отображает $\vec{x}$ как вершину $P + \vec{\alpha}'$ в $\vec{x}$ как соответствующую вершину P_0, а следовательно, отображает $P + \vec{\alpha}'$ в P_0. Тогда по лемме 10.8 $P + \vec{\alpha}'$ касается P_0 в $\vec{x}$.

Если $\vec{x}$ не является вершиной P_0, обозначим грань минимальной размерности в P_0, содержащую $\vec{x}$, через Q_0. Ясно, что $\vec{x}$ лежит во внутренности Q_0. Поскольку $P_0 = (n+2)P$, то существует грань Q многогранника P, такая что $Q_0 = (n+2)Q$. По лемме 10.9 мы можем найти сдвиг $Q + \vec{\alpha}'$, такой что $\vec{x}$ является вершиной $Q + \vec{\alpha}'$ и $Q + \vec{\alpha}' \subseteq Q_0$. Эта лемма также дает нам гомотетию $h_{\vec{y}}^{n+2}$, центр которой $\vec{y}$ лежит во внутренности Q_0. Теперь рассмотрим $P + \vec{\alpha}'$ и рассмотрим его образ под действием $h_{\vec{y}}^{n+2}$. Вершина $\vec{x}$ отображается под действием этой гомотетии в соответствующую вершину P_0, и следовательно, $P+\vec{\alpha}'$ отображается в P_0. Заметим, что по лемме 10.8 мы также получаем, что $P+\vec{\alpha}'$ пересекает P_0 только по граням, содержащим $\vec{y}$, а значит, только по граням, содержащим $\vec{x}$.

Теперь заметим, что $P + \vec{\alpha}'$ — это сдвиг суммы Минковского $P_1 + \ldots + P_k$, а значит, для всякого P_j существует сдвиг $\vec{\alpha}$, такой что $P_j + \vec{\alpha}$ лежит в $P + \vec{\alpha}'$ и содержит точку $\vec{x}$. Поскольку эта точка является вершиной $P+\vec{\alpha}'$, мы получаем, что $\vec{x}$ также является вершиной $P_j+\vec{\alpha}$. Заметим, что $P_j+\vec{\alpha}$ лежит внутри $P+\vec{\alpha}'$, а значит, он может пересекаться с границей P_0 только по граням, содержащим $\vec{x}$. ■

Следствие 10.11. *Для всякой точки $\vec{x}$ на дне P_0 и для всякого f_j существует $\vec{\alpha}$, такой что $G(\phi_j) + \vec{\alpha}$ касается P_0 в $\vec{x}$.*

Доказательство. Заметим, что множество $G(\phi_j) + \vec{\alpha}$ является подмножеством многогранника $P_j + \vec{\alpha}$, но с другой стороны, содержит все его вершины. Следовательно, $G(\phi_j) + \vec{\alpha}$ касается P_0 в $\vec{x}$. ■

Замечание 10.4. *Анализ в этом разделе дословно переносится на случай мин-плюс уравнений.*

10.2.3 Сингулярность грани P_0

В этом разделе мы завершим доказательство теорем 10.2(i) и 10.3(i).

Для удобства в этом разделе мы будем называть $(n+1)$-мерный вектор $\vec{\alpha}$ (или точку в $\mathbb{R}^{n+1}$) целочисленным, если его первые n координат целые.

Следующее наблюдение не потребуется в доказательстве, но оно помогает прояснить интуицию, стоящую за конструкциями в доказательстве.

Утверждение 10.1. *Рассмотрим дно β_{P_0} многогранника P_0 и рассмотрим соответствующий ему вектор $\{a_I\}_I$, то есть $a_I = \beta_{P_0}(I)$, если $\beta_{P_0}(I)$ определено, и $a_I = \infty$ иначе. Рассмотрим мин-плюс многочлен $g = \oplus_I \left(a_I \odot \vec{x}^I\right)$. Тогда для всякого f_j многочлен g лежит в мин-плюс идеале, порожденном f_j (мин-плюс идеал — это просто множество всех многочленов, которые могут быть получены мин-плюс алгебраической комбинацией порождающих многочленов).*

Доказательство. Доказательство проще провести в геометрических терминах. Для всякой целочисленной точки $\vec{x}$ на дне P_0 рассмотрим сдвиг $G(\phi_j) + \vec{\alpha}_{\vec{x}}$, касающийся P_0 в $\vec{x}$, который существует по следствию 10.11. Этот сдвиг соответствует мин-плюс умножению многочлена f_j на моном. Тогда легко видеть,что все целочисленные точки на дне P_0 лежат в объединении $G(\phi_j) + \vec{\alpha}_{\vec{x}}$ по всем $\vec{x}$, и с другой стороны, все остальные целочисленные точки этого объединения лежат в P_0. Операция объединения (с последующим взятием выпуклой оболочки) соответствует операции взятия минимума (мин-плюс сложения) для многочленов. ■

Лемма 10.12. *Пусть мин-плюс линейная система $M_N \odot \vec{y}$ имеет решение $\vec{a}$.*

(i) Пусть мы рассматриваем случай мин-плюс полукольца $\mathbb{R}$.

(ii) Пусть мы рассматриваем случай мин-плюс полукольца $\mathbb{R}_\infty$, и существует $\vec{x} \in \mathbb{Z}^n$, такой что $\vec{x} \in \mathsf{Dom}\, \beta_{P_0} \cap \mathsf{Dom}\, \phi_{\vec{a}}$.

Тогда существует грань P_0 положительной размерности, такая что всякая гиперплоскость, содержащая эту грань и не пересекающая внутренность P_0, задает решение мин-плюс системы многочленов F.

Доказательство. Рассмотрим функции $\phi_{\vec{a}}$ и β_{P_0}. Поскольку в обоих случаях ($\mathbb{R}$ и $\mathbb{R}_\infty$) существует точка $\vec{x} \in \mathsf{Dom}\, \beta_{P_0} \cap \mathsf{Dom}\, \phi_{\vec{a}}$, мы получаем, что существует сингулярная точка в $\mathsf{Sing}(\phi_{\vec{a}}, \beta_{P_0})$. Дальнейшее доказательство работает сразу для обоих случаев.

Для всякой точки $\vec{x} \in \mathsf{Sing}(\phi_{\vec{a}}, \beta_{P_0})$ рассмотрим минимальную размерность грани P_0, содержащей точку $(\vec{x}, \beta_{P_0}(\vec{x}))$, и далее через $\vec{x}$ будем обозначать точку в $\mathsf{Sing}(\phi_{\vec{a}}, \beta_{P_0})$, для которой максимизируется эта минимальная размерность. Другими словами, нас интересует сингулярная точка в наиболее общем положении относительно P_0. Обозначим грань P_0 минимальной размерности, содержащую $(\vec{x}, \beta_{P_0}(\vec{x}))$ через Q_0. Дальше мы доказываем, что эта грань удовлетворяет условиям леммы.

Рассмотрим произвольный многочлен f_j. По следствию 10.11 существует вектор $\vec{\alpha}$, такой что $G(\phi_j) + \vec{\alpha}$ касается P_0 в $(\vec{x}, \beta_{P_0}(\vec{x}))$. Обозначим через ψ функцию с графиком $G(\phi_j) + \vec{\alpha}$ (заметим, что благодаря выбору N, функция ψ соответствует одной из строк M_N с точностью до аддитивной константы). Тогда, в частности, верно, что $\vec{x} \in \mathsf{Sing}(\beta_{P_0}, \psi)$. Поскольку также верно, что $\vec{x} \in \mathsf{Sing}(\phi_{\vec{a}}, \beta_{P_0})$, ясно, что также верно и то, что $\vec{x} \in \mathsf{Sing}(\phi_{\vec{a}}, \psi)$ (действительно, поскольку $\vec{x}$ по лемме 10.3 минимизирует функции $\psi - \beta_{P_0}$ и $\beta_{P_0} - \phi_{\vec{a}}$, он также минимизирует их сумму; заметим, что все три функции определены в точке $\vec{x}$, так что все три минимума существуют). Однако, вспомним, что

$\vec{a}$ является корнем системы $M_N \odot \vec{y}$, и ψ соответствует одной из строк M_N. Следовательно, $|\mathsf{Sing}(\phi_{\vec{a}}, \psi)| \geqslant 2$. Но всякая точка, минимизирующая $\psi - \phi_{\vec{a}}$, должна также минимизировать $\psi - \beta_{P_0}$ и $\beta_{P_0} - \phi_{\vec{a}}$ (поскольку $\vec{x}$ их минимизирует), следовательно, всякая точка в $\mathsf{Sing}(\phi_{\vec{a}}, \psi)$ также лежит в обоих множествах $\mathsf{Sing}(\phi_{\vec{a}}, \beta_{P_0})$ и $\mathsf{Sing}(\beta_{P_0}, \psi)$. В частности, $|\mathsf{Sing}(\beta_{P_0}, \psi)| \geqslant |\mathsf{Sing}(\phi_{\vec{a}}, \psi)|$, и следовательно, существует вторая общая точка у $G(\phi_j) + \vec{\alpha}$ и дном P_0.

