

# Нижние оценки для полиномиального исчисления в случае идеалов, отличных от биномиальных

М. В. Алехнович\*, А. А. Разборов†

13 марта 2003 г.

## Аннотация

В настоящей работе обобщаются недавние линейные нижние оценки на степень вывода в полиномиальном исчислении, основанные на рассмотрении биномиальных идеалов. Мы предлагаем достаточно общий критерий трудности булевых функций (называемый нами *иммунностью*), которому, в частности, удовлетворяет случайная булева функция, и доказываем нижние оценки на степень вывода для широкого класса тавтологий, основанных на иммунных функциях. В качестве одного из приложений наших методов мы обобщаем цейтиновские тавтологии по модулю  $p$  на случай булевых переменных (т.е. в присутствии аксиом  $x_i^2 = x_i$ ) и доказываем трудность их вывода в полиномиальном исчислении над любым полем характеристики, отличной от  $p$ . Затем, по аналогии с цейтиновскими, мы определяем “поточковые” тавтологии, основанные на функции голосования, и показываем их трудность над любым полем. Также мы доказываем нижнюю оценку  $\Omega(n)$  на степень вывода случайных  $k$ -КНФ в полиномиальном исчислении над полями характеристики 2.

---

\*МГУ им М. В. Ломоносова mike@mscme.ru. Работа выполнена при поддержке гранта ИНТАС # 96-753 и Российского Фонда Фундаментальных Исследований

†Математический Институт им. В.А.Стеклова razborov@genesis.mi.ras.ru. Работа выполнена при поддержке гранта ИНТАС # 96-753 и Российского Фонда Фундаментальных Исследований; часть работы выполнена во время визита в Принстонский Университет и Центр Дискретной Математики и Теоретической Информатики (DIMACS)

# 1 Введение

Теория сложности пропозициональных доказательств – направление исследований, развивавшееся особенно бурно на протяжении последних десяти лет. Его роль в развитии общей теории эффективных доказательств можно сравнить с ролью, которую играет сложность булевых схем в теории эффективных вычислений. Несмотря на то, что первоначальные мотивации для изучения сложности пропозициональных доказательств были весьма разнообразны (в частности, пропозициональные системы естественным образом возникают при изучении доказуемости в некоторых теориях первого порядка), в конце концов оказывается, что данная теория практически целиком посвящена следующему фундаментальному вопросу. Что может быть *доказано* (в обычном математическом смысле) при условии, что наши *вычислительные* возможности ограничены вычислением значений “малых” схем из некоторого класса  $\mathcal{C}$  (см., например, [BP98])? Таким образом, теория сложности пропозициональных доказательств в некотором смысле дополняет обычную теорию (неоднородной) вычислительной сложности; более того, между этими дисциплинами существуют довольно богатые и полезные взаимосвязи ([Raz96, BP98]).

В последнее время значительное внимание исследователей привлекают пропозициональные исчисления, являющиеся по существу алгебраическими, которые имитируют процесс доказательства наиболее простых и фундаментальных фактов коммутативной алгебры. Идея использования алгебраической техники в теории доказательств восходит к работе [ВКРР96], в которой определяется так называемое гильбертово исчисление, основанное на теореме Гильберта о нулях (Nullstellensatz proof system). В работе [СЕI96] была предложена еще более естественная алгебраическая система доказательств (названная впоследствии полиномиальным исчислением), которая в точности имитирует процесс порождения идеалов конечными системами порождающих полиномов. Это исчисление обладает некоторыми важными свойствами, которые делают его естественным кандидатом на использование в системах автоматического доказательства теорем [СЕI96]; по этой причине получение нижних оценок для полиномиального исчисления представляется важной и интересной задачей.

Все известные подходы к доказательству нижних оценок на степень вывода в полиномиальном исчислении (с одним важным исключением

[Kra01]) используют идею локализации (которую мы подробно обсудим в разделе 2.3). Неотъемлемой частью первых статей в этом направлении ([Raz98, IPS99]), посвященных доказательству нижних оценок для принципа Дирихле, являлись также довольно специфические и трудоемкие вычисления (“танец голубей”).

В недавней работе Д. Ю. Григорьева [Gri98] была предложена простая идея, позволяющая полностью избежать подобных вычислений и доказать нижнюю оценку  $\Omega(n)$  на степень вывода цейтинговских тавтологий в полиномиальном исчислении. Первоначальное доказательство в [Gri98] охватывало лишь (более слабое) гильбертово исчисление, однако уже в работе [BGIP99] авторы обобщили его на случай полиномиального исчисления; дальнейшие результаты в этом направлении были получены в работах [BI99, Gri01, ABRW00]. Главный недостаток обсуждаемого подхода – это то, что в нем по существу используется биномиальность возникающих идеалов, поэтому он применим лишь в случае, когда базисные функции биномиальны. Проблема, однако, в том, что биномиальные функции встречаются крайне редко: так, если потребовать выполнение булевых соотношений  $x^2 - x = 0$ , то класс биномиальных функций исчерпывается сложением по модулю 2, а если к тому же характеристика основного поля равна 2, то их не существует вообще (иногда с этим недостатком удается справиться используя технику редукций малой степени, как это было сделано в [BGIP99], однако, как видно из примера  $k$ -КНФ в характеристике 2 (см. ниже раздел 4.3), даже такое решение возможно не всегда).

Подобное положение дел сильно отличается от аналогичной ситуации с исчислением резолюций, для которого в работе [ABRW00] приводится общий критерий трудности (устойчивость), которому с высокой вероятностью удовлетворяет случайная функция и доказываемая сложность тавтологий, индуцированных устойчивыми функциями при условии, что основная комбинаторная структура обладает достаточно хорошими свойствами “расширения” (“expansion” в англоязычной литературе). Данная идеология, которую подтверждает приведенный выше результат, напоминает по своему духу идеологию, лежащую в основе “естественных доказательств” [RR97]: любое доказательство нижних оценок, пригодное хотя бы для одной конкретной функции, должно быть также пригодным для широкого класса функций, заданного некоторым конструктивным комбинаторным свойством.

В настоящей статье аналогичная задача решается для полиномиального исчисления. А именно, мы предлагаем общий критерий трудности (иммунность) и доказываем нижние оценки на степень вывода в полиномиальном исчислении для широкого класса тавтологий, основанных на иммунных функциях. Следует отметить, что над полями положительной характеристики  $p$  свойство иммунности, с точностью до отрицания, совпадает с понятием слабой  $MOD_p$ -степени, предложенной в [Gre00] (для произвольных, в том числе и составных значений  $p$ ) в качестве части общего проекта, направленного на понимание *вычислительных* возможностей мультилинейных полиномов.

Как одно из приложений наших методов мы рассматриваем цейтиновские тавтологии по модулю  $p$  (предложенные в работе [BGIP99]) в булевом случае (т.е. когда идеал по умолчанию содержит аксиомы  $x_i^2 = x_i$ ) и доказываем трудность их вывода в полиномиальном исчислении над любым полем характеристики, отличной от  $p$ . Затем мы рассматриваем аналог цейтиновских тавтологий в характеристике 0 (поточковые тавтологии) и доказываем, что они трудны над любым полем. Однако, наиболее важный вклад данной работы заключается в том, что используемые методы позволяют напрямую работать в случае поля  $\mathbb{F}_2$ , который представляет наибольший интерес. В частности, доказывается оптимальная нижняя оценка для случайных  $k$ -КНФ над этим полем, что дает ответ на открытый вопрос, поставленный в [BI99].

Кроме того, мы рассматриваем вариант принцип Дирихле  $EPHP_n^m$ , предложенный в работе [BW99], и доказываем его трудность для полиномиального исчисления. Данный результат следует из [Raz98], однако мы даем существенно более простое доказательство, не использующее трудоемкую технику “танца голубей”. Наконец, мы устанавливаем (довольно слабую) взаимосвязь между устойчивыми функциями из [ABRW00] и иммунными полиномами в случае нулевой характеристики, что позволяет получать нижние оценки для *полиномиального исчисления* (также в нулевой характеристике), основанные лишь на *устойчивости* базисных функций.

Статья организована следующим образом. Раздел 2 содержит необходимый предварительный материал, а также общее описание метода доказательства нижних оценок для полиномиального исчисления, основанного на локализации. Основные утверждения о трудности тавтологий рассматриваемого вида доказываются в разделе 3, описанным выше приложениям посвящен раздел 4. В заключительном разделе 5 приводятся

несколько открытых вопросов.

## 2 Предварительные сведения

Пусть  $\mathbb{F}$  – произвольное поле. Мы будем в основном работать в  $\mathbb{F}$ -алгебре  $S_n(\mathbb{F})$ , которая получается при факторизации кольца коммутативных полиномов  $\mathbb{F}[x_1, \dots, x_n]$  по идеалу, порожденному полиномами  $x_i^2 - x_i$  ( $1 \leq i \leq n$ ). Любой элемент  $f \in S_n(\mathbb{F})$  обладает единственным представлением в виде мультилинейного полинома (которое, в частности, определяет его *степень*  $\deg(f)$ ), а также единственным представлением в виде  $\mathbb{F}$ -значной функции на  $\{0, 1\}^n$ . Мы будем попеременно пользоваться этими представлениями в зависимости от контекста. В случае, если не оговорено противное, все полиномы рассматриваемые в данной статье будут мультилинейными, поэтому мы иногда будем опускать этот термин.

Для полинома  $f$  обозначим через  $\text{Vars}(f)$  множество всех его существенных переменных. *Назначением (переменных для полинома  $f$ )* мы будем называть отображение  $\alpha : \text{Vars}(f) \rightarrow \{0, 1\}$ .

В силу исторических причин при изучении полиномов обычно интересуются множеством их *корней*, поэтому мы ассоциируем нулевой элемент поля с логической константой ИСТИНА. Таким образом, назначение переменных  $\alpha$  *удовлетворяет* полиному  $f$  в том и только том случае, когда  $\alpha$  является его корнем. В соответствии с этим, любая булева функция  $g$  единственным образом определяет мультилинейный полином  $p_g$ , который обращается в 0 при назначении  $\alpha$  в случае  $g(\alpha) = 1$  и обращается в 1 если  $g(\alpha) = 0$ .

*Подстановкой (переменных для полинома  $f$ )* мы будем называть отображение  $\rho : \text{Vars}(f) \rightarrow \{0, 1, \star\}$ . Через  $|\rho|$  будет обозначаться число назначенных переменных, т.е.  $|\rho| \stackrel{\text{def}}{=} |\rho^{-1}(\{0, 1\})|$ . Для подстановки  $\rho$  и полинома  $f$  полином  $f|_\rho$  получается из  $f$  подстановкой  $\rho(x)$  вместо каждой переменной  $x \in \rho^{-1}(\{0, 1\})$ , при этом все переменные  $x \in \rho^{-1}(\star)$  остаются без изменения.

Для кортежа переменных  $\vec{v} = \{v_1, \dots, v_k\}$  и  $\vec{\epsilon} \in \{0, 1\}^k$  обозначим через  $\chi_{\vec{\epsilon}}(\vec{v})$  мультилинейный полином, который обращается в 1 если  $\vec{v} = \vec{\epsilon}$  и в 0 в противном случае (иными словами,  $\chi_{\vec{\epsilon}}(\vec{v}) \stackrel{\text{def}}{=} \prod_{i \in [k]} (1 - v_i - \epsilon_i + 2v_i\epsilon_i)$ ). Следующее тождество, несмотря на его очевидность, является

крайне полезным:

$$f = \sum_{\vec{\epsilon} \in \{0,1\}^k} \chi_{\vec{\epsilon}}(\vec{v}) \cdot (f|_{\vec{v}=\vec{\epsilon}}) \quad (1)$$

(здесь использовано сокращение  $\vec{v} = \vec{\epsilon}$  для обозначения подстановки, назначающей значения  $\epsilon_i$  всем переменным  $v_i$  и оставляющей все остальные переменные без изменения).

