Московский физико-технический институт
(Государственный университет)

Факультет управления и прикладной математики
Кафедра «Интеллектуальные системы»

ДИПЛОМНАЯ РАБОТА

«Тождества глубины 3 с многочленами»

Выполнила:
студентка 4 курса 974 группы
Иванова Алина Владиславовна

Научный руководитель:
к.ф-м.н., с.н.с. ВЦ РАН
Вялый Михаил Николаевич

Москва, 2013

Аннотация

В работе рассматриваются тождества с многочленами, заданные в виде схем глубины 3. Рассмотрен способ проверки на тождество при ограничении на верхний слой. Приведены оценки рангов тождеств глубины 3 для произвольного поля $\mathbb{F}$. Также в данной работе улучшены оценки для рангов простых минимальных тождеств и приведены примеры тождеств для доказательства нижних оценок.

Ключевые слова: *problem identity testing, depth-3 circuit, blackbox.*

1 Введение

Задача проверки тождества связана с классификацией полиномов по сложности вычисления. Входом задачи является многочлен над полем $\mathbb{F}$, заданный в специальном виде. На выходе требуется ответить, является ли исходный многочлен тождественно нулевым.

На данный момент известно несколько вероятностных алгоритмов для решения этой проблемы, но вопрос о существовании детерминированного полиномиального алгоритма остается открытым.

В работе используются арифметические схемы для представления полинома.

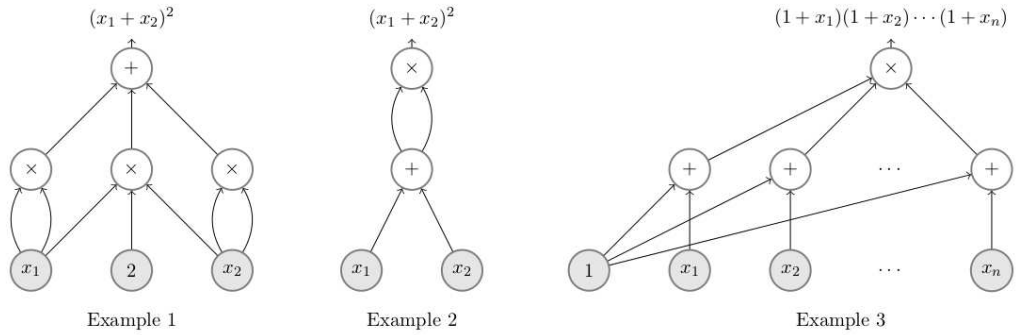

Рис. 1: Примеры схем

Стоит заметить, что по полиному схема восстанавливается не однозначным образом.

Арифметическая схема — ориентированный ациклический граф с одним стоком (называемый выходом). Каждая вершина-источник (вход) обозначена либо переменной x_i, либо элементом соответствующего поля $\mathbb{F}$. Каждый внутренний узел помечен знаком $+$ или $\times$, обозначающим аддитивные и мультипликативные выходы соответственно. Принято ранжировать данные узлы по слоям таким образом, чтобы в каждом слое были вершины одного типа.

Говорят, что схема вычисляет полином $f \in \mathbb{F}[x_1, \ldots, x_n]$, если выход вычисляет f. Схема называется формулой, если выходная степень в графе равна 1. Размером схемы называется количество узлов в ней. Глубина — это длина наибольшего пути от листового узла до стока. Степень схемы - формальная степень полинома (вычисляется рекурсивно).

Задача, рассматриваемая в данной работе, формулируется следующим образом: по данной схеме $\mathcal{C}$ над переменными $x_1, \ldots, x_n$ определить, является ли соответствующий полином тождественным нулем или нет. Несмотря на легкую формулировку, данная

проблема является на данной момент открытой. Теоретические оценки и связь с некоторыми важными задачами можно посмотреть в работах [4, 10–13].

Важным частным случаем данной задачи являются схемы глубины 3, которые и будут рассмотрены в этой работе. Несмотря на достаточно маленькое значение параметра, даже этот случай на данный момент является не разобранным. Стоит отметить, что для случая глубины 3 имеет смысл рассматривать лишь схемы вида $\Sigma\Pi\Sigma$, так как иначе схема сводится к достаточно простому случаю глубины 2. Схемы глубины 4 рассматриваются, например, в работе [3].

Подробный обзор задачи проверки тождеств проведен в работе [2]. Рассмотрены различные подходы к решению задачи: вероятностные алгоритмы, неадаптивные алгоритмы, и другие детерминированные алгоритмы.

Вероятностные алгоритмы рассматриваются в работах [1, 5, 8, 9]. Они решают поставленную задачу за полиномиальное время, но лишь с некоторой точностью. Поэтому наибольший интерес представляют детерминированные алгоритмы.

Основные результаты, произведенные в данной задаче, относятся к случаям глубины 3 с ограниченным верхним слоем. Это значит, что полином представляется в виде суммы произведений линейных форм, причем количество слагаемых в этой сумме $O(1)$. Это ограничение связано с тем, что во всех известных алгоритмах показатель k, равный количеству этих слагаемых, появляется в оценке сложности в показателе степени некоторого числа. Данный случай исследован в очень большом количестве работ, в том числе в данной работе так же будет рассмотрен именно этот частный случай.