Поскольку $G(\phi_j) + \vec{\alpha}$ касается P_0 в $\vec{x}$, верно, что всякая точка в $|\mathsf{Sing}(\beta_{P_0}, \psi)|$ лежит в грани P_0, содержащей $(\vec{x}, \beta_{P_0}(\vec{x}))$. Если она не лежит в грани Q_0, то грань минимальной размерности, содержащей эту точку, имеет большую размерность, чем Q_0, что противоречит максимизации этого свойства у $(\vec{x}, \beta_{P_0}(\vec{x}))$. Следовательно, существует не меньше двух общих точек у $G(\phi_j) + \vec{\alpha}$ и Q_0. Следовательно, всякая гиперплоскость H, проходящая через Q_0, и не пересекающая внутренность P_0, сингулярна к функции, задаваемой $G(\phi_j) + \vec{\alpha}$, и следовательно, задает корень f_j. Поскольку это рассуждение работает для всех f_j, и Q_0 не зависит от f_j, мы получаем, что H сингулярна ко всем $f_1, \ldots, f_k$, и следовательно, задает корень системы F. ■

Замечание 10.5. *Для случая мин-плюс уравнений формулировка леммы 10.12 остается такой же. Доказательство почти полностью повторяет доказательство в случае многочленов. Мы рассматриваем решение $\vec{a}$ для линейной мин-плюс системы уравнений с матрицами Маколея, рассматриваем сингулярную точку $\phi_{\vec{a}}$ и β_{P_0} с таким же максимизационным свойством, как раньше. Мы рассматриваем $G(\phi_j)$ для произвольного j, как и раньше. И здесь у нас будет единственное отличие от прошлого доказательства. Сингулярность $\phi_{\vec{a}}$ и ψ дает нам то, что существуют белая и черная сингулярные точки (см. замечание 10.2). Заметим, что это может быть одна и та же точка с двумя цветами. Далее, такое же рассуждение, как и раньше, показывает, что точки обоих цветов лежат в Q_0, что завершает доказательство.*

Таким образом, лемма 10.12(i) дает, что если над $\mathbb{R}$ линейная мин-плюс система многочленов $M_N \odot \vec{y}$ имеет корень, то и система многочленов F имеет корень. Это завершает доказательство теоремы 10.2(i). Мы используем лемму 10.12(ii) в доказательстве теоремы 10.2(ii) позже. Аналогично, теорема 10.3(i) следует из аналога леммы 10.12(i) для уравнений, как описано в замечании 10.5.

10.2.4 Примеры

Мы приводим несколько примеров, показывающих, почему случай $n > 1$ в теореме 10.2(i) существенно сложнее случая $n = 1$.

Ступенчатая пирамида. В случае $n = 1$ в работе [59] было доказано, что если мы рассмотрим любой корень $\{a_i\}_i$ для системы с бесконечной матрицей Маколея и рассмотрим его координаты a_i для достаточно больших i, то в некотором естественном смысле они уже будут задавать корень, являющийся гиперплоскостью (то есть, линейной функцией по i). Эта гиперплоскость сразу дает корень для системы многочленов.

Мы покажем, что это необязательно так уже для случая двух переменных $n = 2$.

Для этого рассмотрим мин-плюс многочлен f с графиком

$$G(f) = \{(0,0,0), (0,1,0),\\ (1,0,0), (1,1,0)\}.$$

Его выпуклая оболочка — это просто квадрат.

Рассмотрим систему мин-плюс многочленов, состоящую из одного многочлена f. Рассмотрим линейную мин-плюс систему с матрицей Маколея, соответствующую системе $\{f\}$. Для этой системы построим решение $\phi\colon \mathbb{Z}^2 \to \mathbb{R}$, такое что даже если мы посмотрим на это решение $\phi(x, y)$ только для достаточно

больших (по абсолютному значению) значений переменных (x, y), функция ϕ все равно будет нелинейной, насколько большие x и y мы бы не брали.

Нам будет удобнее описать непрерывный вариант решения. Дискретное решение определяется целыми точками непрерывного решения.

Пусть $S_k = \{(x, y) | 10(k-1) \leqslant |x|, |y| \leqslant 10k\}$ для $k \geqslant 1$. Для каждого нечетного k мы полагаем решение $\phi\colon \mathbb{R}^2 \to \mathbb{R}$ равным константе на S_k. Для каждого четного k мы делим S_k на четыре области прямыми $y = x$ и $y = -x$. В области с $x \geqslant |y|$ мы полагаем $\phi(x, y) = x + C$, где C мы зафиксируем позднее. Аналогично для $x \leqslant -|y|$ мы полагаем $\phi(x, y) = -x + C$, для $y \geqslant |x|$ мы полагаем $\phi(x, y) = y + C$, и для $y \leqslant -|x|$ мы полагаем $\phi(x, y) = -y + C$. Мы подбираем константы в этих линейных и постоянных функциях так, чтобы ϕ была непрерывной на всей плоскости.

Нетрудно видеть, что график ϕ сингулярен ко всем сдвигам выпуклой оболочки $G(f)$, и, таким образом, является корнем для линейной мин-плюс системы с матрицей Маколея. Действительно, рассмотрим сдвиг f на произвольный вектор (a, b) и обозначим соответствующую функцию через ψ. Ее область определения равна $D = \{(a, b), (a, b+1), (a+1, b), (a+1, b+1)\}$. Рассмотрим сингулярную точку (c, d) в $\mathsf{Sing}(\phi, \psi)$. Без ограничения общности можно предполагать, что $|c| \geqslant |d|$. Тогда нетрудно видеть, что другая точка в D с первой координатой c также является сингулярной точкой. Это можно сделать прямым вычислением с помощью леммы 10.3: значение ψ одинаково для обеих точек, и значение ϕ во второй точке больше либо равно значению ϕ в первой точке.

Полосы. Теперь мы приведем пример, показывающий, что корни системы с матрицей Маколея могут вести себя достаточно сложно. Более конкретно, мы опишем решение с большими разрывами, то есть решение, в котором присутствуют сколь угодно большие разрывы между значениями в соседних точках. Для этого примера нам также хватит $n = 2$ переменных.

Рассмотрим многочлен f с

$$G(f) = \{(0,0,0), (0,1,-1), (0,2,0),$$
$$(1,0,0), (1,1,-1), (1,2,0)\}.$$

Выпуклая оболочка этих точек является призмой.

Рассмотрим множество точек, описываемых следующей функцией $\phi\colon \mathbb{Z}^2 \to \mathbb{R}$:

$$\phi(x,y) = \begin{cases} y, & \text{если } \lfloor x/2 \rfloor \text{ четно;} \\ -y, & \text{если } \lfloor x/2 \rfloor \text{ нечетно.} \end{cases}$$

Нетрудно видеть, что график ϕ сингулярен к выпуклым оболочкам всех сдвигов $G(f)$. Действительно, рассмотрим произвольный сдвиг $G(f)$ на вектор (a,b) и обозначим соответствующую функцию через ψ. Ее область определения — это множество $D = \{(a,b), (a,b+1), (a,b+2), (a+1,b), (a+1,b+1), (a+1,b+2)\}$. Рассмотрим сингулярную точку $\vec{\alpha}$ в $\mathsf{Sing}(\phi,\psi)$. Без ограничения общности предположим, что ее координата по оси x равна a. Тогда оказывается, что одна из соседних точек в D с координатой по оси x, равной a, также является сингулярной. Это можно проверить прямым вычислением с помощью леммы 10.3.

Таким образом, вектор $\{\phi(I)\}_{|I|\leqslant N}$ является решением системы с матрицей Маколея, соответствующей f. С другой стороны, заметим, что разрывы между значениями ϕ в соседних точках в $\mathbb{Z}^2$ могут быть сколь угодно большими.

10.2.5 Теоремы о нулях в двойственной форме над $\mathbb{R}_\infty$

В этом разделе мы докажем следующую более точную версию теоремы 10.2(ii).

Теорема 10.6. *Над полукольцом $\mathbb{R}_\infty$ система мин-плюс многочленов $F = \{f_1, \ldots, f_k\}$ степени не больше d от n переменных имеет корень тогда и только тогда, когда неоднородная линейная система с матрицей Маколея M_N для*

$$N = 2(n+2)^2 k (4d)^{\min(n,k)+2}$$

имеет корень.

Доказательство. Пусть дана система мин-плюс многочленов F, рассмотрим соответствующую неоднородную линейную систему с матрицей Маколея $M_N \odot (0, \vec{y})$. Мы уже доказали теорему в одну сторону: если F имеет корень, то и $M_N \odot (0, \vec{y})$ имеет корень.

В обратную сторону, предположим, что $\vec{a}$ — решение неоднородной линейной системы с матрицей M_N. Это значит, что в $\vec{a}$ координата, соответствующая постоянному моному, конечна. Если для объемлющего многогранника P_0, построенного в разделе 10.2.2, существует $\vec{x} \in \mathbb{Z}^n$, такой что $\vec{x} \in \mathsf{Dom}\, \beta_{P_0} \cap \mathsf{Dom}\, \phi_{\vec{a}}$, то мы можем сразу воспользоваться леммой 10.12(ii). Но изначально мы знаем лишь, что $\vec{0} \in \mathsf{Dom}\, \phi_{\vec{a}}$, при этом возможно, что $\vec{0} \notin \mathsf{Dom}\, \beta_{P_0}$ (и может не быть сдвига $P_0 + \vec{\alpha}$ многогранника P_0, не выходящего за пределы $\mathbb{Z}^n_+$, такого что $\vec{0} \in \mathsf{Dom}\, \beta_{P_0+\vec{\alpha}}$). Ниже мы описываем, как решать эту проблему.