$Span(f_1, \dots, f_k)$  будет обозначать идеал, порожденный полиномами  $f_1, \dots, f_k$ . Мы будем говорить, что полином  $g$  является *семантическим следствием* полиномов  $f_1, \dots, f_k$  (обозначение  $f_1, \dots, f_k \models g$ ), если  $\forall \alpha \in \{0, 1\}^V (f_1(\alpha) = \dots = f_k(\alpha) = 0 \Rightarrow g(\alpha) = 0)$ , где  $V = Vars(f_1) \cup \dots \cup Vars(f_k) \cup Vars(g)$ . Хорошо известно (см., например, [BIKPRS96, теорема 5.2]), что в интересующем нас случае алгебры  $S_n(\mathbb{F})$ ,  $f_1, \dots, f_k \models g$  имеет место тогда и только тогда, когда  $g \in Span(f_1, \dots, f_k)$ .

Обозначим через  $T_n$  множество всех *мультилинейных термов*, т.е. произведений вида  $x_{i_1} x_{i_2} \dots x_{i_d}$ , где  $1 \leq i_1 < i_2 < \dots < i_d \leq n$ . *Степенью*  $\deg(t)$  *терма*  $t$  называется число входящих в него переменных. Обозначим  $T_{n,d} \stackrel{\text{def}}{=} \{t \in T_n \mid \deg(t) \leq d\}$ , и пусть  $S_{n,d}(\mathbb{F}) \stackrel{\text{def}}{=} \mathbb{F}T_{n,d}$  – линейное пространство, образованное всеми мультилинейными полиномами, степень которых не превышает  $d$ . Запись  $t \in f$  будет обозначать, что терм  $t$  содержится в полиноме  $f$  с ненулевым коэффициентом.

Для натурального числа  $n$  положим  $[n] \stackrel{\text{def}}{=} \{1, 2, \dots, n\}$ . В дальнейшем мы используем (стандартные для теории сложности) обозначения  $\Omega, \omega$ , в точности противоположные по смыслу  $O, o$ -обозначениям. Таким образом,  $\Omega(f(n))$  обозначает некоторую функцию  $g(n)$  такую, что  $(\exists \epsilon > 0)(\forall n)(g(n) \geq \epsilon f(n))$ ; аналогично, запись  $\omega(f(n))$  означает функцию  $g(n)$  со свойствами  $\lim_{n \rightarrow \infty} \frac{g(n)}{f(n)} = \infty$ .

## 2.1 Полиномиальное исчисление

**Определение 2.1** ([SEI96]) Строки вывода в полиномиальном исчислении суть элементы  $S_n(\mathbb{F})$ , при этом имеются два правила вывода, называемые *аддитивным* и *мультипликативным* соответственно:

$$\frac{f \quad g}{\alpha f + \beta g} \quad (2)$$

и

$$\frac{f}{f \cdot x}, \quad (3)$$

где  $f, g \in S_n(\mathbb{F})$ ;  $\alpha, \beta \in \mathbb{F}$  и  $x$  – произвольная переменная. Для полиномов  $f_1, \dots, f_m, g \in S_n(\mathbb{F})$  выводом  $g$  из  $f_1, \dots, f_m$  в полиномиальном исчислении называется вывод, в котором все исходные полиномы находятся среди  $f_1, \dots, f_m$ , а заключительным полиномом является  $g$ . Опровержением системы полиномов  $f_1, \dots, f_m$  называется вывод 1 из  $f_1, \dots, f_m$ .

Очевидно, что  $g$  обладает выводом из  $f_1, \dots, f_m$  в полиномиальном исчислении тогда и только тогда, когда  $g \in \text{Span}(f_1, \dots, f_m)$ , что, как мы уже отметили выше, эквивалентно  $f_1, \dots, f_m \models g$ . В частности, система полиномов  $(f_1, \dots, f_m)$  опровержима в том и только том случае, когда система уравнений  $f_1 = f_2 = \dots = f_m = 0$  не имеет 0-1 решений.

Степенью данного применения (2) аддитивного правила вывода назовем  $\max\{\deg(f), \deg(g)\}$ , а степень мультипликативного правила (3) определим как  $\deg(f) + 1$ . Степень вывода, по определению, равна максимальной степени всех встречающихся применений правил вывода.

## 2.2 Тавтологии, индуцированные расширителями

В этом разделе мы определяем требования, накладываемые на основную комбинаторную структуру наших тавтологий. Мы используем понятие расширителя (expander), предложенное (в контексте 0-1 матриц) в работах [CS88, ABRW00].

Для  $(m \times n)$  0-1 матрицы  $A$  положим  $J_i(A) \stackrel{\text{def}}{=} \{j \in [n] \mid a_{ij} = 1\}$ .

**Определение 2.2 ([ABRW00])** Границей  $\partial_A(I)$  множества строк  $I \subseteq [m]$  матрицы  $A$  называется множество всех столбцов  $j \in [n]$  (в свою очередь называемых *граничными элементами*) таких, что  $\{a_{ij} \mid i \in I\}$  содержит в точности одну единицу. Матрица  $A$ , по определению, является  $(r, s, c)$ -расширителем если  $|J_i(A)| \leq s$  для всех  $i \in [m]$  и, кроме того, выполнено условие  $\forall I \subseteq [m](|I| \leq r \Rightarrow |\partial_A(I)| \geq c \cdot |I|)$ .

Данное определение обобщает понятие расширителя в контексте гиперграфов из [CS88] (в последней работе рассматриваются расширители лишь в случае  $c = 1/2$ ). В разделе 4.1 мы обсудим явные конструкции хороших расширителей.

Положим  $X_i(A) \stackrel{\text{def}}{=} \{x_j \mid j \in J_i(A)\}$ . Пусть даны полиномы  $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$  такие, что  $\text{Vars}(f_i) \subseteq X_i(A)$ . В настоящей работе нас интересуют системы полиномиальных уравнений вида

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \dots \\ f_m(x_1, \dots, x_n) = 0. \end{cases} \quad (4)$$

В [ABRW00] было доказано, что если  $f_i$  (более точно, характеристические функции множества их нулей) в некотором смысле сложны (а именно, являются устойчивыми), а  $A$  – достаточно хороший расширитель, то система уравнений (4) трудна для исчисления резольвий. Опираясь на технику, первоначально развитую в [Gr98, BGIP99], в работе [ABRW00] было показано, что система (4) трудна также для полиномиального исчисления, но лишь в случае, когда  $f_i$  соответствуют функциям логического сложения по модулю 2 и  $\text{char } \mathbb{F} \neq 2$ . Мы предлагаем *общий* критерий сложности для функций  $f_i$ , из которого вытекает трудность системы (4) для полиномиального исчисления.

**Определение 2.3** Полином  $f$  является  $\ell$ -*иммунным* если для любого ненулевого мультилинейного полинома  $g$  из  $f \models g$  вытекает  $\deg(g) \geq \ell$ . Булева функция  $g$  называется  $\ell$ -*иммунной* над некоторым полем, если таковым является ассоциированный с ней над этим полем полином  $p_g$ .

В соответствии с данным определением, полином считается сложным, если у него нет нетривиальных семантических следствий малой степени. Очевидно, что полином является  $\ell$ -иммунным в том и только том случае, когда этим свойством обладает характеристическая функция множества его нулей.

В случае поля положительной характеристики  $p$  иммунитет полинома тесно связана со следующим понятием:

**Определение 2.4 ([Gre00])** Слабой  $\text{MOD}_p$ -*степенью* булевой функции  $g(x_1, \dots, x_n)$  называется наименьшая возможная степень ненулевого мультилинейного полинома  $f(x_1, \dots, x_n)$  с целочисленными коэффициентами такого, что для всех  $\alpha \in \{0, 1\}^n$  имеет место импликация  $g(\alpha) = 0 \Rightarrow f(\alpha) = 0 \pmod p$ .

Чтобы связать эти понятия, нам понадобится следующая элементарная лемма.

**Лемма 2.5** Полином  $f(x_1, \dots, x_n)$  над полем  $\mathbb{F}$  является  $\ell$ -иммунным тогда и только тогда, когда для любого ненулевого мультилинейного

полинома  $g(x_1, \dots, x_n)$  с целочисленными коэффициентами из  $f \models g$  следует  $\deg(g) \geq \ell$ .

**Доказательство.** Часть “только тогда” очевидна. Для доказательства обратного утверждения будем рассуждать от противного. Пусть  $g_0 \in S_n(\mathbb{F})$ ,  $f \models g_0$  и  $\deg(g_0) < \ell$ . Мы покажем, как найти *целочисленный* полином  $g$  с теми же свойствами.

Для этого рассмотрим  $\mathbb{F}$ -значные переменные  $g_t$  для  $t \in T_n$ , соответствующие неизвестным коэффициентам полинома  $g$ . В терминах этих переменных, условие  $f \models g$  записывается в виде системы линейных уравнений  $\{ \sum_{t \in T_n} g_t t(\alpha) = 0 \mid f(\alpha) = 0 \}$  с целыми коэффициентами. Добавим к этой системе уравнения  $g_t = 0$  для всех термов  $t$  таких, что  $\deg(t) \geq \ell$ , а также неравенство  $g_{t_0} \neq 0$  для произвольно выбранного терма  $t_0$  из числа встречающихся в  $g$  с ненулевыми коэффициентами.

Определенная таким образом система однородных линейных уравнений и неравенств с целыми коэффициентами имеет решение в поле  $\mathbb{F}$ . Из элементарной линейной алгебры вытекает, что в этом случае она также обладает целочисленным решением, и это решение определяет полином  $g$  с требуемыми свойствами. ■

**Следствие 2.6** 1. Булева функция является  $\ell$ -иммунной над полем  $\mathbb{F}$  характеристики  $p > 0$  тогда и только тогда, когда слабая  $MOD_p$ -степень ее отрицания больше или равна  $\ell$ .

2. Булева функция  $g(x_1, \dots, x_n)$  является  $\ell$ -иммунной над полем  $\mathbb{F}$  нулевой характеристики тогда и только тогда, когда всякий ненулевой мультилинейный полином  $f(x_1, \dots, x_n)$  с целыми коэффициентами, обладающий свойством  $\forall \alpha \in \{0, 1\}^n (g(\alpha) = 1 \Rightarrow f(\alpha) = 0)$  имеет степень больше или равную  $\ell$ .

Таким образом, над полями положительной характеристики иммунитет совпадает (с точностью до отрицания) со слабой степенью, и главная причина, по которой мы вводим новый термин для этого понятия состоит в том, что для полей характеристики 0 устоявшееся определение “слабой степени” (см. [ABFR94]) совершенно непригодно для наших целей.

Следующая простая лемма устанавливает, что иммунитет хорошо себя ведет по отношению к подстановкам.

**Лемма 2.7** 1. Если полином  $f$  является  $\ell$ -иммунным, то для любой подстановки  $\rho$  полином  $f|_\rho$  является  $(\ell - |\rho|)$ -иммунным.

2. Пусть  $V \subseteq \text{Vars}(f)$ , и предположим, что для любой подстановки  $\rho$  такой, что  $\rho^{-1}(\star) = V$  полином  $f|_\rho$  является  $\ell$ -иммунным. Тогда и сам  $f$  является  $\ell$ -иммунным.

**Доказательство. Часть 1)** Допустим, что  $\rho$  присваивает значения  $\epsilon_1, \dots, \epsilon_k$  переменным  $v_1, \dots, v_k$ , и предположим, что найдется  $g \neq 0$  степени  $\deg(g) < \ell - k$  такой, что  $f|_{\vec{v}=\vec{\epsilon}} \models g$ . Без ограничения общности мы можем также предположить, что  $\text{Vars}(g) \cap \{v_1, \dots, v_k\} = \emptyset$ . Тогда, очевидно,  $f \models \chi_{\vec{\epsilon}}(\vec{v}) \cdot g$  и  $\chi_{\vec{\epsilon}}(\vec{v}) \cdot g \neq 0$ , полученное противоречие доказывает часть 1).

**Часть 2)** Предположим противное, т.е.  $f \models g$  для некоторого  $g \neq 0$  такого, что  $\deg(g) < \ell$ . Выберем произвольным образом подстановку  $\rho$  такую, что  $\rho^{-1}(\star) = V$  и  $g|_\rho \neq 0$ . Тогда  $f|_\rho \models g|_\rho$ , что противоречит  $\ell$ -иммунности полинома  $f|_\rho$ . ■

### 2.3 Доказательство нижних оценок для полиномиального исчисления, основанное на методе локализации

В этом разделе мы кратко опишем, как идея локализации помогает при доказательстве нижних оценок на степень вывода в полиномиальном исчислении. Для начала напомним несколько стандартных понятий из коммутативной алгебры (адаптированных к интересующему нас случаю кольца  $S_n(\mathbb{F})$ ).