Для случая глубины 3 с ограниченным верхним слоем был разработан алгоритм, описанный в работе [7]. Идея алгоритма, который использует локальные кольца, сильно отличается от тех, которые рассматриваются в этой работе. Его сложность зависит от k экспоненциально.

Случай $\mathbb{F} = \mathbb{Q}$ рассмотрен в работе [6].

Важным типом алгоритмов являются так называемые неадаптивные алгоритмы (black-box). Они основаны на следующей идее: выбирается некоторое множество точек $p_1, \ldots, p_s$, причем так, что схема $\mathcal{C}$ вычисляет тождественный нулю полином тогда и только тогда, когда значение соответствующего полинома во всех этих точках будет 0. Из формулировки алгоритма понятно, что на размер множества точек должны накладываться полиномиальные ограничения для построения эффективных оценок. С другой стороны, так как множество не привязано к определенным многочленам, то оно должно быть достаточно широким. На основе этого алгоритма мы и будем проводить анализ задачи, а также разрабатывать возможные улучшения и исправления. В частности, в качестве основной идеи будет использоваться алгоритм из работы [14].

2 Основные определения

Везде далее (кроме отдельно обговоренных случаев) все операции будут проводиться в поле $\mathbb{F}$ произвольного вида.

Пусть дано некоторое ориентированное дерево, в листовых вершинах которого записано либо число $\alpha \in \mathbb{F}$, либо одна из переменных $x_1, \ldots, x_n$, а в узлах (нелистовые вершины) одна из операций: мультипликативная ($\times$) или аддитивная ($+$). Помимо этого, выделен некоторый узел — *сток*. Дерево с такими свойствами называются *схемой*. Каждой вершине дерева сопоставим некоторый многочлен: для листовых вершин это будут мономы, записанные в них, а для узловых вершин — операция над многочленами, соответствующих детям этого узла. Тогда говорят, что *многочлен вычисляется схемой*, если он соответсвует её стоку.

Очевидно, что наличие ребенка с пометкой $\times$ у вершины с такой же операцией, является избыточным: можно просто заменить ребенка на всех его собственных потомков. При этом многочлен, который вычисляется схемой, не изменится. То же самое произойдет, если вместо умножения будет стоять операция сложения. Поэтому считается, что в схеме вершины, помеченные $\times$, могут соединяться только с вершинами, помеченными $+$, и наоборот (это касается только для узлов). Таким образом, всю схему можно отранжировать по слоям, соответствующим умножению и сложению. На самом нижнем слое находятся листья, сток считается нулевым уровнем. Для того, чтобы осуществить первое условие, нужно отметить, что ребра могут идти не только из соседних слоев.

Высота построенного таким образом дерева (номер нижнего уровня) называется *глубиной* схемы. Количество вершин в первом слое будет обозначатся k.

Понятие формальной степени полинома p будет определятся индуктивно, двигаясь от листьев к стоку. Степень листовой вершины будет соответсвенно равна степени монома, записанного в нем. Для узлов с пометкой $+$ она будет определятся как максимум формальных степеней дочерних вершин, а для узлов, соответствующих мультипликативной операции — их суммой. Таким образом, формальная степень многочлена p, вычисляемого схемой $\mathcal{C}$ определяется как соответсвующее число стока. Очевидно, что формальная степень может отличатся от действительной. Тем не менее, везде далее в этой работе будет использоваться первое понятие.

Для удобства в работе будет использоваться обозначение $[k] := \{1, 2, \ldots, k\}$.

Важным частным случаем схем являются схемы глубины 3 над полем $\mathbb{F}$, имеющие вид:

$$C(x_1, \ldots, x_n) = \sum_{i=1}^{k} T_i,$$

где T_i (мультипликативный член) является произведением d_i линейных функций $l_{i,j}$ над полем $\mathbb{F}$. Случай линейных функций сводится к линейным формам. Также с помощью операции гомогенизации можно свести задачу общего вида к случаю $d_1 = \cdots = d_k =: d$ (см. раздел 7). Из-за этого вводится альтернативное определение.

Определение 2.1. *Схема $\mathcal{C}$ глубины 3 обозначается $\Sigma\Pi\Sigma(k, d)$, если:*

- *верхний слой C содержит k узлов;*

- $d_1 = \cdots = d_k = d$;
- *для любого* $i \in [k]$, $j \in [d]$, l_{ij} - *однородная линейная форма, то есть* $l_{ij} = l_{ij}^1 \cdot x_1 + \cdots + l_{ij}^n \cdot x_n$.

Вводятся следующие важные характеристики схемы:

Определение 2.2. [**Простая схема**] *Схема* $\mathcal{C}$ *называется простой, если не существует ненулевой линейной формы, делящей каждый* T_i.