Рассмотрим столбец M_N, соответствующий постоянному моному. Если он не содержит конечных ячеек, то неоднородная система с матрицей Маколея имеет бесконечный корень. С другой стороны, система многочленов F также имеет бесконечный корень. Действительно, в этом случае ни один многочлен системы не содержит конечного свободного члена. Таким образом, этот случай простой, и мы дальше предполагаем, что столбец M_N, соответствующий постоянному моному, содержит конечную ячейку. Это означает, что в F есть многочлен с конечным свободный членом. Для простоты в обозначений будем считать, что это многочлен f_1.

Теперь на основе системы многочленов F мы построим систему многочленов F' со следующими свойствами:

1. каждый многочлен в F' является (мин-плюс) алгебраической комбинацией многочленов в F;

2. каждый многочлен в F' имеет конечный свободный член;

3. F' имеет корень тогда и только тогда, когда F имеет корень;

4. число K многочленов в F' не превышает $(n+2)k$, и максимальная степень d' многочленов в F' не превышает $2(4d)^{\min(n,k)+2}$.

Утверждение. *Если семейство многочленов F' с перечисленными выше свойствами существует, то теорема 10.6 верна.*

Доказательство утверждения. Нам достаточно доказать теорему 10.6 лишь в обратную сторону. Рассмотрим корень $\vec{a}$ системы $M_N \odot (0, \vec{y})$. Рассмотрим неоднородную систему с матрицей M'_N, соответствующую F'. Поскольку все многочлены в F' являются мин-плюс алгебраической комбинацией многочленов из F, строки M'_N являются мин-плюс линейными комбинациями строк M_N. Следовательно, $\vec{a}$ является решением $M'_N \odot (0, \vec{y})$. Рассмотрим расширенные многогранники Ньютона $P'_1, P'_2 \ldots, P'_K$ для многочленов из системы F' и рассмотрим объемлющий многогранник P'_0 (см. раздел 10.2.2). Заметим, что для всякой функции $f \in F'$ верно, что $\vec{0} \in \mathsf{Dom}\, \phi_f$. Следовательно, то же самое верно и для соответствующих многогранников, а значит, и для объемлющего многогранника P'_0. Заметим, что $N = 2(n+2)^2 k(4d)^{\min(n,k)+2} = (n+2)Kd'$. Следовательно, мы можем воспользоваться леммой 10.12(ii) и получить корень $\vec{b} = (-b_1, \ldots, -b_n) \in \mathbb{R}^n$ для F'. Это в свою очередь влечет, что и у F есть корень. ■

Таким образом, чтобы закончить доказательство теоремы 10.6, нам осталось построить систему многочленов F' и доказать необходимые свойства.

Идея конструкции F' состоит в том, чтобы встроить f_1 во все многочлены f_i в F для того, чтобы гарантировать, что их постоянный член конечен. То есть, каждый многочлен в F' будет равен (мин-плюс) сумме f_1 и алгебраической комбинации других многочленов из F. В частности, расширенный многогранник Ньютона многочлена в F' будет выпуклой оболочкой объединения P_1 с некоторыми сдвигами других многогранников из $P_2, \ldots, P_k$. Однако, мы

хотим избежать появления новых корней у системы F'. Если некоторая грань P_1 в результате окажется гранью всех многогранников для многочленов в F', это породит новый корень для F'. Так что нам нужно строить новые многогранники P'_i так, чтобы как можно большее число вершин P_1 оказывались во внутренности P'_i, и благодаря этому, число граней P_1 в многогранниках P'_i было как можно меньше. Потребность в избегании новых корней в F' добавляет много технических трудностей.

Теперь мы перейдем к построению F'.

Ниже нам потребуется следующая величина:

$$\Delta = \max_{1\leqslant i_1,i_2\leqslant k} \max_{\vec{x}\in \mathsf{Dom}\,\phi_{i_1},\ \vec{y}\in \mathsf{Dom}\,\phi_{i_2}} |\phi_{i_1}(\vec{x}) - \phi_{i_2}(\vec{y})|. \tag{10.2}$$

Неформально, она измеряет максимальную совокупную вариацию ϕ-функций для системы F.

Мы также можем предполагать, что $\min_I \phi_i(I) = 0$ для всех i, поскольку прибавление (в классическом смысле) константы ко всем коэффициентам многочлена не влияет на сингулярность.

Чтобы построить F' мы сначала для всех $i = 2, \ldots, k$ и $j = 1, \ldots, n$ определим многочлены следующего вида:

$$g_{ij} = (-C) \odot x_j^{\alpha} \odot f_i.$$

Здесь параметры C и α можно зафиксировать следующим образом:

$$C = 3\Delta(4d)^{2\min(n,k)+2}, \quad \alpha = (4d)^{\min(n,k)+2}.$$

Далее, для всех $i > 1$ мы определим

$$f'_i = f_1 \oplus g_{i1} \oplus g_{i2} \oplus \ldots \oplus g_{in}. \tag{10.3}$$

Также для всех $i = 2, \ldots, k$ и $j = 1, \ldots, n$ мы вводим многочлен

$$f'_{ij} = f_1 \oplus g_{i1} \oplus g_{i2} \oplus \ldots \oplus g_{i,j-1} \oplus (-1) \odot g_{ij} \oplus g_{i,j+1} \oplus \ldots \oplus g_{in}.$$

То есть, разница между f_i' и f_{ij}' состоит в том, что в последнем коэффициент при $x_j^\alpha \odot f_i$ равен $(-C-1)$, а не $-C$. Мы полагаем

$$F' = \{f_1\} \cup \{f_i' \mid i = 2, \dots, k\} \cup \{f_{ij}' \mid i = 2, \dots, k,\ j = 1, \dots, n\}.$$

Таким образом, F' состоит из $K = (n+1)(k-1)+1 \leqslant (n+2)k$ многочленов степени не больше $\alpha + d \leqslant 2(4d)^{\min(n,k)+2}$. Мы обозначаем расширенный многогранник Ньютона функции f_i' через P_i', а функцию $\phi_{f_i'}$ — через ϕ_i'. Аналогично, для функции f_{ij}' мы обозначаем ее расширенный многогранник Ньютона через P_{ij}', а функцию $\phi_{f_{ij}'}$ — через ϕ_{ij}'.

Мин-плюс слагаемые в сумме (10.3) мы будем называть ниже *компонентами* многочлена f_i'. Мы будем специально выделять f_1-компоненту. Все остальные компоненты мы будем называть f_i-компонентами. Когда нам потребуется их различать, компоненту g_{ij} мы будем называть j-й компонентой f_i'.

Все свойства F' ясны непосредственно из конструкции, кроме свойства 3. Более того, в одну сторону доказательство свойства 3 простое: поскольку F' состоит из алгебраических комбинацией многочленов из F, всякий корень F также является корнем F'. Таким образом, нам осталось доказать следующую лемму.

Лемма 10.13. *Если у системы F' есть корень, то и у системы F есть корень.*

Доказательство этой леммы имеет геометрическую интуицию, но эту интуицию непросто увидеть за техническими деталями. Так что прежде чем переходить к доказательству, мы объясним интуицию для случая $n = 2$ и $k = 3$. После этого мы дадим формальное доказательство в общем случае.

Неформальное доказательство для $n = 2$ и $k = 3$. Неформально удобно думать о константах C и α как об очень больших параметрах, которые мы зафиксируем позже. В формальном доказательстве леммы 10.13 мы покажем, что значения C и α, указанные выше, годятся.

Полезно посмотреть на расширенный многогранник Ньютона P_2', соответствующий функции f_2'. Его построение можно разбить на два шага: сначала мы объединяем график ϕ_1 и две копии графика ϕ_2, сдвинутые далеко вдоль каждой из осей x_1 и x_2, а также далеко вниз вдоль вертикальной оси, а затем мы берем расширенный многогранник Ньютона получившегося объединения. Идея конструкции f_2' состоит в том, что все точки многогранника P_1 (соответствующего ϕ_1), кроме, быть может, точек на осях x_1 и x_2, лежат во внутренности многогранника P_2'.

Мы объясним смысл добавления многочленов $f_{21}', f_{22}', f_{31}', f_{32}'$ в систему F', когда они нам понадобятся.

Предположим, что у системы F' есть корень $\vec{b} = (-b_1, -b_2)$. Заметим, что поскольку каждый многочлен в F' имеет конечный свободный член, значение каждого многочлена в F' конечно на всяком входе. Так что мы можем предполагать, что $\vec{b} \in \mathbb{R}^2$. Если это не так, просто заменим бесконечные координаты $\vec{b}$ на достаточно большие конечные значения. Напомним, что корень соответствует плоскости $\chi_{\vec{b}}(\vec{x}) = b_1x_1 + b_2x_2$ (в 3-мерном пространстве), сингулярной к ϕ_f для всех многочленов $f \in F'$. Естественной первой попыткой было бы попробовать доказать, что эта гиперплоскость также сингулярна к функциям ϕ_1, ϕ_2, ϕ_3, соответствующим многочленам f_1, f_2, f_3. Мы уже знаем, что она сингулярна к ϕ_1, поскольку $f_1 \in F'$. Чтобы доказать, что она сингулярна к ϕ_2 и ϕ_3, посмотрим подробнее на многочлены f_2' и f_3'. Без ограничения общности рассмотрим f_2'.