**Определение 2.8** Линейный порядок  $\preceq$  на множестве всех термов  $T_n$  называется *допустимым*, если выполнены следующие два условия:

1.  $\forall t_1, t_2 \in T_n (\deg(t_1) < \deg(t_2) \Rightarrow t_1 \prec t_2)$ .
2. Если  $t_1 \preceq t_2$  и терм  $t \in T_n$  не содержит переменных из  $t_1, t_2$ , то  $tt_1 \preceq tt_2$ .

Зафиксируем произвольный допустимый порядок  $\preceq$  на множестве  $T_n$ . Для  $f \in S_n(\mathbb{F})$  обозначим через  $LT(f) \in T_n$  *старший терм* полинома  $f$  по отношению к  $\preceq$ . Из части 1 определения 2.8 вытекает, что  $\deg(LT(f)) = \deg(f)$ .

**Определение 2.9** Пусть  $V$  – идеал в кольце  $S_n(\mathbb{F})$ . Терм  $t$  *приводим* mod  $V$  (по отношению к данному допустимому порядку  $\preceq$ ) если  $V$  содержит ненулевой полином  $f$  такой, что  $LT(f) = t$ . Множество всех неприводимых термов  $\Delta$  является линейно независимым по модулю  $V$ , и алгебра  $S_n(\mathbb{F})$  раскладывается в прямую сумму линейных пространств

$$S_n(\mathbb{F}) = \mathbb{F}\Delta \oplus V.$$

Оператор проекции на первую компоненту в этом разложении называется *оператором редукции* и обозначается  $R_V$ . Он отображает терм  $t$  в полином  $R_V(t) \in \mathbb{F}\Delta$ , однозначно определяемый свойством  $t - R_V(t) \in V$ .

В работе [CEI96] эти классические понятия впервые рассматриваются в случае, когда  $V$  является всего лишь псевдоидеалом, т.е. линейным пространством, не обязательно замкнутым относительно мультипликативного правила. Соответствующие определения распространяются на этот случай следующим образом.

Для полиномов  $f_1, \dots, f_m \in S_{n,d}(\mathbb{F})$  обозначим через  $V_{n,d}(f_1, \dots, f_m)$  множество всех  $g \in S_{n,d}(\mathbb{F})$ , получаемых из  $f_1, \dots, f_m$  выводом в полиномиальном исчислении степени, не превышающей  $d$ . Ввиду наличия аддитивного правила,  $V_{n,d}(f_1, \dots, f_m)$  – линейное подпространство в  $S_{n,d}(\mathbb{F})$ . Назовем терм  $t \in T_{n,d}$  *приводимым*, если  $t = LT(f)$  для некоторого  $f \in V_{n,d}(f_1, \dots, f_m)$  и *неприводимым* в противном случае. Через  $\Delta_{n,d}(f_1, \dots, f_m)$  обозначим множество всех неприводимых термов в  $T_{n,d}$ . Термы из  $\Delta_{n,d}(f_1, \dots, f_m)$  линейно независимы по модулю  $V_{n,d}(f_1, \dots, f_m)$ , и так же, как и в классическом случае, мы получаем разложение

$$S_{n,d}(\mathbb{F}) = \mathbb{F}\Delta_{n,d}(f_1, \dots, f_m) \oplus V_{n,d}(f_1, \dots, f_m). \quad (5)$$

Обозначим оператор проекции на первую координату (как и ранее называемый *оператором редукции*) через  $R_{n,d,f_1,\dots,f_m}$ .

Чтобы доказать  $1 \notin V_{n,d}(f_1, \dots, f_m)$ , нам следует показать

$$R_{n,d,f_1,\dots,f_m}(1) \neq 0.$$

Для этого достаточно построить нетривиальный линейный оператор  $R \neq 0$  на  $S_{n,d}(\mathbb{F})$  который был бы сильнее  $R_{n,d,f_1,\dots,f_m}$  в смысле

$$\text{Ker}(R_{n,d,f_1,\dots,f_m}) \subseteq \text{Ker}(R).$$

В следующей лемме содержатся некоторые достаточные условия для того, чтобы  $R$  обладал этим свойством.

**Лемма 2.10 ([Raz98])** Пусть дано множество аксиом  $f_1, \dots, f_m$ , и допустим также, что  $d < n$ . Если существует линейный оператор  $R \neq 0$  на  $S_{n,d}(\mathbb{F})$  такой, что:

- 1)  $\forall i R(f_i) = 0$ ;
- 2)  $\forall t, x_j (\deg(t) < d \rightarrow R(x_j \cdot t) = R(x_j \cdot R(t)))$ ,

то любое опровержение  $(f_1, \dots, f_m)$  в полиномиальном исчислении имеет степень больше  $d$ .

В работе [Raz98] было предложено определять искомый оператор  $R$  локальным образом

$$R(t) \stackrel{\text{def}}{=} R_{V(t)}(t), \quad (6)$$

где  $R_{V(t)}$  – классический оператор редукции по модулю настоящего идеала  $V(t)$ , порожденного некоторым “небольшим” подмножеством аксиом, определяемым термом  $t$ . Преимущество такого подхода состоит в том, что нам гораздо более понятна структура классических операторов редукции, чем операторов редукции для псевдоидеалов; более того, в классическом случае для их изучения можно применять семантические средства.

Если  $R$  – произвольный оператор, удовлетворяющий условиям леммы 2.10, то всякий полином  $f = \sum_i a_i t_i$ , получаемый из  $\{f_1, \dots, f_m\}$  выводом степени  $\leq d$  допускает альтернативное представление в виде суммы

$$f = \sum_i a_i (t_i - R(t_i)).$$

Если, помимо этого, операторы  $R(t)$  задаются формулой (6), то  $t_i$  являются старшими термами полиномов  $(t_i - R(t_i))$ , не сокращающимися друг с другом в этой сумме и, более того, всякий полином  $t_i - R(t_i)$  является следствием “небольшого” числа аксиом. В этом и состоит идея локализации: мы пытаемся доказать, что всякий полином в  $V_{n,d}(f_1, \dots, f_m)$  можно на самом деле представить в виде суммы полиномов, каждый из которых является следствием малого числа аксиом, причем старшие термы этих полиномов не сокращаются друг с другом. Или, говоря неформально, *все что можно вывести, используя полиномы малой степени, можно по существу вывести локально.*

### 3 Основные результаты

Наш первый основной результат (теорема 3.8) утверждает, что для любого  $(r, s, c)$ -расширителя  $A$  и  $\ell$ -иммунных полиномов  $f_i$  всякое опровержение системы (4) в полиномиальном исчислении обязано иметь степень, превышающую  $r(\ell/4 - (s - c))$ . Эта оценка существенно использует неравенство  $\ell > 4(s - c)$  и по этой причине она неприменима к расширителям, для которых  $s$  и  $c$  являются небольшими константами. Нам удалось доказать более сильную оценку  $rc/2$  лишь в случае, когда полиномы  $f_i$  имеют максимально возможную иммунность  $s$  (теорема 3.13). Эта последняя оценка будет использована в разделе 4.3 для установления трудности опровержения случайных  $k$ -КНФ при малых значениях  $k$  в полиномиальном исчислении над полями характеристики 2.

Центральным местом всего доказательства является следующая теорема.

**Теорема 3.1** *Предположим, что  $\vec{y}, \vec{v}, \vec{z}$  образуют разбиение множества переменных  $\{x_1, \dots, x_n\}$ ;  $\vec{P} = \vec{P}(\vec{y}, \vec{v})$ ,  $Q = Q(\vec{v}, \vec{z})$  – полиномы, зависящие от переменных  $\vec{y} \cup \vec{v}$ ,  $\vec{v} \cup \vec{z}$  соответственно, и пусть известно, что  $Q$  является  $(2|\vec{v}| + 1)$ -иммунным. Пусть терм  $t(\vec{y}, \vec{v})$ , не содержащий  $z$ -переменных, приводим по модулю идеала  $\text{Span}(\vec{P}, Q)$  по отношению к некоторому фиксированному допустимому порядку. Тогда терм  $t$  также приводим по модулю  $\text{Span}(\vec{P})$  по отношению к тому же порядку.*

**Доказательство.** Наивная попытка доказать эту теорему состоит в применении произвольного гомоморфизма вида  $\rho : \vec{z} \rightarrow \vec{f}(\vec{v})$ , который отображает  $Q$  в 0 и, следовательно, обладает свойством  $t = \rho(R_{\text{Span}(\vec{P}, Q)}(t)) \bmod \text{Span}(\vec{P})$  (такой гомоморфизм заведомо найдется так как полином  $Q$  имеет иммунность большую чем  $|\vec{v}|$  и, следовательно, ни один из полиномов  $\chi_{\vec{c}}(\vec{v})$  в разложении  $\sum \chi_{\vec{c}}(\vec{v})Q|_{\vec{v}=\vec{c}} = Q$  не является его семантическим следствием). К сожалению, эта простая идея не работает в общем случае ввиду того, что степень некоторых термов в  $R_{\text{Span}(\vec{P}, Q)}(t)$  может под действием  $\rho$  возрасти и превысить  $\deg(t)$ . Тем не менее, как мы увидим ниже в доказательстве леммы 3.14, этой идеи вполне достаточно в частном случае, когда полином  $Q$  имеет максимально возможную иммунность. В общем же случае нам придется использовать более сложные методы.

В определении 3.2 и последующих леммах мы предполагаем фиксированными некоторые  $\vec{x}, \vec{y}, \vec{z}, \vec{P}, Q$ , удовлетворяющие предположениям теоремы 3.1, а все операторы редукции определяются по отношению к произвольному фиксированному допустимому порядку  $\preceq$ . Обозначим  $k \stackrel{\text{def}}{=} |\vec{v}|$ .

**Определение 3.2 (Оператор  $R^Q$ )** Линейный оператор  $R^Q$  на  $S_n(\mathbb{F})$  определяется действием на базисные элементы  $T_n$  следующим образом:

$$R^Q(t) \stackrel{\text{def}}{=} \sum_{\vec{c} \in \{0,1\}^k} \chi_{\vec{c}}(\vec{v}) \cdot R_{\text{Span}(Q|_{\vec{v}=\vec{c}})}(t|_{\vec{v}=\vec{c}}).$$

Интуитивный смысл этой конструкции заключается в том, что мы пытаемся уменьшить  $z$ -степень терма  $t$  локально и независимо на подкубах булева куба  $\{0,1\}^n$ , определяемых всеми возможными подстановками переменных из  $\vec{v}$ . Описанный оператор полностью игнорирует  $y$ -переменные (поскольку они не встречаются в  $Q$ ), и главная проблема состоит в том, что  $R^Q$ , вообще говоря, может увеличить  $v$ -степень.

**Лемма 3.3** Для любого полинома  $f$  имеет место  $f = R^Q(f) \bmod \text{Span}(Q)$ .

**Доказательство.** Ввиду линейности оператора  $R^Q$  нам достаточно проверить, что  $Q \models t - R^Q(t)$  для любого терма  $t$ . Это эквивалентно тому, что для любого кортежа  $\vec{c}$  полином  $Q|_{\vec{v}=\vec{c}}$  семантически влечет

$$(t - R^Q(t))|_{\vec{v}=\vec{c}} = (t|_{\vec{v}=\vec{c}} - R_{\text{Span}(Q|_{\vec{v}=\vec{c}})}(t|_{\vec{v}=\vec{c}})).$$

Последнее соотношение очевидно. ■

**Лемма 3.4** Если  $|\text{Vars}(t) \cap \vec{z}| \leq k$ , то  $R^Q(t) = t$ .

**Доказательство.**

Мы должны проверить, что полиномы  $t$  и  $R^Q(t)$  совпадают. Для этого достаточно проверить совпадение полиномов  $t|_{\vec{v}=\vec{c}}$  и  $R^Q(t)|_{\vec{v}=\vec{c}} = R_{\text{Span}(Q|_{\vec{v}=\vec{c}})}(t|_{\vec{v}=\vec{c}})$  для каждого кортежа  $\vec{c} \in \{0,1\}^k$ . Однако поскольку  $Q$  является  $(2k+1)$ -иммунным, полином  $Q|_{\vec{v}=\vec{c}}$  имеет иммунитет  $(k+1)$  на основании леммы 2.7(1). Следовательно, терм  $t|_{\vec{v}=\vec{c}}$  степени  $\leq k$  неприводим по модулю идеала  $\text{Span}(Q|_{\vec{v}=\vec{c}})$ . ■

Следующая лемма лежит в основе всего нашего доказательства.