[**Минимальная схема**] *Схема* $\mathcal{C}$ *называется минимальной, если для любого собственного подмножества* $S \in [k]$: $\sum_{i \in S} T_i$ *не нулевая.*

[**Ранг схемы**] *Ранг схемы,* $rank(\mathcal{C})$, *определяется как ранг семейства линейных форм* $l_{i,j}$, *рассматриваемых как* n*–мерные вектора над полем* $\mathbb{F}$.

3 Постановка задачи и состояние на данный момент

Problem Identity Testing: Пусть дана схема $\mathcal{C}$, которая вычисляет многочлен p. Требуется ответить на вопрос: является ли p тождественным нулем или нет.

В общем случае решение этой задачи за полиномиальное время от параметров задачи неизвестно. Более того, только недавно были получены результаты для частных случаев. В частности, известен алгоритм для схем глубины 3 при ограничении на верхний слой: $k = O(1)$. Также решены некоторые еще более частные случаи для глубины 4, рассматриваемые в работах [15,18,19]. Такая сложность, возникающая уже на схемах маленькой глубины, объясняется в работе [3]: если известен «эффективный» (полиномиальный) алгоритм для глубины 4, то можно построить квазиполиномиальный алгоритм для схем любой глубины.

4 Связь схем глубины 3 с другими задачами

В данном разделе будут предложены идеи, показывающие, что случай глубины 3 действительно является достаточно сложной задачей. Для этого будут рассмотрены основные результаты из работы [16].

В этой работе было показано, что для случая многочлена на n переменных над полем $\mathbb{C}$ степени d, вычисляемого схемой размера s, можно построить схему глубины 3 размера $\exp O(\sqrt{d \log d \log n \log s})$. Отсюда следует, что если доказать нижнюю оценку $\exp \omega(\sqrt{d} \cdot log^{\frac{3}{2}} d)$ на размер схемы глубины 3, которая будет вычислять перманент матрицы размера $d \times d$, то будут доказаны суперполиномиальные оценки на сложность вычисления перманента для любой схемы. Это утверждение указывает на сложность случая схем глубины 3.

Определение 4.1. *(***ABP***) ABP это граф, вершины которого разбиты на слои, а ребра идут из слоя* i *в слой* $i+1$. *Каждое ребро* e *такого графа помечено линейными многочленами* l_e. *Первый слой содержит ровно одну вершину, которая называется*

источником. Аналогично с последним слоем, вершина в нем называется стоком. Для любого пути $\gamma = (e_1, \ldots, e_d)$ *из источника в сток, вес пути определяется как произведение линейных форм соответствующих ребер:* $wt(\gamma) = l_{e_1} \ldots l_{e_d}$. *Говорят, что ABP вычисляет многочлен, равный* $\sum_\gamma wt(\gamma)$, *где* γ *пробегает все пути из источника в сток.*

Основная идея сводимости между задачами заключается в следующем. Во-первых, без ограничения общности, можно считать, что ABP однородная, так как, как и в случае схем глубины 3, существует полиномиальная сводимость к такому типу задач.

Во-вторых, от ABP можно перейти к схемам вида $\Sigma\Pi^{[a]}\Sigma\Pi^{[d/a]}$, где индекс сверху над произведением означает ограничение на степень соответствующей операции. Таким образом, на первом уровне происходит перемножение не более чем $[d/a]$ мономов, а на втором - не более чем $[a]$ многочленов. Метод основан на том, что подсчет многочлена ABP легко интерпретируется как перемножение d матриц. Таким образом, если разделить все матрицы на a блоков по d/a матриц в каждой, то получится как раз схема указанного вида. В работе [16] показано, что в случае $a = \sqrt{\frac{d \log n}{\log s}}$ новая схема будет размера $s_1 = \exp O(\sqrt{d \log n \log s})$.

В-третьих, из получившихся схем задачу можно свести к схемам вида $\Sigma \wedge^{[a]} \Sigma \wedge^{[d/a]} \Sigma$, где $\wedge$ означает возведение многочлена в степень. Такая сводимость возможна с использованием следующей леммы.

Лемма 4.1. *Для любого* n, *моном* $x_1 \ldots x_n$ *может быть представлен в виде ленейной комбинации*

$$2^{n-1} \cdot n! \cdot x_1 \ldots x_n = \sum_{(r_2,\ldots,r_n)\in\{\pm 1\}^{n-1}} (x_1 + \sum_{i=2}^{n} r_i x_i)^n \cdot (-1)^{wt(\mathbf{r})},$$

где $wt(\mathbf{r}) = |\{i : r_i = -1\}|$.

Благодаря ней, между схемами указанного выше вида существует простая сводимость. При этом размер схемы становится $s_2 = \exp(O(\sqrt{d \log n \log s}))$.

Наконец, последним шагом является сводимость между $\Sigma \wedge^{[a]} \Sigma \wedge^{[d/a]} \Sigma$ и $\Sigma\Pi\Sigma$. Основным инструментом в такой сводимости является следующая лемма:

Лемма 4.2. *Над полем комплексных чисел, для любых* m, d, *существуют однородны полиному* $f_{ij} \in \mathbb{C}[u]$ *со степенью не более, чем* d, *такие, что*

$$(u_1 + \cdots + u_m)^d = \sum_{i=1}^{md+1} \prod_{j=1}^{m} f_{ij}(u_j).$$

Доказательство можно найти в [18].