Мы знаем, что гиперплоскость $\chi_{\vec{b}}$ имеет не меньше двух сингулярных точек с ϕ_2'. Заметим, что сингулярные точки можно выбрать среди вершин P_2'. Однако, если сингулярные точки принадлежат различным компонентам f_2', это не говорит нам ничего о сингулярности $\chi_{\vec{b}}$ к какому-либо ϕ_i. Таким образом, мы хотим доказать, что есть две сингулярные точки в одной компоненте f_2'. Предположим, что есть не больше одной сингулярной точки в каждой компоненте f_2'. Заметим, что если есть хотя бы одна сингулярная точка в f_1-компоненте,

то в ней есть две сингулярные точки, поскольку гиперплоскость $\chi_{\vec{b}}$ сингулярна к ϕ_1. Случай, когда гиперплоскость $\chi_{\vec{b}}$ имеет только одну сингулярную точку в одной из f_2-компонент, это ровно тот случай, для которого нам нужны многочлены f'_{21}, f'_{22}. Действительно, нетрудно видеть, что в этом случае один из этих многочленов имеет всего одну сингулярную точку (суммарно во всех компонентах), а значит, гиперплоскость не сингулярна ϕ'_{21} или ϕ'_{22}.

Таким образом, мы получили, что каждый из многочленов f'_2 и f'_3 имеет не меньше двух сингулярных точек в одной и той же компоненте. Если это f_2-компонента и f_3-компонента соответственно, то доказательство на этом завершается: ясно, что гиперплоскость сингулярна к ϕ_2 и ϕ_3. Таким образом, остается разобрать случай, когда один из многочленов (или оба) имеют две точки сингулярности в f_1-компоненте.

Здесь мы сталкиваемся с серьезным препятствием. Например, предположим, что $\mathsf{Dom}\,\phi_2$ и $\mathsf{Dom}\,\phi_3$ не пересекаются с $\{(t, 0) \mid t \in \mathbb{R}\}$ — множеством точек на оси x_1. Тогда гиперплоскость, имеющая две сингулярные точки с ϕ_1 на оси x_1 и убывающая очень быстро вдоль оси x_2, задает корень системы F', но не обязательно системы F.

Таким образом, не всегда верно, что корень F' является корнем F. Однако, в примере выше мы можем заменить b_2 на $b'_2 = -\infty$ и получить корень $\vec{b'}$ для F.

Оказывается, что этого приема в сочетании с некоторыми дополнительными усилиями достаточно для завершения доказательства. Действительно, пусть сингулярные точки гиперплоскости $\chi_{\vec{b}}$ к, например, ϕ'_2 лежат в f_1-компоненте. Тогда нетрудно видеть, что все эти сингулярные точки лежат либо на оси x_1, либо на оси x_2. Действительно, для всякой точки $\vec{a} \in \mathsf{Dom}\,\phi'_2$, у которой обе координаты положительны, точка $(\vec{a}, \phi'_2(\vec{a})) \in \mathbb{R}^3$ лежит в P_1, а значит, во внутренности P'_2, благодаря свойствам конструкции ϕ'_2. Таким образом, $\vec{a}$ не является сингулярной точкой. Если же, с другой стороны, существует сингулярная точка $\vec{a}$ с положительной x_1-координатой, и существует другая сингулярная точка

$\vec{a}'$ с положительной x_2-координатой, тогда точка $((\vec{a}+\vec{a'})/2, (\phi_1(\vec{a})+\phi_1(\vec{a'}))/2)$ лежит в P_1 в силу его выпуклости, а значит лежит во внутренности P'_2, что противоречит сингулярности $\vec{a}$ и $\vec{a}'$. Следовательно, этот случай также невозможен, и все сингулярные точки лежат на одной из осей.

Без ограничения общности предположим, что все сингулярные точки к f'_2 лежат на оси x_1. Поскольку хотя бы две сингулярные точки на этой прямой лежат в f_1-компоненте, b_1 не может быть слишком большим или слишком маленьким, или более формально, его абсолютное значение ограничено Δ (а значит, не зависит от C и α). Поскольку мы можем зафиксировать C сколь угодно большим, это в частности означает, что $\mathsf{Dom}(\phi_2)$ не пересекается с осью x_1. Иначе сингулярная точка гиперплоскости $\chi_{\vec{b}}$ с ϕ'_2 была бы в 1-компоненте, а не в f_1-компоненте. Таким образом, чтобы получить корень системы $\{f_1, f_2\}$, мы можем просто положить $b'_2 = -\infty$ и получить новый потенциальный корень $\vec{b'} = (-b_1, -b'_2)$ для F.

Отметим, что в данный момент мы доказали теорему для случая $n = 2$ и $k = 2$. Но нам нужно еще одно наблюдение, чтобы завершить рассуждение для случая $k = 3$.

Рассмотрим оставшийся многочлен f'_3. Если область определения ϕ_3 также не пересекается с осью x_1, то $\vec{b'}$ также является корнем f'_3.

Так что мы можем предполагать, что есть точка $\vec{y}$ в $\mathsf{Dom}(\phi_3)$, лежащая на оси x_1. Тогда аналогично случаю ϕ'_2, сингулярные точки ϕ'_3 лежат не в f_1-компоненте. Следовательно, они лежат в какой-то из f_3-компонент, и следовательно, $\chi_{\vec{b}}$ сингулярна к самой ϕ_3. Но мы положили $b'_2 = -\infty$, и сингулярность может не перенестись на $\vec{b'}$. Это произойдет, если есть только одна сингулярная точка в $\mathsf{Sing}(\chi_{\vec{b}}, \phi_3)$ на оси x_1. Но тогда есть другая сингулярная точка $\vec{z}$ в $\mathsf{Sing}(\chi_{\vec{b}}, \phi_3)$, лежащая не на оси x_1.

Рассмотрим обе точки $\vec{y}, \vec{z} \in \mathbb{Z}^2$ на двумерной решетке. Чтобы попасть из точки $\vec{y}$ в точку $\vec{z}$ в этой решетке, нам нужно сделать несколько (не больше d) шагов вдоль оси x_1 в положительном или отрицательном направлении, а также

хотя бы один шаг в положительном направлении вдоль оси x_2. Вдоль этого пути значение ϕ_3, а значит, и $\chi_{\vec{b}}$ не может уменьшиться больше, чем на Δ. Действительно, поскольку $\vec{z}$ — сингулярная точка, разность значений $\chi_{\vec{b}}$ ограничена снизу разностью значений ϕ_3 в тех же точках. Поскольку абсолютное значение b_1 также ограничено, из этого мы можем заключить, что b_2 ограничено снизу некоторой величиной, зависящей только от F.

Теперь, выбирая C достаточно большим, мы можем получить противоречие с тем, что сингулярные точки $\phi_{f_2'}$ лежат в f_1-компоненте: и b_1, и b_2 не слишком маленькие, и если мы поместим f_2-компоненты достаточно низко, сингулярные точки будет лежать в этих компонентах.

Это доказательство (с некоторыми дополнительными техническими приемами) переносится и на общий случай.

Далее мы переходим к формальному доказательству леммы 10.13.

Доказательство леммы 10.13. План доказательства состоит в том, чтобы рассмотреть корень F' и заменить часть его координат на бесконечность. Ниже мы описываем, как правильно выбрать множество этих координат. Рассуждение будет достаточно прямым: мы будем сохранять конечными только те координаты, для которых у нас есть явные причины сохранять их конечными, а остальные заменим на бесконечность.

Рассмотрим корень $\vec{b} = (-b_1, \dots, -b_n) \in \mathbb{R}^n$ системы F'. Мы можем предполагать, что корень лежит в $\mathbb{R}^n$ по тем же соображениям, что и в неформальном доказательстве. Как обсуждалось в разделе 10.2.1, это означает, что гиперплоскость $\chi_{\vec{b}}(\vec{x}) = \sum_i b_i x_i$ сингулярна ко всем ϕ_f для $f \in F'$.

Заметим, что для всякого многочлена f_i' существуют две сингулярные точки в одной и той же компоненте. Действительно, если это не так, рассмотрим j-компоненту с одной сингулярной точкой и рассмотрим многочлен f_{ij}'. У него есть только одна сингулярная точка, а это дает противоречие (такое же рас-

суждение работает и для f_1-компоненты: в этом случае мы можем рассмотреть многочлен f_1).

Ниже для множества $T \subseteq \mathbb{R}^n$ и для множества $S \subseteq \{1, \ldots, n\}$ мы обозначаем через $T\big|_S$ множество точек $\vec{x} \in T$, таких что $x_j = 0$ для всех $j \notin S$.

Мы определим последовательность множеств следующей итеративной процедурой. Сначала рассмотрим множество $\mathsf{Sing}(\chi_{\vec{b}}, \phi_1)$ сингулярных точек для $\chi_{\vec{b}}$ и ϕ_1. Положим $j \in S_0$ тогда и только тогда, когда существует $\vec{x} \in \mathsf{Sing}(\chi_{\vec{b}}, \phi_1)$, такой что $x_j \neq 0$. Предположим, что мы определили S_l рекурсивно по $l \geqslant 0$. Если есть многочлен $f_i \in F$, такой что $\left|\mathsf{Sing}(\chi_{\vec{b}}, \phi_i)\right| > \left|\mathsf{Sing}(\chi_{\vec{b}}, \phi_i)\big|_{S_l}\right|$ и $\mathsf{Dom}(\phi_i)\big|_{S_l} \neq \emptyset$, то мы определяем S_{l+1}, полагая $S_l \subseteq S_{l+1}$ и $j \in S_{l+1} \setminus S_l$ тогда и только тогда, когда существует $\vec{x} \in \mathsf{Sing}(\chi_{\vec{b}}, \phi_i)$, такой что $x_j \neq 0$. Если такого f_i нет, то процесс заканчивается.