**Лемма 3.5** Пусть  $f$  – произвольный полином такой, что  $\vec{P}, Q \models f$ . Тогда  $\vec{P} \models R^Q(f)$ .

**Доказательство.** Как обычно, нам достаточно показать, что для любого кортежа  $\vec{c}$  имеет место  $\vec{P}|_{\vec{v}=\vec{c}} \models R^Q(f)|_{\vec{v}=\vec{c}}$ . Поскольку  $\vec{P}, Q \models f$ , согласно лемме 3.3 мы имеем  $\vec{P}, Q \models R^Q(f)$ , и поэтому  $\vec{P}|_{\vec{v}=\vec{c}}, Q|_{\vec{v}=\vec{c}} \models R^Q(f)|_{\vec{v}=\vec{c}}$ .

Зафиксируем назначение  $\vec{\delta}$  переменных  $\vec{y}$  такое, что  $\vec{P}|_{\vec{v}=\vec{c}}(\vec{\delta}) = 0$ . Тогда

$$Q|_{\vec{v}=\vec{c}} \models R^Q(f)|_{\vec{v}=\vec{c}, \vec{y}=\vec{\delta}}, \quad (7)$$

и мы должны показать, что

$$R^Q(f)|_{\vec{v}=\vec{c}, \vec{y}=\vec{\delta}}$$

на самом деле равен 0. Заметим, что  $R^Q(f)|_{\vec{v}=\vec{c}, \vec{y}=\vec{\delta}} = R_{Span(Q|_{\vec{v}=\vec{c}})}(f|_{\vec{v}=\vec{c}})|_{\vec{y}=\vec{\delta}}$ . Ясно, что все термы в  $R_{Span(Q|_{\vec{v}=\vec{c}})}(f|_{\vec{v}=\vec{c}})$  неприводимы по модулю  $Span(Q|_{\vec{v}=\vec{c}})$ . Поскольку множество неприводимых термов замкнуто вниз по включению, аналогичное утверждение справедливо для

$$R_{Span(Q|_{\vec{v}=\vec{c}})}(f|_{\vec{v}=\vec{c}})|_{\vec{y}=\vec{\delta}}.$$

Принимая во внимание также (7), мы получаем отсюда  $R^Q(f)|_{\vec{v}=\vec{c}, \vec{y}=\vec{\delta}} = 0$ , что и завершает доказательство леммы 3.5. ■

**Лемма 3.6** Пусть  $\vec{P} \models f_0 + \sum_{z_i \in Z} z_i f_i$ , и  $f_0$  не содержит  $z$ -переменных. Тогда  $\vec{P} \models f_0$ .

**Доказательство.** Достаточно применить подстановку, назначающую нули всем переменным  $z_i$ . ■

Мы готовы завершить доказательство теоремы 3.1. Положим  $f \stackrel{\text{def}}{=} R_{Span(\vec{P}, Q)}(t)$  и  $f' \stackrel{\text{def}}{=} R^Q(f)$ .

Согласно лемме 3.5 имеем  $\vec{P} \models R^Q(t - f)$ , а согласно лемме 3.4,  $R^Q(t) = t$ . Таким образом,  $\vec{P} \models (t - f')$ . Наша цель состоит в том, чтобы проверить, что все термы в  $f'$  либо  $\preceq$ -меньше чем  $t$  либо содержат  $z$ -переменные: после этого мы сможем применить лемму 3.6 и установить, что  $t$  приводим по модулю  $Span(\vec{P})$ .

Разделим все входящие в  $f$  термы на две группы следующим образом:

$$\begin{aligned} G_1 &= \{t_1 \mid |Vars(t) \cap \vec{z}| \leq k\} \\ G_2 &= \{t_1 \mid |Vars(t) \cap \vec{z}| > k\}. \end{aligned}$$

Рассмотрим произвольный терм  $t'_1 \in f'$  такой, что  $|Vars(t'_1) \cap \vec{z}| = \emptyset$ . Очевидно, что для некоторого  $t_1 \in f$  имеет место  $t'_1 \in R^Q(t_1)$ . Если  $t_1 \in G_1$ , то, поскольку на основании леммы 3.4  $G_1$  не изменяется под действием  $R^Q$ , мы сразу получаем  $t'_1 = t_1 \prec t$ . Поэтому допустим, что  $t_1 \in G_2$ . В этом случае  $\deg(t'_1) = |Vars(t'_1) \cap \vec{v}| + |Vars(t'_1) \cap \vec{y}| \leq k + |Vars(t'_1) \cap \vec{y}| = k + |Vars(t_1) \cap \vec{y}| < |Vars(t_1) \cap \vec{y}| + |Vars(t_1) \cap \vec{z}| \leq \deg(t_1) \leq \deg(t)$ .

Итак, все термы в  $f'$ , не содержащие  $z$ -переменных либо содержатся в  $f$  либо имеют степень меньше чем  $\deg(t)$ . Применяя лемму 3.6, получаем, что  $t$  приводим по модулю  $\vec{P}$ . Тем самым теорема 3.1 доказана. ■

**Следствие 3.7** В предположениях теоремы 3.1 имеет место

$$R_{Span(\vec{P}, Q)}(t) = R_{Span(\vec{P})}(t).$$

**Доказательство.** Очевидно, все термы в  $R_{Span(\vec{P})}(t)$  не содержат  $z$ -переменных. Следовательно, на основании теоремы 3.1 все они неприводимы по модулю  $Span(\vec{P}, Q)$ . ■

**Теорема 3.8** Пусть матрица  $A$  является  $(r, s, c)$ -расширителем,  $\ell$  – натуральное число такое, что  $s \leq r(\ell/4 - (s - c))$  и  $f_1, \dots, f_m$  –  $\ell$ -иммунные полиномы над некоторым полем  $\mathbb{F}$  такие, что  $Vars(f_i) \subseteq X_i(A)$ . Тогда всякое опровержение системы  $f_1 = \dots = f_m = 0$  в полиномиальном исчислении над  $\mathbb{F}$  обязано иметь степень, превышающую  $r(\ell/4 - (s - c))$ .

**Доказательство.** Идея доказательства состоит в том, чтобы сконструировать линейный оператор  $R$ , локально ведущий себя как оператор редукции по модулю соответствующего идеала и затем использовать лемму 2.10. Для построения  $R$  достаточно определить его на множестве всех термов  $t$  таких, что  $\deg(t) \leq r(\ell/4 - (s - c))$ . Прежде всего, нам потребуются еще несколько определений.

**Определение 3.9** Пусть дана  $(m \times n)$ -матрица  $A$ , и пусть  $f_1, \dots, f_m$  – полиномы, удовлетворяющие  $\text{Vars}(f_i) \subseteq X_i(A)$ . Для терма  $t$  обозначим через  $J(t)$  множество индексов  $\{j | t \text{ содержит } x_j\}$ . Для множества строк  $I \subseteq [m]$  положим  $\text{Span}(I) \stackrel{\text{def}}{=} \text{Span}(\{f_i | i \in I\})$ .

Теперь мы готовы описать линейный оператор  $R$ . Зафиксируем  $A, f_1, \dots, f_m, r, s, c, \ell$ , удовлетворяющие предположениям теоремы 3.8. Мы собираемся определить множество аксиом  $\text{Sup}(t) \subseteq [m]$  для любого терма  $t$ ; после этого применение к  $t$  оператора  $R$  будет заключаться в его редукции по модулю идеала  $\text{Span}(\text{Sup}(t))$ .

**Определение 3.10** Для терма  $t$  определим следующее отношение выводимости  $\vdash_t$  на множестве  $[m]$  всех строк матрицы  $A$ :

$$I \vdash_t i \equiv \left| J_i(A) \cap \left[ \bigcup_{i' \in I} J_{i'}(A) \cup J(t) \right] \right| > \frac{\ell}{4}. \quad (8)$$

Носителем  $\text{Sup}(t)$  терма  $t$  назовем замыкание пустого множества строк относительно отношения выводимости  $\vdash_t$ . Наконец, положим  $R(t) \stackrel{\text{def}}{=} R_{\text{Span}(\text{Sup}(t))}(t)$ .

Оставшаяся часть доказательства теоремы 3.8 состоит в проверке для оператора  $R$  условий 1) и 2) из леммы 2.10. Прежде всего, нам нужна оценка на мощность  $\text{Sup}(t)$ .

**Лемма 3.11** Для любого терма  $t$  такого, что  $\text{deg}(t) \leq r(\ell/4 - (s - c))$ , имеет место  $|\text{Sup}(t)| < r$ .

**Доказательство.** Предположим противное. Тогда существует множество  $I = \{i_1, \dots, i_r\}$  попарно различных строк такое, что  $\{i_1, \dots, i_{\nu-1}\} \vdash_t i_\nu$  ( $1 \leq \nu \leq r$ ). Согласно определению 2.2, это множество содержит по крайней мере  $cr$  граничных элементов. На основании (8), всякая строка  $i \in I$  содержит менее  $s - \ell/4$  граничных элементов, не содержащихся в  $J(t)$ . Поэтому  $J(t)$  содержит более чем  $cr - r(s - \ell/4) = r(\ell/4 - (s - c))$  элементов. Полученное противоречие доказывает лемму 3.11. ■

**Лемма 3.12** Предположим, что  $s - c < \ell/4$ ,  $t$  – произвольный терм и  $I$  – множество строк такое, что  $I \supseteq \text{Sup}(t)$  и  $|I| \leq r$ . Тогда

$$R_{\text{Span}(I)}(t) = R_{\text{Span}(\text{Sup}(t))}(t).$$

**Доказательство.** Применим определение расширителя ко множеству строк  $I \setminus Sup(t)$  и выберем строку  $i \in I \setminus Sup(t)$ , содержащую по крайней мере  $c$  граничных элементов. Тем самым,

$$J_i(A) \cap [\cup_{i' \in I \setminus (Sup(t) \cup \{i\})} J_{i'}(A)] \leq s - c.$$

Ввиду того, что  $Sup(t)$  замкнуто относительно  $\vdash_t$ , мы также получаем

$$J_i(A) \cap [\cup_{i' \in Sup(t)} J_{i'}(A) \cup J(t)] \leq \ell/4.$$

Сравнивая эти два неравенства, получаем

$$J_i(A) \cap [\cup_{i' \in I \setminus \{i\}} J_{i'}(A) \cup J(t)] \leq (s - c) + \ell/4 < \ell/2.$$

Полагая в формулировке теоремы 3.1

$$\begin{aligned} \vec{y} &:= \{x_1, \dots, x_n\} \setminus J_i(A) \\ \vec{v} &:= J_i(A) \cap [\cup_{i' \in I \setminus \{i\}} J_{i'}(A) \cup J(t)] \\ \vec{z} &:= J_i(A) \setminus [\cup_{i' \in I \setminus \{i\}} J_{i'}(A) \cup J(t)] \\ \vec{P} &:= \{f_{i'} \mid i' \in I \setminus \{i\}\} \\ Q &:= f_i, \end{aligned}$$

применим в этой ситуации ее следствие 3.7. Получаем  $R_{Span(I)}(t) = R_{Span(I \setminus \{i\})}(t)$ . Остается рекурсивно продолжить этот процесс удаления элементов из  $I$  до тех пор, пока в правой части не останется  $R_{Sup(t)}(t)$ . ■

Мы готовы завершить доказательство теоремы 3.8. Мы уже построили линейный оператор  $R$  на  $T_n$ ; рассмотрим теперь его ограничение на  $T_{n, r(\ell/4 - (s - c))}$ . Осталось проверить, что это ограничение в самом деле удовлетворяет требованиям леммы 2.10.