5 Алгоритмы для частных случаев схем глубины 3

5.1 Основные виды известных алгоритмов

Как уже было упомянуто, в общем случае решения даже для схем глубины 3 нет. Поэтому существует множество алгоритмов, рассматривающих частные случаи. Многие алгоритмы используют ограничения $k = O(1)$. Дело в том, что ограничение на другие параметры не вызывает сложности: если рассматривать случай $n = O(1)$, то решение сводится к перебору маленького количества точек (полиномиального от d). То же происходит и в случае ограничения на d. С другой стороны, ограничения на степень многочлена и количество переменных довольно сильные. Поэтому везде дальше будет учитываться ограничение $k = O(1)$ ($bounded\ top - fanin$).

В основном в этой области алгоритмы бывают адаптивными и неадаптивными, вероятностными и детерминированными. Первые и вторые имеют общее свойство: они находят множество точек. По анализу значений в этих точках можно установить, является ли многочлен тождественным нулем. В первом случае считается, что правильный ответ дается с некоторой заранее определенной вероятностью: чем выше точность определения, тем большее множество точек придется брать. Формально множество точек для вероятностных алгоритмов должно обладать следующим свойством (с заранее выбранным S):

Утверждение 1. *(***Шварц-Зиппель***)* *Пусть многочлен $p(x_1, \ldots, x_n)$ - ненулевой многочлен над полем $\mathbb{F}$ формальной степени d. Пусть S - любое подмножество $\mathbb{F}$ и точка $(a_1, \ldots, a_n)$ выбрана случайным образом из S. Тогда*

$$P[p(a_1, \ldots, a_n) = 0] \leq \frac{d}{|S|}.$$

Доказательство утверждения можно найти в [17].

Для неадаптивных алгоритмов множество точек $\mathcal{H}$ должно обладать другим свойством:

Утверждение 2. • *для любой схемы $\mathcal{C} = \Sigma\Pi\Sigma(k, d, n)$ над $\mathbb{F}$ ею вычисляется нулевой многочлен $\Leftrightarrow \forall a \in \mathcal{H} :\ \mathcal{C}(a) = 0$*

5.2 Неадаптивный алгоритм для случая $k = O(1)$

В данном разделе приведен алгоритм из работы [14]. В начале приводится необходимое множество точек, удовлетворяющее определению из утверждения 5.1. Далее будут рассмотрены основные утверждения, показывающие, что это действительно так.

Множество $\mathcal{H}$ строится следующим образом:

- Пусть $S \subset \mathbb{F}$ - произвольное множество размера $dnk^2 + 1$.
- Пусть $T \subset \mathbb{F}$ - произвольное множество размера $d + 1$.

- $\forall \beta \in S,\ (\gamma_1, \ldots, \gamma_k) \in \mathbb{F}^k$ определяется вектор $\bar{\delta}$ следующим образом:

$$\delta_i = \sum_{j \in [k]} \beta^{ij} \gamma_j.$$

- Множество $\mathcal{H}$ состоит из всех таких векторов $\bar{\gamma}$. Заметим, что в данном случае подразумевается, что вышеуказанные множества существуют, то есть $|\mathbb{F}| > dnk^2$. В случае, когда это неравенство не выполняется, можно перейти к расширению поля $\mathbb{F}$. Поэтому без ограничения общности можно считать, что неравенство верно.

Основная идея, используемая в этом алгоритме для решения задачи проверки на тождество, заключается в том, что вместо исходной задачи решаются более простые того же вида:

Теорема 1. *Пусть $\mathbb{F}$ — произвольное поле, такое, что $|\mathbb{F}| > dnk^2$. Тогда существует детерминированный алгоритм, который берет на вход тройку (k, d, n) натуральных чисел и за время $poly(kdn)$ строит отображение $\Psi_i : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[y_1, \ldots, y_k]$ $(1 \leq i \leq poly$ Тогда*

$$\Sigma\Pi\Sigma(k, d, n) \text{ схема } \mathcal{C} \text{ вычисляет нулевой многочлен } \Leftrightarrow \forall i : \Psi_i(\mathcal{C}) = 0.$$

Такие отображения можно записать в явном виде. Рассмотрим гомоморфизм Ψ_β такой, что

$$\forall i \in [n],\ \Psi_\beta : x_i \mapsto \sum_{j=1}^{k} \beta^{ij} y_j. \tag{1}$$

Считается, что $\Psi_\beta(\alpha) = \alpha,\ \forall \alpha \in \mathbb{F}$.
Пусть $\mathcal{R} = \mathbb{F}[x_1, \ldots, x_n],\ \mathcal{R}' := \mathbb{F}[y_1, \ldots, y_k]$.