В результате этой процедуры мы получаем последовательность $S_0, S_1, \ldots S_r$ и соответствующую последовательность многочленов $g_1, g_2, \ldots, g_r$, где для каждого l верно $g_l \in F$. Для удобства введем обозначение $g_0 = f_1$. Заметим, что $r \leqslant k$, поскольку каждый многочлен в F может встретиться в последовательности не больше одного раза. Также $r \leqslant n$, поскольку каждое S_l является подмножеством $\{1, \ldots, n\}$ и каждое следующее множество больше предыдущего. Следовательно, $r \leqslant \min(n, k)$.

Мы можем доказать следующую оценку на координаты $\vec{b}$, лежащие в S_r.

Утверждение. *Для всех $l = 0, \ldots, r$, если существует $j \in S_l$, такое что $b_j \leqslant -2\Delta(4d)^l$, то существует $j' \in S_l$, такое что $b_{j'} \geqslant |b_j|/(4d)^{l+1}$.*

Неформально, если есть очень маленькая координата b_j, то есть и довольно большая координата $b_{j'}$.

Доказательство. Доказательство проходит индукцией по l.

Для случая S_0 рассмотрим координату j, такую что $b_j \leqslant -2\Delta$, и рассмотрим $\vec{x} \in \mathsf{Sing}(\chi_{\vec{b}}, \phi_1)$, такой что $x_j \neq 0$ (такой $\vec{x}$ существует по определению S_0). Рассмотрим $\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{0}) = \sum_p x_p b_p$. Поскольку $\vec{x} \in \mathsf{Sing}(\chi_{\vec{b}}, \phi_1)$, по лемме 10.3

$\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{0}) \geqslant \phi_1(\vec{x}) - \phi_1(\vec{0}) \geqslant -\Delta$. Заметим, что $x_j > 0$ (а следовательно, $x_j \geqslant 1$) и для всех p верно, что $x_p \geqslant 0$. Следовательно,

$$\sum_{p \neq j} x_p b_p \geqslant -x_j b_j - \Delta \geqslant -b_j - \Delta \geqslant -b_j/2.$$

С другой стороны, заметим, что

$$\sum_{p \neq j} x_p b_p \leqslant \max_{p \neq j} b_p \sum_{p \neq j} x_p \leqslant d \max_{p \neq j} b_p.$$

Таким образом, существует j', такое что $b_{j'} = \max_{p \neq j} b_p \geqslant -b_j/2d$.

Для шага индукции рассмотрим $j \in S_l$, такое что $b_j \leqslant -2\Delta(4d)^l$. Если $j \in S_{l-1}$, утверждение следует из предположения индукции. Предположим, что $j \notin S_{l-1}$. Рассмотрим многочлен g_l. По его определению, мы имеем следующее.

1. Существует $\vec{y} \in \mathsf{Dom}(\phi_{g_l})\big|_{S_{l-1}}$. В частности, $y_j = 0$.

2. Существует сингулярная точка $\vec{x} \in \mathsf{Sing}(\chi_{\vec{b}}, \phi_{g_l})$, такая что $x_j \neq 0$.

Рассмотрим $\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{y}) = \sum_p (x_p - y_p) b_p$. В силу сингулярности $\vec{x}$ по лемме 10.3 верно $\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{y}) \geqslant \phi_{g_l}(\vec{x}) - \phi_{g_l}(\vec{y}) \geqslant -\Delta$. Аналогично базе индукции

$$\sum_{p \neq j} (x_p - y_p) b_p \geqslant -(x_j - y_j) b_j - \Delta \geqslant -b_j - \Delta \geqslant -b_j/2.$$

Разобьем сумму слева на две части:

$$\sum_{p \neq j, p \in S_{l-1}} (x_p - y_p) b_p + \sum_{p \neq j, p \notin S_{l-1}} (x_p - y_p) b_p \geqslant -b_j/2.$$

Заметим, что во второй сумме $(x_p - y_p)$ неотрицательны, поскольку $y_p = 0$. В силу того, что

$$\sum_{p \neq j} |x_p - y_p| \leqslant 2d,$$

либо существует $p \notin S_{l-1}$, такое что $b_p \geqslant -b_j/4d$, либо существует $p \in S_{l-1}$, такое что $|b_p| \geqslant -b_j/4d$. В первом случае доказательство завершается сразу. Во втором случае доказательство завершается в силу предположения индукции. ■

Чтобы получить новый корень, мы фиксируем все координаты корня, не лежащие в S_r, равными ∞, то есть мы полагаем $b'_j = -\infty$, если $j \notin S_r$, и $b'_j = b_j$, если $j \in S_r$. Обозначим результат через $\vec{b}' = (-b'_1, \dots, -b'_n) \in \mathbb{R}^n_\infty$.

Мы утверждаем, что $\vec{b}'$ является корнем системы F.

Действительно, предположим обратное: пусть существует многочлен $f_i \in F$, такой что есть только одна точка $\vec{z} \in \mathsf{Sing}(\chi_{\vec{b}'}, \phi_i)$. Ясно, что $\vec{z} \in \mathbb{Z}^n\big|_{S_r}$. Более того, ни одна другая точка изначальной гиперплоскости $\chi_{\vec{b}}$ не может быть сингулярной к ϕ_i. Действительно, другая сингулярная точка может лежать только вне $\mathbb{Z}^n\big|_{S_r}$, и если она существует, то по нашей конструкции мы должны были бы добавить дополнительные координаты в S_r. Таким образом, существует лишь одна сингулярная точка в $\mathsf{Sing}(\chi_{\vec{b}}, \phi_i)$, а значит, сингулярные точки $\chi_{\vec{b}}$ к $\phi_{f'_i}$ лежат в f_1-компоненте. Пусть $\vec{y} \in \mathsf{Sing}(\chi_{\vec{b}}, \phi_{f'_i})$ — одна из этих сингулярных точек. Заметим, что по определению S_0 верно, что $\vec{y} \in \mathbb{Z}^n\big|_{S_0} \subseteq \mathbb{Z}^n\big|_{S_r}$. Дальше мы придем к противоречию.

Пусть $Min = \min_{j \in S_r} b_j$ и $Max = \max_{j \in S_r} b_j$. Рассмотрим j и j', такие что $b_j = Min$ и $b_{j'} = Max$. Рассмотрим j'-компоненту f'_i и положим $\vec{x}$ равным сдвигу $\vec{z}$ в эту компоненту, то есть $\vec{x} = \vec{z} + \alpha \cdot \vec{e_{j'}}$. Поскольку $\vec{z} \in \mathbb{Z}^n\big|_{S_r}$ и $j' \in S_r$, верно, что $\vec{x} \in \mathbb{Z}^n\big|_{S_r}$.

Наша цель — доказать неравенство $\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{y}) > \phi_{f'_i}(\vec{x}) - \phi_{f'_i}(\vec{y})$, которое противоречит лемме 10.3, поскольку $\vec{y} \in \mathsf{Sing}(\chi_{\vec{b}}, \phi_{f'_i})$.

Заметим, что

$$\phi_{f'_i}(\vec{x}) - \phi_{f'_i}(\vec{y}) = \phi_{f'_i}(\vec{z} + \alpha \cdot \vec{e_{j'}}) - \phi_1(\vec{y}) = (\phi_i(\vec{z}) - C) - \phi_1(\vec{y}) \leqslant -C + \Delta,$$

где второе равенство следует из определения f'_i (10.3), а последнее неравенство следует из определения Δ (10.2). Следовательно, нам достаточно доказать, что $\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{y}) > -C + \Delta$.

Теперь заметим, что

$$x_{j'} - y_{j'} = x_{j'} - z_{j'} + z_{j'} - y_{j'} \geqslant \alpha - 2d$$

и

$$\sum_{p\neq j'} |x_p - y_p| = \sum_{p\neq j'} |z_p - y_p| \leqslant 2d.$$

Рассмотрим сумму

$$\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{y}) =$$
$$\sum_{p\neq j', x_p - y_p > 0} (x_p - y_p)b_p + \sum_{p\neq j', x_p - y_p \leqslant 0} (x_p - y_p)b_p + (x_{j'} - y_{j'})b_{j'} \geqslant$$
$$Min \cdot \sum_{p\neq j', x_p - y_p > 0} (x_p - y_p) + Max \cdot \sum_{p\neq j', x_p - y_p \leqslant 0} (x_p - y_p) + Max \cdot (x_{j'} - y_{j'}).$$

Если $Max \leqslant 0$, то по утверждению выше мы получаем $Min \geqslant -2\Delta(4d)^r$, и следовательно, $Max \geqslant -2\Delta(4d)^r$. В этом случае мы получаем

$$\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{y}) \geqslant$$
$$-2d2\Delta(4d)^r + 0 - 2\Delta(4d)^r(\alpha - 2d) = -\alpha 2\Delta(4d)^r.$$

Если $Max \geqslant 0$, мы получаем

$$\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{y}) \geqslant$$
$$Min \cdot \sum_{p\neq j', x_p - y_p > 0} (x_p - y_p) - Max \cdot 2d + Max \cdot (\alpha - 2d) =$$
$$Min \cdot \sum_{p\neq j', x_p - y_p > 0} (x_p - y_p) + Max \cdot (\alpha - 4d).$$

Если $Min \geqslant -2\Delta(4d)^r$, эта сумма больше, чем $-2\Delta 2d(4d)^r$.