Чтобы проверить равенство  $R(f_i) = 0$  для каждой аксиомы  $f_i$ , положим  $t_i \stackrel{\text{def}}{=} \prod X_i(A)$ . Напомним, что  $\deg(t_i) \leq s \leq r(\ell/4 - (s - c))$ . Поэтому  $|Sup(t_i)| < r$  (на основании леммы 3.11) и для любого встречающегося в  $f_i$  терма  $t$  очевидным образом выполнено  $Sup(t) \subseteq Sup(t_i)$ . Далее,  $i \in Sup(t_i)$ . Согласно лемме 3.12,  $R(f_i) = R_{Sup(t_i)}(f_i) = 0$ . Таким образом, условие 1) выполнено.

Для проверки второго условия рассмотрим произвольный терм  $t$  такой, что  $\deg(t) \leq r(\ell/4 - (s - c)) - 1$  и переменную  $x_j$ . На основании леммы 3.11,  $|Sup(x_j t)| < r$ . Принимая также во внимание лемму 3.12, получаем  $R_{Sup(t)}(t) = R_{Sup(x_j t)}(t)$ . Далее, для любого терма  $t' \in R_{Sup(t)}(t)$  имеет

место  $Sup(x_j t') \subseteq Sup(x_j t)$ . Чтобы убедиться в этом, достаточно заметить, что  $J(t') \subseteq \bigcup_{i' \in Sup(t)} J_{i'}(A) \cup J(t)$ . Таким образом,  $R_{Sup(x_j t')}(x_j t') = R_{Sup(x_j t)}(x_j t')$  и

$$R(x_j R(t)) = R_{Sup(x_j t)}(x_j R_{Sup(x_j t)}(t)) = R_{Sup(x_j t)}(x_j t),$$

где последнее равенство вытекает из того, что  $x_j R_{Sup(x_j t)}(t)$  и  $x_j t$  равны по модулю идеала  $Span(Sup(x_j t))$ .

Наконец, для любого  $i \in [m]$  имеет место  $|J_i(A)| \geq \ell$  (поскольку  $f_i$   $\ell$ -иммунен), следовательно  $Sup(1) = \emptyset$  и  $R(1) = 1$ .

Теорема 3.8 полностью доказана. ■

Доказанная в теореме 3.8 оценка неприменима в случае, когда  $c$  – небольшая константа (например,  $c < 1$ ). Мы покажем в разделе 4.1, что для достаточно больших постоянных значений  $s$  существуют “хорошие” расширители (для которых коэффициент расширения  $c$  близок к  $s$ ), но для малых  $s$  вопрос о сложности системы (4) остается открытым даже для случайных матриц. В этой ситуации нам удалось доказать нижние оценки только в частном случае, когда все  $f_i$  имеют максимальную иммунность  $\ell = s$  (нетрудно видеть, что класс полиномов максимальной иммунности в точности состоит из полиномов вида  $\alpha \cdot \chi_{\vec{z}}(\vec{v})$ ,  $\alpha \in \mathbb{F}^*$ ).

**Теорема 3.13** Пусть матрица  $A$  является  $(r, s, c)$ -расширителем и  $\epsilon^{(i)} \in \{0, 1\}^{X_i(A)}$ . Тогда всякое опровержение системы  $\{\chi_{\epsilon^{(i)}}(X_i(A)) \mid i \in [m]\}$  в полиномиальном исчислении обязано иметь степень, превышающую  $(rc/2)$ .

**Доказательство.** Аналогично доказательству теоремы 3.8, с той разницей, что в данном частном случае формулировка теоремы 3.1 может быть усилена, в то время как доказательство становится тривиальным:

**Лемма 3.14** Предположим, что  $\vec{y}, \vec{v}, \vec{z}$  образуют разбиение множества переменных  $\{x_1, \dots, x_n\}$ ;  $\vec{P} = \vec{P}(\vec{y}, \vec{v})$ ,  $Q = Q(\vec{v}, \vec{z})$  – полиномы, зависящие от переменных  $\vec{y} \cup \vec{v}$ ,  $\vec{v} \cup \vec{z}$  соответственно, и пусть известно, что  $Q$  делится на  $(z - \epsilon)$  для некоторых  $z \in \vec{z}$ ,  $\epsilon \in \{0, 1\}$ . Пусть терм  $t(\vec{y}, \vec{v})$ , не содержащий  $z$ -переменных, приводим по модулю идеала  $Span(\vec{P}, Q)$  по отношению к некоторому фиксированному допустимому порядку. Тогда терм  $t$  также приводим по модулю  $Span(\vec{P})$  по отношению к тому же порядку.

**Доказательство.** Рассмотрим произвольный полином  $f$  такой, что  $\vec{P}, Q \models f$  и  $t = LT(f)$ . Применяв подстановку  $z = \epsilon$ , мы получим  $\vec{P}|_{z=\epsilon}, Q|_{z=\epsilon} \models f|_{z=\epsilon}$ . Поскольку  $\vec{P}$  не зависит от  $z$  и  $Q|_{z=\epsilon} = 0$ , имеем  $\vec{P} \models f|_{z=\epsilon}$ , и  $t = LT(f|_{z=\epsilon})$ . ■

Теперь мы определим оператор  $R$  тем же способом, как и в определении 3.10, но на этот раз мы будем использовать другое отношение вывода (следует обратить внимание на то, что данное отношение на каждом шаге выводит множество строк вместо одной строки):

**Определение 3.15** Для терма  $t$  определим следующее отношение вывода  $\vdash_t$  на множестве  $[m]$  всех строк матрицы  $A$ :

$$I \vdash_t I_1 \equiv |I_1| \leq r/2 \wedge \partial_A(I_1) \subseteq \left[ \bigcup_{i \in I} J_i(A) \cup J(t) \right]. \quad (9)$$

Носителем  $Sup(t)$  терма  $t$  назовем замыкание пустого множества строк относительно отношения выводимости  $\vdash_t$ . Наконец, положим  $R(t) \stackrel{\text{def}}{=} R_{Span(Sup(t))}(t)$ .

**Лемма 3.16** Для произвольного терма  $t$  такого, что  $\deg(t) \leq (cr/2)$ , имеет место  $|Sup(t)| \leq r/2$ .

**Доказательство.** Предположим противное. Тогда существует последовательность множеств  $I_1, \dots, I_2, \dots$  такая, что  $I_1 \cup \dots \cup I_{\nu-1} \vdash_t I_\nu$  и  $|\cup_\nu I_\nu| > r/2$ . Пусть  $k$  - наименьший индекс, для которого  $|\bigcup_{\nu=1}^k I_\nu| > r/2$ . Тогда, очевидно,  $|\bigcup_{\nu=1}^k I_\nu| \leq r$  (поскольку  $|I_\nu| \leq r/2$ ). Таким образом,  $|\partial_A(\bigcup_{\nu=1}^k I_\nu)| > (rc/2)$ . С другой стороны, из (9) следует, что любой новый граничный элемент, получающийся путем применения  $\vdash_t$  обязан принадлежать  $J(t)$ , поэтому  $\partial_A(\bigcup_{\nu=1}^k I_\nu) \subseteq J(t)$ . Полученное противоречит предположению  $\deg(t) \leq (cr/2)$ , что и доказывает лемму 3.16. ■

Аналог леммы 3.12 выглядит следующим образом.

**Лемма 3.17** Предположим, что  $t$  - произвольный терм и  $I$  - множество строк такое, что  $I \supseteq Sup(t)$  and  $|I| \leq r/2$ . Тогда

$$R_{Span(I)}(t) = R_{Span(Sup(t))}(t).$$

**Доказательство.** Поскольку  $Sup(t) \not\vdash_t I \setminus Sup(t)$ , из (9) следует, что существует некоторая строка  $i \in I \setminus Sup(t)$  содержащая элемент из  $\partial_A(I) \setminus J(t)$ .

Удалим эту строку используя лемму 3.14. Продолжая рекурсивно этот процесс удаления, мы постепенно избавимся от всех аксиом из  $I \setminus Sup(t)$ . ■

Оставшаяся часть доказательства проходит так же, как в доказательстве теоремы 3.8. ■

## 4 Приложения

В этом разделе мы опишем некоторые конкретные нижние оценки, которые доказываются с использованием результатов из раздела 3.

### 4.1 Конструкция расширителей

В работе [CS88] авторы определяют понятие разреженного гиперграфа, которое на нашем языке (строки соответствуют ребрам, столбцы – вершинам) выглядит следующим образом:  $(m \times n)$  0-1 матрица  $A$  является  $(x, y)$ -разреженной если для любого  $J \subseteq [n]$  такого, что  $|J| \leq xn$  имеет место  $|\{i \in [m] \mid J_i(A) \subseteq J\}| \leq y \cdot |J|$ . Также в этой работе была установлена (в неявном виде, для случая  $c = 1/2$ ) следующая связь между разреженностью и расширением (*union bound*), которая позже используется в работах [BP96, VKPS98, ABRW00]: любая  $(m \times n)$   $\left(\frac{r(k+c)}{2n}, \frac{2}{k+c}\right)$ -разреженная матрица, каждая строка которой содержит ровно  $k$  единиц, является  $(r, k, c)$ -расширителем для произвольных параметров  $r, k, c$ .

В [CS88, лемма 1] было приведено достаточное условие для того, чтобы случайная  $(\Delta n \times n)$  матрица (содержащая в каждой строке  $k$  единиц) была  $(x, y)$ -разреженной. Авторы рассмотрели лишь случай, когда параметры  $k, y, \Delta$  (последний обозначается в [CS88] через  $c$ ) являются фиксированными константами. Нам потребуется простое обобщение их леммы:

*Пусть  $k$  – фиксированное целое,  $y = y(n)$  – произвольный вещественный параметр такой, что  $(k - 1)y > 1$  и  $\Delta = \Delta(n)$  – произвольный целочисленный параметр, удовлетворяющий*

$$\Delta = o\left(n^{(k-1)y^{-1}}\right). \quad (10)$$

Тогда случайная  $(\Delta n \times n)$  матрица, в которой каждая строка имеет в точности  $k$  единиц, является  $(\Omega(\Delta^{-y/((k-1)y-1)}, y)$ -разреженной с вероятностью  $1 - o(1)$ .

Доказательство дословно повторяет доказательство леммы 1 в [CS88], необходимо лишь изменить оценки  $f(n), g(n)$  на

$$f(n) \stackrel{\text{def}}{=} e \left( \frac{e}{y} \right)^y \cdot n^{-((k-1)y-1)/2} \cdot \Delta^{y/2},$$

$$g(n) \stackrel{\text{def}}{=} \left( n \cdot \Delta^{-1/(k-1-y^{-1})} \right)^{1/2}.$$

Требуемая асимптотика  $f(n) \rightarrow 0, g(n) \rightarrow \infty$  следует тогда из (10).

Собирая все воедино и полагая  $y \stackrel{\text{def}}{=} \frac{2}{k+c}$ , мы имеем:

**Лемма 4.1** Пусть  $k \geq 3$  – фиксированное целое,  $0 < c = c(n) < k - 2$  – произвольный вещественный параметр и  $\Delta = \Delta(n)$  – произвольный целый параметр, удовлетворяющий  $\Delta = o(n^{(k-c-2)/2})$ . Тогда случайная  $(\Delta n \times n)$  матрица  $A$ , в которой каждая строка  $J_i(A)$  выбирается из всех  $\binom{n}{k}$   $k$ -подмножеств  $[n]$  равномерно и независимо является  $(\Omega(\frac{n}{\Delta^{2/(k-c-2)}}), k, c)$ -расширителем с вероятностью  $1 - o(1)$ .