Лемма 5.1. *Пусть $\Psi_\beta : \mathcal{R} \to \mathcal{R}'$ является линейным гомоморфизмом, определенным в (1). Пусть $S \in L(\mathcal{R})$ — подмножество линейных форм, такое, что $rk(S) \leq k$. Тогда для всех, кроме, быть может, nk^2 значений β, $rk(\Psi_{beta}(S)) = rk(S)$.*

Гомоморфизм зависит только от тройки (k, d, n) и вычисляется за время $poly(kdn)$.

Доказательство этой леммы можно посмотреть в [14]. С помощью нее доказывается основная теорема.

Стоит отметить, что доказательство теоремы 1 в одну сторону (слева направо) является следствием того, что полученные преобразования — гомоморфизмы. Доказательство обратного утверждения использует результат теоремы 5.

6 Оценки ранга тождеств

Под тождествами понимают такие схемы $\mathcal{C}$, для которых выполняется тождественное равенство нулю: $C \equiv 0$. Для таких схем существуют оценки на их ранги, а именно:

$$rank(C) = O(k^2 \log d).$$

О чем свидетельствуют данные ограничения? Кажется, что если получится доказать, что ранг достаточно маленький, то отсюда следует ограничение на количество независимых переменных. С помощью афинного преобразования, можно будет перейти в пространство с меньшим порядком переменных. Также существуют алгоритмы, позволяющие эффективно решать задачу PIT в случае маленьких рангов.

В этой работе будет рассмотрен способ оценки рангов тождеств $\Sigma\Pi\Sigma$ при помощи конфигураций Сильвестра-Галлаи.

Определение 6.1. *Пусть S — конечное подмножество проективного пространства $\mathbb{FP}^n$. Иначе говоря, S — подмножество векторов в $\mathbb{F}^{n+1}$ такое, что ни один вектор в S не является коллинеарным другому. Предположим, что для любого множества $V \subset S$, состоящего из k линейно независимых векторов, линейная оболочка V содержит как минимум $k+1$ вектор из S. Тогда S называется SG_k-замкнутым.*

Наибольший возможный ранг SG_k-замкнутого множества из не более, чем m векторов $\mathbb{F}^n$ (для любого n) обозначается как $SG_k(\mathbb{F}, m)$.

Основные теоремы данного раздела — теорема о величине SG_k и связь между ней и рангом тождеств:

Теорема 2. *(SG_k для любого поля) Для любого поля $\mathbb{F}$ и $k, m \in \mathbb{N}^{>1}$, $SG_k(\mathbb{F}, m) \leq 9k \lg m$.*

Теорема 3. *(Связь SG_k с рангом тождеств) Пусть $|\mathbb{F}| > d$. Тогда ранг минимального и простого тождества $\Sigma\Pi\Sigma(k, d)$ над $\mathbb{F}$ не превосходит $\frac{3(k-1)(k-2)}{2} + k \cdot SG_k(\mathbb{F}, d)$.*

Основной вывод из этих утверждений сформулирован следующим образом:

Теорема 4. *Пусть $\mathcal{C}$ является $\Sigma\Pi\Sigma(k, d)$ над полем $\mathbb{F}$, причем она минимальная, простая и нулевая. Тогда:*

- *для $\mathbb{F} = \mathbb{R}$, $rk(\mathcal{C}) < k^2 + \frac{3(k-1)(k-2)}{2}$;*
- *для любого поля $\mathbb{F}$, $rk(\mathcal{C}) < k^2(\lg d) + \frac{3(k-1)(k-2)}{2}$.*

Следующее утверждение объясняет, каким образом вышеуказанные теоремы приводят к сравнительно простому алгоритму проверки полинома на тождественный ноль в поле $\mathbb{Q}$:

Утверждение 3. *Существует детерминированный алгоритм, который берет на вход тройку (k, d, n) натуральных чисел и за время $poly(nd^{k^2})$ выдает множество $\mathcal{H}$ со следующими свойствами:*

1. *Для любой схемы* $\mathcal{C} = \Sigma\Pi\Sigma(k, d, n)$ *над* $\mathbb{R}$ *вычисляет нулевой многочлен* $\Leftrightarrow \forall a \in \mathcal{H}, \mathcal{C}(a) = 0$.

2. $\mathcal{H}$ *содержит не более* $poly(nd^{k^2})$ *точек.*

3. *Битовая длина каждой точки в* $\mathcal{H}$ *является* $poly(kn \log d)$.

Таким образом, построив проверяющее множество $\mathcal{H}$, мы сможем эффективно проверить, вычисляет ли данная схема нулевой многочлен. Так как размер множества точек полиномиально зависит от параметров задачи (с учетом $k = O(1)$), то время проверки также будет полиномиальным.

6.1 Критерий для проверки равенства нулю

Вводятся следующие определения:

Определение 6.2. *Пусть мультипликативный член* f *имеет вид:* $f := c \cdot \prod_{l \in S} l, c \in \mathbb{F}^*$ *и* S *- список ненулевых линейных форм. Тогда* $L(f)$ *обозначает список* S *линейных форм из произведения выше, а*

$$M(S) = \begin{cases} \prod_{l \in S} l, & S \neq \emptyset, \\ 1, & S = \emptyset. \end{cases}$$

$L(\mathcal{C})$ *обозначает, соответственно, список всех линейных форм в схеме* $\mathcal{C}$.