Если $Min \leqslant -2\Delta(4d)^r$, то по утверждению 10.2.5 $Max \geqslant -Min/(4d)^{r+1}$ и мы получаем

$$\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{y}) \geqslant$$
$$2dMin - (\alpha - 4d)Min/(4d)^{r+1} \geqslant 0.$$

Во всех этих случаях $\chi_{\vec{b}}(\vec{x}) - \chi_{\vec{b}}(\vec{y})$ больше, чем $-C + \Delta$, и мы приходим к противоречию с сингулярностью $\vec{y}$.

Это завершает доказательство леммы 10.13, теоремы 10.6, а значит, и теоремы 10.2(ii). ■

Замечание 10.6. *Для случая мин-плюс уравнений конструкция системы F' и ее свойства переносятся с очевидными изменениями (мин-плюс уравнение — это пара мин-плюс многочленов; мы работаем с парой матриц Маколея вместо одной матрицы). Доказательство утверждения 10.2.5 также переносится с очевидными изменениями. Мы не пытаемся перевести на этот случай неформальное доказательство, поскольку это не добавляет интуитивного понимания. Формальное доказательство дается в терминах функций ϕ_i и ϕ'_i, так что оно тоже легко переносится. Единственная разница состоит в том, что вместо свойства «иметь только одну сингулярную точку» мы используем свойство «иметь сингулярные точки только одного цвета» (см. замечание 10.2). В остальном доказательство остается без изменений.*

10.2.6 Нижние оценки

В этом разделе мы приведем примеры, показывающие, что наши оценки на N в теореме 10.2 близки к оптимальным. Мы также покажем аналогичные оценки для теоремы 10.3. Мы перенесем эти оценки на теоремы 10.4 и 10.5 в разделе 10.3.

Нижняя оценка для теоремы 10.2(i). Сначала мы докажем нижнюю оценку для случая $\mathbb{R}$. А именно, для любого $d \geqslant 2$ мы предъявим семейство F из $n+1$ многочлена от n переменных степеней не больше d, такое что F не имеет корня, но соответствующая система с матрицей Маколея $M_{(d-1)(n-1)} \odot \vec{y}$ имеет корень.

Наша конструкция адаптирует известный пример нижней оценки для классической теоремы о нулях, принадлежащий Лазару, Море и Филиппону (см. [25, 64]).

Рассмотрим следующую систему F мин-плюс многочленов

$$\begin{aligned} f_1 &= 0 \oplus 0 \odot x_1, \\ f_{i+1} &= 0 \odot x_i^{\odot d} \oplus 0 \odot x_{i+1}, \text{ для } 1 \leqslant i \leqslant n-1, \\ f_{n+1} &= 0 \oplus 1 \odot x_n. \end{aligned}$$

Нетрудно видеть, что эта система не имеет корней. Действительно, если у нее есть корень, то из f_1 мы получаем, что $x_1 = 0$, далее из f_2 мы получаем, что $x_2 = 0$ и так далее. В конце из f_n мы получим, что $x_n = 0$. Однако, из f_{n+1} мы получаем, что $x_n = -1$, что приводит нас к противоречию.

Таким образом, нам остается доказать, что система с матрицей Маколея $M_{(d-1)(n-1)}$, соответствующей системе F, имеет решение.

Напомним, что столбцы $M_{(d-1)(n-1)}$ соответствуют мономам. Мы сопоставляем неориентированный граф G с матрицей $M_{(d-1)(n-1)}$ следующим естественным образом. Вершины G — это мономы от переменных $x_1, \ldots, x_n$ степени не больше $(d-1)(n-1)$ (или, что то же самое, столбцы $M_{(d-1)(n-1)}$). Мы соединяем два монома ребром, если они встречаются в одном и том же многочлене вида $\vec{x}^I \odot f_i$ для $i \in \{1, \ldots, n\}$. Или другими словами, мы соединяем два монома, если есть строка в $M_{(d-1)(n-1)}$, соответствующая не многочлену f_{n+1}, и такая что ячейки в столбцах, соответствующих этим мономам, обе конечны в этой строке.

Мы припишем веса $w(m)$ мин-плюс мономам m следующим образом. Во-первых, $w(x_i) = d^{i-1}$ для всех $i = 1, \ldots, n$. Во-вторых, для всех мономов m_1 и m_2 от различных переменных мы полагаем $w(m_1 \odot m_2) = w(m_1) + w(m_2)$. Таким образом, если $m = x_1^{\odot a_1} \odot \ldots \odot x_n^{\odot a_n}$, то $w(m) = a_1 + a_2 d + \ldots a_n d^{n-1}$.

Оказывается, что выполняется следующая лемма.

Лемма 10.14. *Если для двух мономов m_1 и m_2 выполняется $w(m_1) \geqslant kd^{n-1}$ и $w(m_2) < kd^{n-1}$ для некоторого целого k, то m_1 и m_2 не достижимы друг из друга в G.*

Доказательство. Заметим, что если два монома соединены ребром, соответствующим одному из многочленов $f_2, \dots, f_n$, то их веса совпадают. Если они соединены ребром, соответствующим многочлену f_1, то их веса отличаются на 1.

Заметим, что для произвольного k всякий моном веса $kd^{n-1}-1$ имеет степень не меньше $(k-1)+(d-1)(n-1)$. Действительно, рассмотрим такой моном $m = x_1^{\odot a_1} \odot \dots \odot x_n^{\odot a_n}$ минимальной степени. Если есть $i = 1, \dots, n-1$, такое что $a_i \geqslant d$, то мы можем заменить a_i на $a_i - d$ и a_{i+1} на $a_{i+1}+1$ и получить другой моном того же веса, но меньшей степени. Следовательно, $(a_1, \dots, a_{n-1})$ соответствует d-ичному представлению числа $kd^{n-1}-1$ по модулю d^{n-1}. А значит, для всех $i = 1, \dots, n-1$ выполняется $a_i = d-1$, и значит, $a_n = k-1$.

Благодаря ограничению на степени мономов в графе G, в нем есть только один моном веса $d^{n-1}-1$, и нет мономов веса $kd^{n-1}-1$ для $k > 1$. Более того, единственный моном веса $d^{n-1}-1$ имеет максимальную степень $(d-1)(n-1)$, а значит, он не соединен ребрами с мономами большей степени.

Лемма вытекает из этих наблюдений. Действительно, если мономы m_1 и m_2 достижимы, то на пути между ними есть ребро, соединяющее мономы веса $kd^{n-1}-1$ и kd^{n-1}. Однако, как мы доказали, это невозможно. ■

Теперь мы готовы предъявить корень системы с матрицей Маколея $M_{(d-1)(n-1)} \odot \vec{y}$. Для монома с весом $kd^{n-1}+s$, где $s < d^{n-1}$, положим соответствующую переменную в $\vec{y}$ равной k. Заметим, что по лемме 10.14, если два монома соединены, то значения соответствующих переменных равны. Таким образом, построенный $\vec{y}$ является корнем многочленов в $M_{(d-1)(n-1)} \odot \vec{y}$, соответствующих многочленам $f_1, \dots, f_n$. Для строк, соответствующих f_{n+1}, он также является корнем, поскольку веса этих мономов отличаются равно на d^{n-1}.

Замечание 10.7. *Пример без труда переносится на случай мин-плюс уравнений (см. теорему 10.3(i)). Действительно, поскольку каждый многочлен содержит лишь два монома, единственный способ подобрать к нему корень — это приравнять эти мономы. Таким образом, достаточно рассмотреть*

следующую систему мин-плюс уравнений F:

$$(0, 0 \odot x_1),$$
$$(0 \odot x_i^{\odot d}, 0 \odot x_{i+1}), \text{ для } 1 \leqslant i \leqslant n-1,$$
$$(0, 1 \odot x_n).$$

Нижняя оценка для теоремы 10.2(ii) Теперь мы докажем нижнюю оценку для случая $\mathbb{R}_\infty$.

Рассмотрим следующую систему F мин-плюс многочленов от переменных $x_1, \ldots, x_n, y$.

$$f_1 = 0 \odot x_1 \odot y \oplus 0,$$
$$f_{i+1} = 0 \odot x_i^{\odot d} \oplus 0 \odot x_{i+1}, \text{ для } i = 1, \ldots, n-1,$$
$$f_{n+1} = 0 \odot x_{n-1}^{\odot d} \oplus 1 \odot x_n.$$

Легко видеть, что эта система не имеет корней. Действительно, предполагая противное, мы можем последовательно доказать, что все координаты корня должны быть конечны, а тогда многочлены f_n и f_{n+1} дают противоречие.

Теперь рассмотрим неоднородную систему с матрицей Маколея: $M_{d^{n-1}-1} \odot (0, \vec{z})$. Мы построим корень для этой системы. Для мин-плюс монома $x_1^{a_1} \ldots x_n^{a_n} y^b$ положим его вес равным

$$a_1 + da_2 + d^2 a_3 + \ldots + d^{n-1} a_n.$$

Отметим, что степень y не учитывается в весе. Рассмотрим все мономы, у которых степень по переменной y совпадает с их весом, и положим соответствующие координаты $\vec{z}$ равными 0. Для всех остальных мономов положим соответствующие координаты $\vec{z}$ равными ∞. Теперь мы докажем, что это действительно корень системы $M_{d^{n-1}-1} \odot (0, \vec{z})$. Рассмотрим граф на координатах $(0, \vec{z})$, в котором две координаты соединены, если соответствующие мономы встречаются в одной строке матрицы $M_{d^{n-1}-1}$. Нетрудно видеть, что все мономы, у которых

координата вектора $(0, \vec{z})$ конечна, составляют компоненту связности графа, содержащую координату, соответствующую постоянному члену. Более того, благодаря ограничениям на размер матрицы, ни один моном в этой компоненте не содержит переменную x_n. Следовательно, наш вектор является корнем для всех строк матрицы Маколея.