Обратимся теперь к одной явной конструкции хороших расширителей. Для неориентированного графа  $G = (V, E)$  и  $r \geq 1$  положим

$$c_E(r, G) \stackrel{\text{def}}{=} \min_{|U| \leq r} \frac{e(U, V - U)}{|U|},$$

где  $e(U, W)$  – число ребер между  $U$  и  $W$ . Данная характеристика является незначительным обобщением коэффициента реберного расширения  $c_E(G) = c_E(|V|/2, G)$ , изучавшегося ранее в теории графов (см., например, [Alo98], а также приводимый там список литературы). Ясно, что матрица инцидентности  $A_G$  графа  $G$  является  $(r, d(G), c_E(r, G))$ -расширителем для произвольного  $r$  (ср. [ABRW00, пример 4]), где  $d(G)$  – максимальная степень вершин.

Предположим теперь, что  $G$  –  $d$ -регулярный граф. Тогда, очевидно,  $c_E(r, G) = d - \max_{|U| \leq r} ad(G|_U)$ , где  $G|_U$  – индуцированный на  $U$  подграф и  $ad$  – средняя степень. В [BCS78] доказывается следующая оценка данной величины в терминах второго собственного значения  $\lambda_2(G)$  графа  $G$ :

$$ad(G|_U) \leq \frac{|U|(d - \lambda_2(G))}{|V|} + \lambda_2(G).$$

Отсюда следует

$$c_E(r, G) \geq d \left( 1 - \frac{r}{|V|} \right) - \lambda_2(G).$$

Напомним, что *графы Рамануджана* – это  $d$ -регулярные графы  $G$ , для которых  $\lambda_2(G) \leq 2\sqrt{d-1}$ ; явные конструкции подобных графов приводятся в [LPS88, Mar88]. Подводя итог вышесказанному, имеет место:

**Лемма 4.2** *Матрица инцидентности произвольного  $d$ -регулярного графа Рамануджана  $G$  на  $n$  вершинах является  $(r, d, d(1 - r/n) - 2\sqrt{d-1})$ -расширителем для любого значения  $r > 0$ .*

## 4.2 Цейтиновские тавтологии: булев случай

Цейтиновские тавтологии представляют собой невыполнимые КНФ, которые выражают базовый комбинаторный принцип, утверждающий, что сумма степеней всех вершин в произвольном графе четна. Эти тавтологии были впервые использованы Цейтиным [Цей68] для доказательства первой сверхполиномиальной нижней оценки на размер опровержений в некотором ограниченном подклассе резолюций (в регулярных резолюциях).

В последующих работах [Gri98, BGIP99, BI99] авторы изучали трудность цейтиновских тавтологий для полиномиального исчисления. Это исследование существенно использовало тот факт, что данные тавтологии могут быть записаны в виде биномиальных идеалов. В этом случае аргументы, предложенные в [BGIP99] (и впоследствии упрощенные в [BI99]) позволяют показать, что любое опровержение цейтиновских тавтологий в полиномиальном исчислении имеет степень  $\Omega(n)$ .

В работе [BGIP99] авторы обобщают принцип Цейтина на случай, когда каждая вершина графа содержит функцию  $MOD_p$  (и после этого используют его для получения нижних оценок на степень вывода принципа  $Count_p$ ). В этом случае определение в терминах потоков на графе неформально утверждает следующее: каждому ориентированному ребру  $e$  соответствует переменная  $x_e$ , принимающая значения из множества  $\{0, \dots, p-1\}$ ; интуитивный смысл  $x_e$  – это количество некоторой “субстанции”, которое протекает по ребру  $e$ . Принцип Цейтина  $\text{mod}_p$  утверждает, что общий суммарный поток по всем вершинам равняется 0  $\text{mod}_p$ .

Данное определение естественным образом обобщает обычные цейтиновские тавтологии  $\text{mod}_2$ . В [BGIP99] была доказана нижняя оценка

$\Omega(n)$  на степень вывода этих тавтологий в варианте полиномиального исчисления, в котором соотношения  $x_i^2 - x_i$  (постулированные в нашем определении  $S_n(\mathbb{F})$ ) ослабляются до  $x_i^p - x_i$ . Авторы также отметили, что цейтиновские тавтологии  $\text{mod}_p$  можно определить и в обычном булевом случае, если продублировать каждое ребро в остовном графе  $p$  раз. В настоящей работе мы предлагаем иное определение, которое представляется нам более естественным и не использует дополнительных конструкций.

В нашем варианте переменная  $x_e$ , записанная на ориентированном ребре  $e$  может иметь только булевы значения 0 и 1. Имеются две различные константы  $F_0$  и  $F_1$  из  $\{0, \dots, p-1\}$ , которые определяют размер потока вдоль ребра  $e$  в случае, если  $x_e$  равно 0 и 1 соответственно. Легко показать (путем применения аффинного преобразования), что конкретные значения констант не играют большой роли; для определенности положим  $F_0 := 0$ ,  $F_1 := 1$ .

**Определение 4.3 (Принцип Цейтина  $\text{mod}_p$ )** Пусть  $G$  – конечный ориентированный граф, и  $\sigma : V(G) \rightarrow \{0, \dots, p-1\}$  – произвольная функция. Поставим в соответствие отдельную булеву переменную  $x_e$  каждому ориентированному ребру  $e \in E(G)$ . Для  $v \in V(G)$  обозначим через  $MOD_p(G, \sigma, v)$  следующий предикат:

$$\sum_{\{w \mid \langle w, v \rangle \in E\}} x_{\langle w, v \rangle} - \sum_{\{w \mid \langle v, w \rangle \in E\}} x_{\langle v, w \rangle} = \sigma(v) \pmod{p}.$$

$\text{mod}_p$  Принцип Цейтина, соответствующий данным  $G$  и  $\sigma$  определяется как

$$T_p(G, \sigma) \stackrel{\text{def}}{=} \bigwedge_{v \in V(G)} \{MOD_p(G, \sigma, v)\}.$$

Легко видеть, что класс  $T_2(G, \sigma)$  совпадает с обычными цейтиновскими тавтологиями. Мы докажем, что для графов  $G$  с достаточно хорошим реберным расширением всякое опровержение  $T_p(G, \sigma)$  в полях  $\mathbb{F}$  с  $\text{char } \mathbb{F} \neq p$  имеет большую степень.

**Теорема 4.4** Булева функция от  $d$  переменных, принимающая значение 1 на наборе  $\alpha_1, \dots, \alpha_d$  тогда и только тогда, когда  $\sum_{j=1}^d \epsilon_j \alpha_j \equiv \sigma \pmod{p}$ , где  $\epsilon_j \in \{\pm 1\}$  и  $\sigma \in \{0, 1, \dots, p-1\}$  – произвольные параметры, является  $\lfloor \frac{d}{4(p-1)} \rfloor$ -иммунной над любым полем  $\mathbb{F}$  характеристики, отличной от  $p$ .

**Доказательство.** Предположим без ограничения общности, что  $\epsilon_1 = \epsilon_2 = \dots = \epsilon_{d_1} = 1$ ,  $\epsilon_{d_1+1} = \dots = \epsilon_d = -1$  и  $d_1 \geq d/2$ . Используя следствие 2.6(1), легко видеть, что из основного результата [Gre00] (теорема 3.4) следует, что для любого  $\sigma \in \{0, 1, \dots, p-1\}$ ,  $MOD_{p,\sigma}(x_1, \dots, x_{d_1})$  является  $\lfloor \frac{d_1}{2(p-1)} \rfloor \geq \lfloor \frac{d}{4(p-1)} \rfloor$ -иммунной над любым полем  $\mathbb{F}$  с  $\text{char } \mathbb{F} \notin \{0, p\}$ . Согласно следствию 2.6(2) эта оценка обобщается на поля  $\mathbb{F}$  характеристики 0. Теорема 4.4 следует теперь из леммы 2.7(2), примененной к  $V \stackrel{\text{def}}{=} \{x_{d_1+1}, \dots, x_d\}$ . ■

На основании теоремы 3.8, леммы 4.2 и теоремы 4.4 имеет место

**Следствие 4.5** *Для любого фиксированного простого  $p$  существует константа  $d_0 = d_0(p)$  такая, что имеет место следующее. Если  $d \geq d_0$ ,  $G$  –  $d$ -регулярный граф Рамануджана на  $n$  вершинах (с произвольной ориентацией ребер) и  $\text{char } \mathbb{F} \neq p$ , то для любой функции  $\sigma$  всякое опровержение  $T_p(G, \sigma)$  в полиномиальном исчислении над полем  $\mathbb{F}$  имеет степень  $\Omega(dn)$ .*

### 4.3 Случайные $k$ -КНФ в характеристике 2

Интересным тестом для пропозициональной системы доказательств является проверка того, насколько она эффективна для случайной тавтологии.

**Определение 4.6 (Случайные  $k$ -КНФ)** Пусть  $\mathcal{F} \sim \mathcal{F}_k^{n,\Delta}$  обозначает, что  $\mathcal{F}$  – случайная  $k$ -КНФ от  $n$  переменных и  $\Delta \cdot n$  дизъюнкций, выбранных (с повторением) независимо и равномерно из множества всех  $\binom{n}{k} \cdot 2^k$  дизъюнкций.  $\Delta$  называется *плотностью дизъюнкций*.

В [CS88] было установлено, что случайные 3-КНФ от  $n$  переменных и  $\Delta \cdot n$  дизъюнкций требуют экспоненциального опровержения в резолюциях для произвольной константы  $\Delta$ . В [BI99] было доказано, что опровержение в полиномиальном исчислении случайной 3-КНФ требует степени  $\Omega(n)$  для любого поля  $\mathbb{F}$  с  $\text{char } \mathbb{F} \neq 2$  при условии, что плотность  $\Delta = \Delta(n)$  достаточно мала. Авторы последней работы использовали предложенную в [BGIP99] биномиальную технику и доказанный в [CS88] факт, что случайная КНФ обладает свойствами “хорошего” расширителя. Авторы [BI99] также высказали предположение, что та же

оценка на степень справедлива для 3-КНФ над полями  $\mathbb{F}$  характеристики  $\text{char } \mathbb{F} = 2$ .

Мы даем положительный ответ на этот вопрос. Именно, на основании теоремы 3.13 и леммы 4.1 с  $c = 1/\ln(\Delta + 2)$  мы немедленно получаем

**Следствие 4.7** Пусть  $\mathcal{F} \sim \mathcal{F}_k^{n,\Delta}$ , где  $k \geq 3$  – фиксированное целое и  $\Delta = \Delta(n)$  – произвольный параметр, удовлетворяющий  $\Delta \leq o(n^{(k-2)/2})$ . Тогда любое опровержение  $\mathcal{F}$  в полиномиальном исчислении над произвольным полем  $\mathbb{F}$  имеет степень  $\Omega\left(\frac{n}{\Delta^{2/(k-2)} \cdot \log \Delta}\right)$  с вероятностью  $1 - o(1)$ .

#### 4.4 Тривиализуемые функции и потоковые тавтологии

В этом разделе мы опишем широкий класс *тривиализуемых* функций и покажем, что они имеют хорошую иммунность. После этого мы определим аналог цейтиновских тавтологий в характеристике ноль, в котором каждая вершина содержит линейное неравенство над  $\mathbb{R}$ . Принцип будет утверждать, что поток не может быть положительным во всех вершинах графа. Мы назовем это семейство *потокowymi тавтологиями*.

**Определение 4.8** Назовем булеву функцию  $f$   $\ell$ -тривиализуемой если для любого подмножества переменных  $S \subseteq \{x_1, \dots, x_n\}$ , удовлетворяющего  $|S| < \ell$ , существует подстановка  $\rho$ , которая оставляет переменные из  $S$  неназначенными и такая, что  $f|_\rho = 1$ . Полином называется  $\ell$ -тривиализуемым, если таковой является характеристическая функция множества его корней на  $\{0, 1\}^n$ .

Иными словами, полином  $f \in S_n(\mathbb{F})$  является  $\ell$ -тривиализуемым если и только если для любого выбора  $n - \ell + 1$  переменных мы можем сделать его равным нулю путем применения некоторой подстановки, назначая этим переменным значения 0 или 1. Оказывается, что тривиализуемые полиномы имеют высокую иммунность.