[**Линейная оболочка** $sp(\cdot)$ **и ранг** $rk(\cdot)$] *Пусть* S *— список линейных форм, тогда* $sp(S)$ *— линейная оболочка над линейными формами из* S *над* $\mathbb{F}$. $rk(S)$ *обозначает ранг множества* S *как набор векторов в линейном пространстве над* $\mathbb{F}$.

[**radsp**$(\cdot)$] *Пусть* $S := \{f_1, \ldots, f_m\}$ *— мультипликативные члены, порождающие идеал* I. *Обозначим линейное пространство* $radsp(S) := sp(L(f_1 \cap \cdots \cap f_m))$. *Когда множество* S *будет очевидно из контекста, будет использоваться просто запись* $radsp(I)$. *Запись* $radsp(I, f)$ *в таком случае обозначает* $radsp(S \cap \{f\})$.

[**Подобные формы**] *для любых двух полиномов* f, g *назовем* f *похожим на* g, *если* $\exists c \in \mathbb{F}^* : f = cg$. *Аналогично определяется сходство по модулю некоторого идеала* I. *Очевидно, что понятие сходства является отношением эквивалентности.*

[**Узлы**] *Пусть* f *некоторый мультипликативный член и идеал* I *порожден какими-то мульитипликативными членами. Тогда «сходство по модулю* $radsp(I)$*» является отношением эквивалентности на* $L(\mathcal{R})$ *и делит список* $L(f)$ *на классы эквивалентности.*

[$\mathbf{rep}_I(f)$] *Для каждого такого класса выбирается представитель* l_i *и определяется совокупность* $\mathbf{rep}_I(f) := \{l_1, \ldots, l_r\}$ *(*r *- количество классов эквивалентности).*

[$\mathbf{nod}_I(f)$] *Для любой формы* $l_i \in rep_I(f)$ *перемножаются все формы, похожие на* $l_i \mod radsp(I)$*:*

$$nod_I(f) := \{M(L(f) \cap (\mathbb{F}^* l + radsp(I)))) | l \in rep_I(f)\}.$$

[**Пути**] *Пусть I - идеал, порожденный какими-то мультипликативными членами. Пусть также $\mathcal{C} = \sum_{i\in[k]} T_i$ является $\Sigma\Pi\Sigma(k,d)$. Пусть v_i - подчлен T_i ($L(v_i) \subset L(T_i)$), $\forall i \in [k]$. Назовем кортеж $(I, v_1, \ldots, v_k)$ путем $\mathcal{C}$ по модулю I, если*

$$\forall i \in [k] : \ v_i \ \in \ nod_{\langle I, v_1, \ldots, v_{i-1}\rangle}(T_i).$$

Также $\forall S \subset [k] : \mathcal{C}_S := \sum_{s\in S} T_s$.
$\forall i \in \{0, \ldots, k-1\}$ определим $[i]' := [k] \ \setminus \ [i], [0] := \emptyset, \mathcal{C}_\emptyset := 0$.

Следующая теорема показывает, насколько тождественное равенство нулю связано с введенным понятием пути. Другими словами, она является критерием того, является ли схема нулевой или нет.

Теорема 5. *Пусть I - идеал, порожденный мультипликативными членами. Пусть $\mathcal{C} = \sum_{i\in[k]} T_i$ является $\Sigma\Pi\Sigma(k,d)$ и не является нулевой по модулю I. Тогда $\exists i \in \{0, \ldots, k-1\} : \ \mathcal{C}_{[i]} mod I$ имеет путь p такой, что*

$$\mathcal{C}_{[i]'} \equiv \alpha \cdot T_{i+1} \not\equiv 0 (mod\ p).$$

В работе [KS05] описан алгоритм, корректность которого доказывается с помощью приведенной теоремы. Однако, необходимое множество построено лишь для случая $\mathbb{F} = \mathbb{R}$, причем сложность алгоритма по прежнему зависит от k экспоненциально. В общем случае задача построения критериального множества остается открытым.
Доказательство. Выберем $i \in \{0, \ldots, k-1\}$ и путь p подсхемы $\mathcal{C}_{[i]} \bmod I$, что:

1. $C_{[i]'} \notin \langle p \rangle$,
2. $J_i := \{j \in [i]' | T_j \notin \langle p \rangle\} \neq \emptyset$ наименьшее из возможных (по всем i).

Так как для $i = 0, p = (I)$ выполняются оба условия, то $J_i \neq \emptyset$, а значит, можно найти такие i и p, чтобы выполнялись оба условия.

Пусть $j^* = \min\limits_{j\in J_i} j$. Это означает, что $\forall m, \ i < m < j^* : T_m \ \in \langle p \rangle$. Это значит, что $v_m := M(L_{radsp(p)}(T_m)) \in \langle p \rangle$, то есть добавление этих элементов к p не меняет $\langle p \rangle$. Тогда докажем, что $q := (p, (v_m | i < m < j^*))$ путь из условия теоремы.