Замечание 10.8. *Для случая мин-плюс уравнений (см. теорему 10.3(ii)) заметим, что верно то же наблюдение, что и в замечании 10.7. Так что достаточно рассмотреть систему уравнений*

$$\begin{aligned}
&(0 \odot x_1 \odot y, 0),\\
&(0 \odot x_i^{\odot d}, 0 \odot x_{i+1}),\ \textit{для } i = 1, \ldots, n-1,\\
&(0 \odot x_{n-1}^{\odot d}, 1 \odot x_n).
\end{aligned}$$

10.3 Теоремы о нулях в прямой форме

Теперь мы выведем теоремы о нулях для мин-плюс многочленов и мин-плюс уравнений в прямой форме. Начнем с теоремы для мин-плюс уравнений.

Доказательство теоремы 10.4. Мы используем линейную двойственность для мин-плюс уравнений для доказательства этой теоремы. Начнем со случая полукольца $\mathbb{R}$.

По теореме 10.3(i) система уравнений F не имеет решений над $\mathbb{R}$ тогда и только тогда, когда соответствующая линейная система мин-плюс уравнений с матрицей Маколея

$$Ml_N \odot \vec{y} = Mr_N \odot \vec{y} \tag{10.4}$$

не имеет конечных решений. Эта система эквивалентна системе мин-плюс неравенств

$$\begin{pmatrix} Ml_N \\ Mr_N \end{pmatrix} \odot \vec{y} \leqslant \begin{pmatrix} Mr_N \\ Ml_N \end{pmatrix} \odot \vec{y}.$$

Действительно, мы просто заменили каждое уравнение $\vec{a} \odot \vec{y} = \vec{b} \odot \vec{y}$ в (10.4) на пару неравенств $\vec{a} \odot \vec{y} \leqslant \vec{b} \odot \vec{y}$ и $\vec{a} \odot \vec{y} \geqslant \vec{b} \odot \vec{y}$.

По следствию 9.13 эта система не имеет конечных решений тогда и только тогда, когда двойственная система

$$\begin{pmatrix} Mr_N^T & Ml_N^T \end{pmatrix} \odot \begin{pmatrix} \vec{z_1} \\ \vec{z_2} \end{pmatrix} < \begin{pmatrix} Ml_N^T & Mr_N^T \end{pmatrix} \odot \begin{pmatrix} \vec{z_1} \\ \vec{z_2} \end{pmatrix} \tag{10.5}$$

имеет решение $(\vec{y}, \vec{z}) \neq (\infty, \ldots, \infty)$ (напомним, что мы разрешаем обеим частям быть равными бесконечности в некоторых строках).

Эту систему можно проинтерпретировать в терминах многочленов. То есть, мы утверждаем, что линейная система (10.5) имеет решение тогда и только тогда, когда существует алгебраическая комбинация (f, g) мин-плюс уравнений из F, такая что для каждого монома его коэффициент в f меньше его коэффициента в g. Действительно, заметим, что столбцы матриц в (10.5) соответствуют уравнениям из F, домноженным на некоторые мономы $\vec{x}^J$, а строки соответствуют некоторым мономам $\vec{x}^I$. Обе части в (10.5) можно рассматривать как мин-плюс сумму столбцов матриц. Каждый столбец матрицы состоит из коэффициентов одного из многочленов в F, домноженного на моном. Мин-плюс сумма этих столбцов, таким образом, состоит из коэффициентов алгебраической комбинации многочленов из F. Таким образом, решение системы (10.5) соответствует алгебраической комбинации многочленов из F, такой что каждый коэффициент алгебраической комбинации в левой части меньше соответствующего коэффициента алгебраической комбинации в правой части. То, что мы допускаем, что обе части равны бесконечности в некоторых строках, соответствует тому, что некоторые мономы могут не присутствовать в суммах. То, что мы допускаем бесконечные координаты в решении (10.5), соответствует тому, что мы не обязаны использовать все столбцы в мин-плюс сумме, то есть мы не обязаны использовать все многочлены вида $(\vec{x}^I \odot f_j, \vec{x}^I \odot g_j)$ в алгебраической комбинации.

Доказательство второй части теоремы почти такое же. Единственное различие состоит в том, что здесь нам нужно использовать неоднородные системы с матрицами Маколея, которые после применения леммы 9.12 дают алгебраическую комбинацию многочленов с постоянным свободным членом. ■

Теперь перейдем к прямой теореме о нулях для мин-плюс многочленов.

Доказательство теоремы 10.5. По теореме 10.2(i) система многочленов F не имеет решения над $\mathbb{R}$ тогда и только тогда, когда соответствующая система с матрицей Маколея

$$M_N \odot \vec{y}$$

не имеет конечного решения.

По следствию 9.15 это равносильно условию, что существует $\vec{z} \neq (\infty, \ldots, \infty)$ в $\mathbb{R}^n_\infty$, такой что в каждой строке

$$M_N^T \odot \vec{z}$$

минимум достигается лишь один раз или равен ∞, и для любых двух строк конечные минимумы достигаются в разных столбцах. Напомним, что каждый столбец в M_N^T соответствует одному из многочленов $\vec{x}^J \odot f_j$, а строки соответствуют мономам $\vec{x}^I$ в этих многочленах. Таким образом, $\vec{z}$ соответствует алгебраической комбинации многочленов из F, а указанное выше свойство $\vec{z}$ эквивалентно сингулярности этой алгебраической комбинации.

Доказательство для случая $\mathbb{R}_\infty$ полностью аналогично. ■

Нижние оценки на N в теоремах 10.4 и 10.5 можно доказать аналогично рассуждениям выше, рассмотрев системы многочленов и уравнений, построенные в разделе 10.2.6. Там было доказано, что для этих систем многочленов и уравнений соответствующие линейные системы с матрицами Маколея определенного размера имеют решения. Используя линейную двойственность для систем мин-плюс уравнений и многочленов, и интерпретируя результаты в терминах многочленов по аналогии с доказательствами выше, мы можем доказать,

что эти системы многочленов и уравнений дают нижние оценки и для прямых теорем о нулях.

Список работ, в которых опубликованы основные результаты диссертации

(1) K. A. Hansen, V. V. Podolskii, “Exact threshold circuits”, Proc. of 25th Annual IEEE Conference on Computational Complexity (CCC), IEEE Computer Soc., Los Alamitos, CA, 2010, 270–279.

(2) V. V. Podolskii, “Exponential lower bound for bounded depth circuits with few threshold gates”, Inform. Process. Lett., 112:7 (2012), 267–271.

(3) V. V. Podolskii, “Lower bound on weights of large degree threshold functions”, Log. Methods Comput. Sci., 9:2 (2013), 13-17 pp.

(4) Stanislav Kikot, Roman Kontchakov, Vladimir V. Podolskii, Michael Zakharyaschev, “On the Succinctness of Query Rewriting over OWL 2 QL Ontologies with Bounded Chase”, Proceedings of the 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), ACM Digital Library, 2014, 57:1–57:10.

(5) Meghyn Bienvenu, Stanislav Kikot, Vladimir V. Podolskii, “Tree-like Queries in OWL 2 QL: Succinctness and Complexity Results”, 30th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), IEEE, 2015, 317–328.

(6) K. A. Hansen, V. V. Podolskii, “Polynomial threshold functions and Boolean threshold circuits”, Inform. and Comput., 240 (2015), 56–73.

(7) Dima Grigoriev, Vladimir V. Podolskii, “Complexity of tropical and min-plus linear prevarieties”, Comput. Complexity, 24:1 (2015), 31–64.

(8) Meghyn Bienvenu, Stanislav Kikot, Roman Kontchakov, Vladimir V. Podolskii, Michael Zakharyaschev, “Ontology-mediated queries: Combined complexity and

succinctness of rewritings via circuit complexity", Journal of the ACM, 65:5 (2018), 28 , 51 pp.

(9) Dima Grigoriev, Vladimir V. Podolskii, "Tropical effective primary and dual Nullstellensätze", Discrete Comput. Geom., 59:3 (2018), 507–552.

(10) Alexander S. Kulikov, Vladimir V. Podolskii, "Computing Majority by Constant Depth Majority Circuits with Low Fan-in Gates", Theory Comput. Syst., 63:5 (2019), 956–986.

(11) Dima Grigoriev, Vladimir V. Podolskii, "Tropical Combinatorial Nullstellensatz and sparse polynomials", Found. Comput. Math., 20 (2020), 753–781.

Список литературы

[1] *Ajtai M.* Σ_1^1-Formulae on finite structures // Annals of Pure and Applied Logic. 1983. Vol. 24, N. 1. P. 1 – 48.

[2] *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.

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

[4] *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.

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

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

[7] *Amano K., Maruoka A.* On the Complexity of Depth-2 Circuits with Threshold Gates // Proceedings of the 30th International Symposium on Mathematical Foundations of Computer Science. Vol. 3618 of *Lecture Notes in Computer Science*. Springer, 2005. P. 107–118.

[8] *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.

[9] *Artale A., Calvanese D., Kontchakov R., Zakharyaschev M.* The DL-Lite family and relations // Journal of Artificial Intelligence Research (JAIR). 2009. Vol. 36. P. 1–69.