**Теорема 4.9** Любой  $\ell$ -тривиализуемый полином  $f$  является  $\ell$ -иммунным.

**Доказательство.** Предположим, что  $f \not\equiv g$  и  $\deg(g) < \ell$ . Выберем произвольный терм максимальной степени  $t$ , содержащийся в  $g$ . Пусть

$S \stackrel{\text{def}}{=} \text{Vars}(t)$ . По определению  $\ell$ -тривиализуемого полинома существует подстановка  $\rho$ , которая отображает  $f$  (и, следовательно,  $g$ ) в 0 и не трогает  $t$ . Но  $g|_\rho$  по прежнему содержит  $t$  и, следовательно, отличен от нуля. Полученное противоречие доказывает теорему 4.9. ■

Хорошим примером тривиализуемых тавтологий служат пороговые функции  $\sum_{i=1}^n x_i > k$ . В частности, функция голосования  $MAJ_n$ , определяемая предикатом  $\sum_{i=1}^n x_i > n/2$ , является  $n/2$ -тривиализуемой. Чтобы в этом убедиться, предположим, что задано подмножество переменных  $S$  мощности  $|S| < n/2$ . Назначив оставшимся переменным значение 1, мы отобразим функцию в 1. Таким образом, мы показали, что  $MAJ_n$  является  $n/2$ -иммунной над любым полем (другое, более прямое доказательство этого результата может быть получено из доказательства [Tsa96, теорема 4.1]).

Теперь мы готовы определить аналог принципа Цейтина в характеристике 0. Напомним, что в случае характеристики  $p$  имеется ориентированный граф  $G$  с булевыми переменными, соответствующими ребрам, и аксиомы, утверждающие, что в каждой вершине  $v$  поток равен  $\sigma(v) \pmod p$ . Если вместо того, чтобы фиксировать поток в каждой вершине по модулю  $p$  мы потребуем, чтобы он был положительным, то получим *потокосые тавтологии*.

**Определение 4.10 (Потокосые тавтологии)** Пусть  $G$  – конечный ориентированный граф. Поставим в соответствие каждому направленному ребру  $e \in E(G)$  отдельную булеву переменную  $x_e$ . Для  $v \in V(G)$  обозначим через  $PosFlow(G, v)$  следующий предикат:

$$\sum_{\{w | \langle w, v \rangle \in E\}} (1 - 2x_{\langle w, v \rangle}) > \sum_{\{w | \langle v, w \rangle \in E\}} (1 - 2x_{\langle v, w \rangle}).$$

*Потокосый принцип* на  $G$  определяется как формула

$$Fl(G) \stackrel{\text{def}}{=} \bigwedge_{v \in V(G)} PosFlow(G, v).$$

Легко видеть, что с точностью до отрицания некоторых переменных  $PosFlow(G, v)$  совпадает с функцией голосования от  $d(v)$  переменных, и, следовательно, является  $d(v)/2$ -тривиализуемой. Таким образом, согласно теореме 4.9 и лемме 4.2 имеет место

**Следствие 4.11** Если  $G$  –  $d$ -регулярный граф Рамануджана на  $n$  вершинах степени  $d \geq 255$  с произвольной ориентацией ребер, то любое опровержение  $Fl(G)$  в полиномиальном исчислении над произвольным полем имеет степень  $\Omega(dn)$ .

## 4.5 Расширенный принцип Дирихле

В этом разделе мы докажем нижние оценки на степень опровержения расширенного принципа Дирихле, определенного в [BW99].

Принцип Дирихле с  $m$  кроликами и  $n$  клетками<sup>1</sup> утверждает, что при условии  $m > n$  не существует инъективного отображения из  $[m]$  в  $[n]$ . Данное предложение может быть описано формулой, зависящей от  $mn$  переменных  $x_{ij}$ , где  $x_{ij} = 1$  означает, что  $i$  отображается в  $j$ .

**Определение 4.12** Обозначим через  $RHP_n^m$  множество следующих дизъюнкций:

- $P_i \stackrel{\text{def}}{=} \bigvee_{1 \leq j \leq n} x_{ij}$  for  $1 \leq i \leq m$
- $H_{i,i'}^j \stackrel{\text{def}}{=} \bar{x}_{ij} \vee \bar{x}_{i'j}$  for  $1 \leq i < i' \leq m, 1 \leq j \leq n$ .

Проблема с данной классической формализацией принципа Дирихле заключается в том, что дизъюнкции  $P_i$  не могут быть выражены полиномами малой степени. Поэтому в случае полиномиального исчисления обычно рассматривают более сильную версию  $RHP_n^m$ , в которой никакой кролик не может “сидеть” одновременно в двух клетках (что, в частности, позволяет заменить большие дизъюнкции линейными функциями – см., например, [Raz98]). Существует, однако, еще один способ выразить  $RHP_n^m$  с помощью семейства многочленов малой степени, который представляется, быть может, даже более естественным с точки зрения модели, изучаемой в [ABRW00] и в настоящей работе.

**Определение 4.13 ([BW99])** Для булевой функции  $f(\vec{x})$  назовем *недетерминированным расширением*  $f$  произвольную функцию  $g(\vec{x}, \vec{y})$  такую, что  $f(\vec{x}) = 1 \iff \exists y g(\vec{x}, \vec{y}) = 1$ . При этом  $\vec{x}$ -переменные

---

<sup>1</sup>в англоязычной литературе при обсуждении принципа Дирихле вместо кроликов и клеток традиционно используются голуби и норки

называются *исходными* переменными, а  $\vec{y}$ -переменные называются *дополнительными* переменными.

Принцип  $ERHP_n^m$  получается из  $RHP_n^m$  путем замены каждой аксиомы  $P_i$  на произвольное недетерминированное расширение, задаваемое некоторой КНФ формулой  $EP_i$ , причем для разных строк эти КНФ используют попарно различные дополнительные переменные  $\vec{y}_i$ .

Теперь мы можем формализовать принцип Дирихле как семейство полиномов, заменив каждую дизъюнкцию  $C$  из  $ERHP_n^m$  на соответствующий полином  $p_C$ . Так как  $EP_i$  могут быть выбраны в виде 3-CNF, данный подход полностью решает все проблемы со степенью аксиом.

Основной результат этого раздела – новое доказательство следующей теоремы. Преимущество этого доказательства заключается в том, что оно не использует никаких специальных трудоемких вычислений.

**Теорема 4.14** *Для произвольного  $m = O(n)$  любое опровержение принципа  $ERHP_n^m$  в полиномиальном исчислении имеет степень  $\Omega(n)$ .*

#### Доказательство.

Рассмотрим произвольное опровержение  $\mathcal{P}$  принципа  $ERHP_n^m$ . Фиксируем  $m \times n$   $(r, s, c)$ -расширитель  $A$  с постоянными  $s, c$  и  $r = \Omega(n)$  (например, мы можем выбрать случайный расширитель из леммы 4.1). Ограничим теперь принцип Дирихле так, что  $i$ -ый кролик может сидеть только в клетках  $j \in J_i(A)$ . Формально, мы применяем к  $\mathcal{P}$  подстановку  $\rho$ , которая присваивает значения  $x_{ij} = 0$  для всех  $j \notin J_i(A)$ .

Наша следующая задача – удалить из доказательства все вхождения дополнительных переменных. Для этого рассмотрим  $i$ -ую аксиому  $EP_i|_\rho$  в выводе  $\mathcal{P}|_\rho$ . По определению,  $P_i(\vec{x}_i) = 1 \iff \exists \vec{y}_i EP_i(\vec{x}_i, \vec{y}_i) = 1$ . Ясно, что зависимость  $\vec{y}_i$  от  $\vec{x}_i$  может быть сделана явной в том смысле, что существуют функции  $\vec{h}_i(\vec{x}_i)$ , для которых имеет место  $P_i|_\rho(\vec{x}_i) = 1 \iff (EP_i)|_\rho(\vec{x}_i, \vec{h}_i(\vec{x}_i)) = 1$ . Поскольку мы фиксировали значения всех переменных кроме  $s, \vec{h}_i$  можно также выбрать зависящими не более чем от  $s$  переменных. Заменим теперь в доказательстве  $\mathcal{P}|_\rho$  все дополнительные переменные  $y_{ik} \in \vec{y}_i$  на полиномы  $1 - p_{h_{ik}}$ . Ясно, что степень  $\mathcal{P}|_\rho$  увеличится не более, чем в  $s$  раз. Таким образом, чтобы завершить доказательство теоремы, достаточно оценить степень этого нового вывода.

Легко видеть, что исходные полиномы, соответствующие аксиомам  $EP_i$ , отобразятся в полиномы, семантически эквивалентные дизъюнкциям  $\bigvee_{j \in J_i(A)} x_{ij}$ . Без потери общности можно предположить, что они

перейдут в полиномы  $f_i \stackrel{\text{def}}{=} \prod_{j \in J_i(A)} (1 - x_{ij})$  и, таким образом, для системы

$$\{f_1, \dots, f_m\} \cup \{x_{ij} \cdot x_{i'j} \mid i \neq i', j \in J_i(A) \cap J_{i'}(A)\}$$

мы имеем опровержение в полиномиальном исчислении степени, не превышающей  $s \cdot \deg(\mathcal{P})$ .

Для завершения доказательства нам потребуется многозначная версия теоремы 3.13 (ср. [ABRW02]). А именно, предположим, что вместо булевых переменных  $x_j$  имеются многозначные переменные  $\hat{x}_j \in \{1, \dots, d\}$ , представленные кортежами булевых переменных  $\vec{x}_j = (x_{1j}, \dots, x_{dj})$  с подразумеваемым семантическим смыслом  $x_{\ell j} \stackrel{\text{def}}{=} (\hat{x}_j = \ell)$ . Как и в булевом случае, для набора  $\vec{c} \in \{1, \dots, d\}^k$  положим  $\chi_{\vec{c}}(\vec{x}_1, \vec{x}_2, \dots, \vec{x}_k) \stackrel{\text{def}}{=} \prod_{j=1}^k (1 - x_{c_j, j})$ .

Предположим, что помимо уравнений  $f_1(\vec{x}_1, \dots, \vec{x}_n) = \dots = f_m(\vec{x}_1, \dots, \vec{x}_n) = 0$  того же вида, что и раньше, наша система содержит также аксиомы  $x_{\ell j} x_{\ell' j} = 0$  для всех  $j \in [n], 1 \leq \ell < \ell' \leq d$ . Мы слегка подправим определение 3.9 для многозначного случая следующим образом:

$$J(t) \stackrel{\text{def}}{=} \{j \mid t \text{ имеет непустое пересечение с } \vec{x}_j\}$$

и

$$\text{Span}(I) \stackrel{\text{def}}{=} \text{Span}(\{f_i \mid i \in I\} \cup \{x_{\ell j} x_{\ell' j} \mid j \in \bigcup_{i \in I} J_i(A), 1 \leq \ell < \ell' \leq d\}).$$

Тогда аналог теоремы 3.13 в данной многозначной модели будет выглядеть так:

*Пусть матрица  $A$  является  $(r, s, c)$ -расширителем, и пусть  $\vec{c}^{(i)} \in \{1, \dots, d\}^{X_i(A)}$ . Тогда всякое опровержение системы  $\{\chi_{\vec{c}^{(i)}}(X_i(A)) \mid i \in [m]\} \cup \{x_{\ell j} x_{\ell' j} \mid j \in [n], 1 \leq \ell < \ell' \leq d\}$  в полиномиальном исчислении обязано иметь степень, превышающую  $(rc/2)$ .*

В этой форме теорема 3.13 может быть применена к нашему случаю (многозначные переменные  $\hat{x}_j$  принимают значения  $\{i \in [m] \mid j \in J_i(A)\}$ ). Теорема 4.14 доказана. ■

## 4.6 Соотношение между устойчивостью и иммунностью

В этом разделе мы обсудим соотношение между критерием трудности, рассмотренным в [ABRW00] и нашим критерием. Мы покажем, что лю-

бая  $(s - k)$ -устойчивая функция (см. определение ниже) является также  $\omega(1)$ -иммунной в полях характеристики 0 ( $k = \text{const}$ ,  $s \rightarrow \infty$ ). Данная оценка довольно слабая, однако даже достаточно большая постоянная иммунность позволяет получить нетривиальные нижние оценки на степень вывода в полиномиальном исчислении.

**Определение 4.15 ([ABRW00])** Булева функция  $f$  называется  $\ell$ -устойчивой если любая подстановка  $\rho$  такая, что  $f|_{\rho} = \text{const}$  удовлетворяет  $|\rho| \geq \ell$ .