Так как $\mathcal{C}_{[j^*-1]'} \equiv \mathcal{C}_{[i]'} (\mod p)$ и $\mathcal{C}_{[i]'} \notin \langle p \rangle = \langle q \rangle$, то $j^* - 1$ и q также удовлетворяют условиям выше (так как ничего не меняется).

Будем доказывать от противного: пусть $\mathcal{C}_{[j^*-1]'} \notin \langle q, T_{j^*} \rangle$, тогда по китайской теореме об остатках $\exists v_{j^*} \in \mathrm{nod}_{\langle q \rangle}(T_{j^*}) : \ \mathcal{C}_{[j^*-1]'} \notin \langle q, v_{j^*} \rangle$. Тогда новый путь $q' := (q, v_{j^*})$ очевидно будет путем $\mathcal{C}_{[j^*]} \bmod I$. С другой стороны, $J_{j^*} \subset J_i \setminus j^* \subsetneq J_i$, причем $C_{[j^*-1]'} = C_{[j^*]'} - T_{j^*} \neq \langle q' \rangle$, откуда получаем противоречие с минимальностью J_i.

Значит, $\mathcal{C}_{[j^*-1]'} \notin \langle q, T_{j^*} \rangle$, то есть по определению $\exists \alpha$:

$$(C_{[j^*-1]'} - \alpha T_{j^*}) \in \langle q \rangle = \langle p \rangle,$$

откуда и получаем условие теоремы. ■

6.2 Ядерное соответствие

Как уже было сказано выше, основная цель изучения рангов у тождеств и других схем – это понять, насколько на самом деле «просты» эти тождества, то есть каким минимальным количеством переменных они описываются. Как будет показано ниже, мультипликативные члены в тождествах сильно «подобны», а именно: линейные формы, которые в них содержатся, одинаковые по модулю некоторого идеала.

Определение 6.3. [**Соответствия**] *Пусть U, V – списки линейных форм и I – подпространство пространства линейных форм. I-соответствием называется биекция π между списками U, V: $\forall l \in U, \pi(l) \in \mathbb{F}^* l + I$.*

Если f, g – мультипликативные члены, то I-соответствие означает соответствие между $L(f),\ L(g)$.

Следующая теорема показывает, что можно подобрать не очень большое подпространство (в смысле ранга) линейных форм, относительно которого между всеми мультипликативными членами схемы-тождества существует такое соответствие.

Теорема 6. *Пусть $\mathcal{C} = T_1 + \cdots + T_k$ – $\Sigma\Pi\Sigma(k, d)$ схема, причем минимальная и нулевая. Тогда существует подпространство K пространства всех линейных форм, такое, что:*

- $rk(K) \leq (k-1)(k-2)$.
- $\forall i \in [k]\ \exists K$*-соответствие* π_i *между* T_1 *и* T_i.

Такое множество K называется ядерным соответствием $\mathcal{C}$.

Доказательство. Подпространство K будет строится итеративно, причем понадобится не более $k-1$ циклов. На каждом шаге итерации будет поддерживаться множество $\mathcal{P}$, содержащее пути некоторых подсхем $\mathcal{C}$, и неориентированный граф $G = ([k], E)$. Для удобства $U := radsp(p | p \in \mathcal{P})$. На каждом шаге итерации будет поддерживаться инвариант: $(i, j) \in E \Leftrightarrow T_i, T_j$ — U-соответствие. Инициализация: $\mathcal{P} := \{(0)\}, E := \{(i, j) \in [k]^2 | T_i, T_j \text{ схожи}\}$. В итоге хочется получить связный граф G (на самом деле k-клику), сохраняя $rk(U)$ как можно меньше.

Посмотрим, что будет, если получится сохранить инвариант до шага $(r-1) \geq 0$. Если G стал связным, то процесс останавливается. Если нет, то надо попробовать уменьшить количество компонент связности на шаге r. Пусть S - максимальная компонента связности G, $S \neq [k]$. Тогда по свойству минимальности схемы, $\mathcal{C}_S \neq 0$, и можно воспользоваться критерием отличия схемы от нуля:

$$\exists p_S \in \mathcal{C} : \exists i \in S, \mathcal{C}_S \equiv \alpha T_i \not\equiv 0 \pmod{p_S}, \alpha \in \mathbb{F}^*.$$

Пусть $S' := [k] \setminus S$. Тогда

$$\mathcal{C} \equiv \mathcal{C}_{S'} + \alpha T_i \equiv 0 \pmod{p_S}.$$

Значит, из условия выше $\mathcal{C}_{S'} \notin \langle p_S \rangle$. Тогда по тому же критерию, можно построить путь $p_{S'}$ в $\mathcal{C}_{S'} \mod p_S$:

$$C_{S'} \equiv \beta T_j \not\equiv 0 \pmod{p_{S'}},\ \beta \in \mathbb{F}^*$$

$$\Downarrow$$

$$\alpha T_i \equiv -\beta T_j \not\equiv 0(\pmod{p)_{S'}}.$$

Пусть $K' := radsp(p_{S'})$. Теперь можно рассматривать $p_{S'}$ как путь схемы $\mathcal{C} \mod \langle 0 \rangle$, при этом получается, что его длина не более, чем $|S| - 1 + |S'| - 1 = k - 2$, то $rk(K') \leq k - 1$. Можно показать, что сравнение выше приводит к K'-соответствию между T_i и T_j, причем сохраняя соответствия, которые были до этого (см. [14]). При этом количество компонент связности уменьшилось.