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

[11] *Aspvall B., Plass M., Tarjan R.* A linear-time algorithm for testing the truth of certain quantified boolean formulas // Information Processing Letters. 1979. Vol. 8, N. 3. P. 121–123.

[12] *Babai L., Hansen K. A., Podolskii V. V., Sun X.* Weights of Exact Threshold Functions // Mathematical Foundations of Computer Science 2010, 35th International Symposium, MFCS 2010, Brno, Czech Republic, August 23-27, 2010. Proceedings / Ed. by P. Hlinený, A. Kucera. Vol. 6281 of *Lecture Notes in Computer Science*. Springer, 2010. P. 66–77.

[13] *Baget J.-F., Leclère M., Mugnier M.-L., Salvat E.* Extending Decidable Cases for Rules with Existential Variables // Proc. of the 21st Int. Joint Conf. on Artificial Intelligence (IJCAI 2009). IJCAI, 2009. P. 677–682.

[14] *Basu S., Bhatnagar N., Gopalan P., Lipton R. J.* Polynomials that Sign Represent Parity and Descartes' Rule of Signs // Computational Complexity. 2008. Vol. 17, N. 3. P. 377–406.

[15] *Basu S., Pollack R., Roy M.-F.* Algorithms in Real Algebraic Geometry. Algorithms and Computation in Mathematics. Springer, 2006.

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

[17] *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.

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

[19] *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.

[20] *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.

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

[22] *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.

[23] *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. 2015. P. 317–328.

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

[25] *Brownawell W. D.* Bounds for the Degrees in the Nullstellensatz // Annals of Mathematics. 1987. Vol. 126, N. 3. P. 577–591.

[26] *Bruno B.* Personal communication. 2017.

[27] *Buhrman H., de Wolf R.* Complexity measures and decision tree complexity: a survey // Theor. Comput. Sci. October 2002. Vol. 288. P. 21–43.

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

[29] *Calì A., Gottlob G., Lukasiewicz T.* A general Datalog-based framework for tractable query answering over ontologies // Journal of Web Semantics. 2012. Vol. 14. P. 57–83.

[30] *Calì A., Gottlob G., Pieris A.* Advanced Processing for Ontological Queries // PVLDB. 2010. Vol. 3, N. 1. P. 554–565.

[31] *Calì A., Gottlob G., Pieris A.* Towards more expressive ontology languages: The query answering problem // Artificial Intelligence. 2012. Vol. 193. P. 87–128.

[32] *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.

[33] *Calvanese D., De Giacomo G., Lembo D., Lenzerini M., Rosati R.* Tractable Reasoning and Efficient Query Answering in Description Logics: The *DL-Lite* Family // Journal of Automated Reasoning. 2007. Vol. 39, N. 3. P. 385–429.

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

[35] *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.

[36] *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.

[37] *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.

[38] *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.

[39] *Cover T. M., Thomas J. A.* Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing). Wiley-Interscience, 2006.

[40] *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.

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

[42] *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.

[43] *Dubhashi D. P., Panconesi A.* Concentration of Measure for the Analysis of Randomized Algorithms. Cambridge University Press, 2009.

[44] *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.

[45] *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.

[46] *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.

[47] *Forster J., Krause M., Lokam S. V., Mubarakzjanov R., Schmitt N., Simon H.-U.* Relations Between Communication Complexity, Linear Arrangements, and Computational Complexity // Proceedings of the 21st Conference on Foundations of Software Technology and Theoretical Computer Science. Vol. 2245 of *Lecture Notes in Computer Science*. Springer, 2001. P. 171–182.

[48] *Furst M., Saxe J. B., Sipser M.* Parity, circuits, and the polynomial-time hierarchy // Mathematical systems theory. Vol. 17, N. 1. P. 13–27.

[49] *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.

[50] *Garey M. R., Johnson D. S.* Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman, 1979.

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

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

[53] *Goldmann M., Karpinski M.* Simulating Threshold Circuits by Majority Circuits // SIAM Journal on Computing. 1998. Vol. 27, N. 1. P. 230–246.

[54] *Goldreich O.* Valiant's Polynomial-Size Monotone Formula for Majority. 2001. Available at `http://www.wisdom.weizmann.ac.il/~oded/PDF/mono-maj.pdf`.

[55] *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.

[56] *Gottlob G., Kikot S., Kontchakov R., Podolskii V. V., Schwentick T., Zakharyaschev M.* The price of query rewriting in ontology-based data access // Artif. Intell. 2014. Vol. 213. P. 42–59.

[57] *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.

[58] *Grigni M., Sipser M.* Monotone Separation of Logarithmic Space from Logarithmic Depth // J. Comput. Syst. Sci. 1995. Vol. 50, N. 3. P. 433–437.

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

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

[61] *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.

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

[63] *Grigoriev D., Podolskii V. V.* Tropical Effective Primary and Dual Nullstellensätze // Discrete & Computational Geometry. 2018. Vol. 59, N. 3. P. 507–552.

[64] *Grigoriev D., Vorobjov N.* Complexity of Null-and Positivstellensatz proofs. // Ann. Pure Appl. Logic. 2001. Vol. 113, N. 1-3. P. 153–160.

[65] *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.

[66] *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.

[67] *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.

[68] *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.

[69] *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.

[70] *Hardy G., Littlewood J., Pólya G.* Inequalities. Cambridge Mathematical Library. Cambridge University Press, 1988.

[71] *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.

[72] *Håstad J.* Computational limitations of small-depth circuits. Cambridge, MA, USA: MIT Press, 1987.

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

[74] *Hofmeister T.* A note on the simulation of exponential threshold weights // Proceedings of the 2nd Annual International Conference on Computing and Combinatorics. Springer, 1996. Vol. 1090 of *Lecture Notes in Computer Science*. P. 136–141.

[75] *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.

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

[77] *Immerman N.* Nondeterministic space is closed under complementation // Proceedings: Third Annual Structure in Complexity Theory Conference, Georgetown University, Washington, D. C., USA, June 14-17, 1988. 1988. P. 112–115.

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

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

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

[81] *Jukna S.* Boolean Function Complexity: Advances and Frontiers. Springer, 2012.

[82] *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.

[83] *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.

[84] *Karchmer M., Wigderson A.* Monotone Circuits for Connectivity Require Super-logarithmic Depth // Proc. of the 20th Annual ACM Symposium on Theory of Computing (STOC'88). ACM, 1988. P. 539–550.

[85] *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. 2014. P. 57.

[86] *Klauck H.* Algorithms for Parity Games // Automata Logics, and Infinite Games / Ed. by E. Gradel, W. Thomas, T. Wilke. Springer Berlin / Heidelberg, 2002. Vol. 2500 of *Lecture Notes in Computer Science*. P. 553–563.

[87] *Klivans A. R., O'Donnell R., Servedio R. A.* Learning Intersections and Thresholds of Halfspaces // Journal of Computer and System Sciences. 2004. Vol. 68, N. 4. P. 808–840.

[88] *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.

[89] *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.

[90] *Kollár J.* Sharp effective Nullstellensatz // J. Amer. Math. Soc. 1988. Vol. 1. P. 963–975.

[91] *Kontchakov R., Zakharyaschev M.* An Introduction to Description Logics and Query Rewriting // Reasoning Web. Reasoning on the Web in the Big Data Era / edited byM. Koubarakis, G. Stamou, G. Stoilos, I. Horrocks, P. Kolaitis, G. Lausen, G. Weikum. Springer International Publishing, 2014. Vol. 8714 of *Lecture Notes in Computer Science*. P. 195–244.

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

[93] *Krause M., Pudlák P.* Computing Boolean functions by polynomials and threshold circuits // Comput. Complex. 1998. Vol. 7, N. 4. P. 346–370.

[94] *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.

[95] *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.

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

[97] *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.

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

[99] *Motik B., Cuenca Grau B., Horrocks I., Wu Z., Fokoue A., Lutz C.* OWL 2 Web Ontology Language Profiles. W3C Recommendation. 11 December 2012. Available at `http://www.w3.org/TR/owl2-profiles/`.

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

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

[102] *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.

[103] *Myhill J., Kautz W. H.* On the size of weights required for linear-input switching functions // IRE Trans. on Electronic Computers. 1961. Vol. 10, N. 2. P. 288–290.

[104] 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.

[105] *Parberry I.* Circuit complexity and neural networks. Cambridge, MA, USA: MIT Press, 1994.

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

[107] *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.

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

[109] *Razborov A.* Lower Bounds for Deterministic and Nondeterministic Branching Programs // Proc. of the 8th Int. Symposium on Fundamentals of Computation Theory (FCT'91). Vol. 529 of *Lecture Notes in Computer Science*. Springer, 1991. P. 47–60.

[110] *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.

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

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

[113] *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.

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

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

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

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

[118] *Sherstov A. A.* Separating AC^0 from Depth-2 Majority Circuits // SIAM J. Comput. 2009. Vol. 38, N. 6. P. 2113–2129.

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

[120] *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.

[121] *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.

[122] *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.

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

[124] *Szelepcsényi R.* The moethod of focing for nondeterministic automata // Bulletin of the EATCS. 1987. Vol. 33. P. 96–99.

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

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

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

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

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

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

[131] *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.

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

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

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

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

[136] *Подольский, В. В., Шерстов, А. А.* Небольшое уменьшение степени многочлена с заданной знаковой функцией может экспоненциально увеличить его вес и длину // Математические заметки. 2010. Vol. 87. P. 885–899.

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

[138] *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.