Легко видеть, что это понятие инвариантно относительно взятия отрицания. Для того, чтобы сравнить его с неинвариантной иммунностью, назовем функцию  $f$   $\ell$ -полуустойчивой если  $f|_{\rho} \equiv 0$  влечет  $|\rho| \geq \ell$ . Таким образом, булева функция является  $\ell$ -устойчивой если и только если она и ее отрицание являются  $\ell$ -полуустойчивыми. По лемме 2.7(1) любая  $\ell$ -иммунная булева функция  $\ell$ -полуустойчива, следовательно, понятие иммунности является более сильным. Как видно из примера функции  $MOD_p$ , в положительной характеристике иммунность может быть гораздо более сильным ограничением, чем (полу)устойчивость.

В обратную сторону имеет место следующая оценка:

**Теорема 4.16** Пусть  $\text{char } \mathbb{F} = 0$  и  $k$  – фиксированная константа. Тогда любая  $(s - k)$ -полуустойчивая булева функция  $f$  от  $s$  переменных при  $s \rightarrow \infty$  имеет иммунность  $\omega(1)$ .

**Доказательство.** Согласно следствию 2.6(2), мы можем предположить без потери общности, что  $\mathbb{F} = \mathbb{Q}$ . Нам потребуется следующее классическое определение из теории Рамсея.

**Определение 4.17** Число Рамсея  $R_k(l_1, \dots, l_r)$  – это наименьшее  $n$  такое, что если все  $k$ -подмножества  $[n]$  раскрашены в  $r$  цветов, то всегда существует цвет  $\nu$  и  $l_{\nu}$ -подмножество  $[n]$ , все  $k$ -подмножества которого имеют цвет  $\nu$ .

Пусть  $N_k(d)$  – наименьшее  $s$  такое, что для каждого отличного от нуля полинома  $g \in \mathbb{Q}[x_1, \dots, x_s]$  степени  $\deg(g) \leq d$  существует подстановка  $\rho$  такая, что  $|\rho| \leq s - k - 1$  и  $g|_{\rho}$  не имеет  $(0 - 1)$  корней. Таким образом, это обратная функция к той, которую мы изучаем: а именно, если  $g$  – семантическое следствие полинома  $p_f$  (где  $f$  –  $(s - k)$ -полуустойчивая

булева функция), то  $N_k(\deg(g)) > s$ .  $N_k(d)$  монотонно неубывает, и нам достаточно показать, что  $\forall d N_k(d) < \infty$ . Ясно, что  $N_k(0) = k + 1$ . Наш результат получается из следующей рекурсивной оценки:

$$N_k(d) \leq R_d(2^{k+1}d, 2^{k+1}d, N_k(d-1)).$$

Для ее доказательства предположим, что  $s \geq R_d(2^{k+1}d, 2^{k+1}d, N_k(d-1))$ , и пусть  $\deg(g) \leq d$ . Раскрасим все  $d$ -подмножества  $[s]$  в три цвета,  $+$ ,  $-$ ,  $0$ , согласно знаку коэффициента соответствующего термина в  $g$ . Обозначим  $m = 2^{k+1}d$ . В силу определения чисел Рамсея возможны два случая.

**Случай 1.** Для некоторых  $m$  переменных (например,  $x_1, \dots, x_m$ )  $g$  содержит все возможные термины  $x_I$  с  $I \in [m]^d$  с одним и тем же знаком  $+$  или  $-$ . Рассмотрим  $k+1$  переменную  $x_{m+1}, x_{m+2}, \dots, x_{m+k+1}$ . Если существует подстановка  $\rho$ , назначающая все переменные за исключением  $x_{m+1}, x_{m+2}, \dots, x_{m+k+1}$  и такая, что  $g|_\rho$  не имеет  $(0-1)$  корней, тогда наша рекурсивная оценка очевидно имеет место. В противном случае для любого назначения переменных  $\text{Vars}(g) \setminus \{x_{m+1}, x_{m+2}, \dots, x_{m+k+1}\}$  можно назначить оставшиеся переменные  $x_{m+1}, x_{m+2}, \dots, x_{m+k+1}$  таким образом, что  $g$  станет равной 0. Иными словами, по крайней мере одна из функций

$$g|_{(x_{m+1}=\epsilon_1, \dots, x_{m+k+1}=\epsilon_{k+1})}$$

равна 0 на выбранном назначении, что эквивалентно

$$\prod_{\vec{\epsilon} \in \{0,1\}^{k+1}} g|_{(x_{m+1}=\epsilon_1, \dots, x_{m+k+1}=\epsilon_{k+1})} = 0 \text{ в } S_s(\mathbb{Q}).$$

Это, однако, невозможно, так как все термины  $x_I$  с  $I \in [m]^d$  по-прежнему содержатся во всех  $g|_{(x_{m+1}=\epsilon_1, \dots, x_{m+k+1}=\epsilon_{k+1})}$  с одним и тем же знаком, и, таким образом, терм  $\prod_{i=1}^m x_i$  имеет в этом произведении коэффициент, отличный от нуля.

**Случай 2.** Для некоторых  $N_k(d-1)$  переменных (например,  $x_1, \dots, x_{N_k(d-1)}$ )  $g$  не содержит ни одного термина  $x_I$  с  $I \in [N_k(d-1)]^d$ . В этом случае достаточно просто применить любую подстановку к оставшимся переменным, которая не превратит  $g$  в тождественно нулевую функцию (но при этом уменьшит степень) и затем применить индуктивное предположение.

Теорема 4.16 доказана. ■

В соответствии с соглашением, принятым в разделе 2 (ср. определение 2.3), мы будем называть полином  $f$   $\ell$ -полуустойчивым, если таковой является характеристическая функция множества его корней.

**Теорема 4.18** *Для произвольных фиксированных целых  $k, \alpha$  существует целое  $s_0$  такое, что для любых  $s \geq s_0$ ,  $(r, s, s - \alpha)$ -расширителя  $A$  и  $(s - k)$ -полуустойчивых полиномов  $f_1, \dots, f_m$  над произвольным полем характеристики 0, удовлетворяющих  $\text{Vars}(f_i) \subseteq X_i(A)$ , всякое опровержение системы  $f_1 = \dots = f_m = 0$  в полиномиальном исчислении имеет степень  $\Omega(r)$ .*

Эта теорема следует из теорем 3.8 и 4.16. Используя конструкцию случайных расширителей из леммы 4.1, можно построить разнообразные семейства сложных тавтологий, основанные на  $(s - k)$ -полуустойчивых функциях.

## 5 Открытые вопросы

Наиболее интересным из числа оставшихся открытыми представляется вопрос о том, что можно сказать о системе (4) в случае малого коэффициента расширения  $c > 0$ ? Можно ли показать сложность этой системы при условии, что  $f_i$  имеют достаточную (но не полную!) иммунность; иными словами, возможно ли объединение наших теорем 3.8, 3.13 в одно общее утверждение?

Существует ли более сильное соотношение между устойчивостью и иммунностью, чем показанное в теореме 4.16?

## 6 Благодарности

Авторы признательны Яну Крайчеку за предложение применить развитые в данной работе методы к принципу Дирихле.

## Список литературы

- [ABRW02] M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Space complexity in propositional calculus. *SIAM Journal on Computing*, 31(4):1184–1211, 2002.

- [ABRW00] M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Pseudorandom generators in propositional complexity. In *Proceedings of the 41st IEEE FOCS*, 2000. Journal version to appear in *SIAM Journal on Computing*.
- [Alo98] N. Alon. Spectral techniques in graph algorithms. In C. L. Lucchesi and A. V. Moura, editors, *Lecture Notes in Computer Science* 1380, pages 206–215, Berlin, 1998. Springer-Verlag.
- [ABFR94] J. Aspnes, R. Beigel, M. Furst, and S. Rudich. The expressive power of voting polynomials. *Combinatorica*, 14(2):1–14, 1994.
- [BIKPP96] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower bounds on Hilbert’s Nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 73:1–26, 1996.
- [BKPS98] P. Beame, R. Karp, T. Pitassi, and M. Saks. On the complexity of unsatisfiability of random k-cnf formulas. In *Proceedings of the 30th ACM Symposium on Theory of Computing*, pages 561–571, 1998.
- [BP96] P. Beame and T. Pitassi. Simplified and improved resolution lower bounds. In *Proceedings of the 37th IEEE FOCS*, pages 274–282, 1996.
- [BP98] P. Beame and T. Pitassi. Propositional proof complexity: Past, present and future. Technical Report TR98-067, Electronic Colloquium on Computational Complexity, 1998.
- [BI99] E. Ben-Sasson and R. Impagliazzo. Random CNF’s are Hard for the Polynomial Calculus. In *Proceedings of the 40th IEEE FOCS*, pages 415–421, 1999.
- [BW99] E. Ben-Sasson and A. Wigderson. Short proofs are narrow - resolution made simple. In *Proceedings of the 31st ACM STOC*, pages 517–526, 1999.
- [BGIP99] S. Buss, D. Grigoriev, R. Impagliazzo, and T. Pitassi. Linear gaps between degrees for the Polynomial Calculus modulo distinct

- primes. In *Proceedings of the 31st ACM STOC*, pages 547–556, 1999.
- [BIKPRS96] S. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. Razborov, and J. Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computational Complexity* **6**(3) (1996/1997), 256–298.
- [BCS78] F. C. Bussemaker, D. M. Cvetković, and J. J. Seidel. Graphs related to exceptional root systems. In A. Hajnal and V. T. Sós, editors, *Combinatorics, Coll. Math. Soc. J. Bolyai, Vol. 18*, pages 185–191. North-Holland, Amsterdam, 1978.
- [CS88] V. Chvátal, E. Szemerédi. Many hard examples for resolution. *Journal of the ACM*, 35 (4):759–768, October 1988.
- [CEI96] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th ACM STOC*, 1996, 174–183.
- [Gre00] F. Green. A complex-number Fourier technique for lower bounds on the MOD- $m$  degree. *Computational Complexity*, 9(1):16–38, 2000.
- [Gri98] D. Grigoriev. Nullstellensatz lower bounds for Tseitin tautologies. In *Proceedings of the 39th IEEE FOCS*, 1998, 648–652.
- [Gri01] D. Grigoriev. Linear lower bounds on degrees of Postivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259:613–622, 2001.
- [IPS99] R. Impagliazzo, P. Pudlák, and J. Sgall. Lower bounds for the polynomial calculus and the Groebner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999.
- [Kra01] J. Krajíček. On the degree of ideal membership proofs from uniform families of polynomials over a finite field. *Illinois Journal of Mathematics*, 45(1):41–73, 2001.
- [LPS88] A. Lubotsky, R. Philips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8:261–277, 1988.

- [Мар88] Г. А. Маргулис. Явные теоретико-групповые конструкции комбинаторных схем и их применения в построении расширителей и концентраторов. *Проблемы передачи информации*, 24:51–60, 1988. English translation in *Problems of Information Transmission*, Vol. 24, pages 39–46.
- [Raz96] A. Razborov. Lower bounds for propositional proofs and independence results in Bounded Arithmetic. In F. Meyer auf der Heide and B. Monien, editors, *Proceedings of the 23rd ICALP, Lecture Notes in Computer Science*, 1099, pages 48–62, New York/Berlin, 1996. Springer-Verlag.
- [Raz98] A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7:291–324, 1998.
- [RR97] A. Razborov and S. Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997.
- [Tsa96] S.-C. Tsai. Lower bounds on representing Boolean functions as polynomials in  $\mathbb{Z}_m$ . *SIAM Journal on Discrete Mathematics*, 9:55–62, 1996.
- [Цей68] Г. С. Цейтин. О сложности вывода в исчислении высказываний. В сб. А. О. Слисенко (ред.), *Исследования по конструктивной математике и математической логике II; Записки научных семинаров ЛОМИ*, т. 8, стр. 234–259. Наука, Ленинград, 1968. Engl. translation: G. С. Tseitin, On the complexity of derivations in propositional calculus, in: *Studies in mathematics and mathematical logic, Part II*, ed. А. О. Slissenko, pp. 115–125.