На каждой итерации $rk(U)$ увеличивается не более, чем на $k-2$, а итераций всего $k-1$. Следовательно, получается оценка из теоремы. ■

В данной работе оценка улучшена по сравнению с оригинальной версией доказательства. С одной стороны, асимптотически оценка оказалась такой же по порядку, так как авторы показали оценку ранга k^2. Однако, как будет показано ниже, полученная точность будет иметь принципиальное значение для других выводов.

6.3 Сертификат для линейной независимости мультипликативных членов

Теперь хочется построить аналогичные взаимотношения для тех схем, которые не являются тождествами, то есть какие-нибудь соотношения для линейной независимости мультипликативных членов.

Пусть это $T_1, \ldots, T_{[k']}$, и подпространство K' такое, что существует K'-отображение между $T_1, T_i\ \forall i \in [k]$. Пусть также эти мультипликативные формы линейно независимы. Тогда хочется построить такое подпространство K ранга не более $(rk(K') + k'^2)$, чтобы $M(L_K(T_1)), \ldots, M(L_K(T_{k'}))$ тоже были линейно независимы. Здесь введено обозначение $L_K(L(T_i) = L(T_i) \cap K$. Соответственно, схема становится проще, а линейная независимость остается.

Теорема 7. *Пусть* $\mathcal{C} = \sum_{i \in [k]} T_i$ *- минимальное* $\Sigma\Pi\Sigma(k, d)$ *тождество и* $\{T_i | i \in \mathcal{I}\}$ *– максимальное множество независимых термов (мультипликативных членов,* $1 \leq k' := |\mathcal{I}| < k$*). Тогда существует такое линейное подпространство* K*, что:*

- $rk(K) \leq \frac{3(k-1)(k-2)}{2}$.
- $\forall i \in [k]$ *существует* K*-отображение между* T_1, T_i.
- *(*$K_i := M(L_K(T_i))$*.) Мультипликативные члены* $\{K_i | i \in \mathcal{I}\}$ *линейно независимы.*

Такое множество K называется ядром.

Доказательство. Без ограничения общности можно считать, что $\mathcal{I} = [k']$. Процесс итеративный, не более k'^2 циклов, постепенно строится K. На каждом шаге поддерживается пространство U, которое с каждым шагом становится все ближе к K. Считаем $U_i := M(L_U(T_i)), \forall i \in [k']$. Также для $i \in [k'] \setminus \{1\}$ определяется идеал $\mathcal{I}_i := \langle U_1, \ldots, U_{i-1} \rangle$.

Процесс идет по двуступенчатому циклу. Для удобства внешний цикл называется фазой, а внутренний - кругом. На каждом круге U увеличивается максимум на 1, на i-й фазе не более i кругов. Причем после окончания i-й фазы ($i \geq 2$) обеспечивается $T_i \notin \mathcal{I}_i$.

На первой фазе считаем $U := K'$, которое можно найти по предыдущей теореме. Причем получаем, что к концу первой фазы $rk(U) \leq (k-1)(k-2)$.

Фаза $i = 2$: Так как T_1 и T_2 линейно независимы, то $T_1 \notin \langle T_2 \rangle$. Тогда по лемме 6.2 получим, что $\exists v \in \mathrm{nod}_{\langle 0 \rangle}(T_1) : \ T_2 \notin \langle v \rangle$. Обновляем U до $(U + \mathrm{radsp}(v))$. Видно, что $T_2 \notin \langle U_1 \rangle = \mathcal{I}_2$ (иначе получим противоречие с тем, что $T_2 \notin \langle v \rangle$).

Фаза $i > 2$: Считаем, что $\forall r < i : T_r \notin \mathcal{I}_r$. На круге j ($1 \leq j < i$) мы хотим поддерживать условие, что $T_i \notin \langle U_1, \ldots, U_j, T_{j+1}, \ldots, T_{i-1} \rangle$. Если это выполняется, то ничего не делаем. В противном случае необходимо воспользоваться утверждением:

Утверждение 4. *Пусть $i > 2$ и $1 \leq j < i$. Предположим, что $T_r \notin \langle U_1, \ldots, U_{r-1} \rangle$, $\forall\ r\ <\ i$. Пусть $T_i \in \langle U_1, \ldots, U_j, T_{j+1}, \ldots, T_{i-1} \rangle$, но $T_i \notin \langle U_1, \ldots, U_{j-1}, T_j, \ldots, T_{i-1} \rangle$. Тогда*

$$\exists v \in nod_{\langle U_1, \ldots, U_{j-1} \rangle}(T_j) : \ \textit{при } U' \leftarrow (U + radsp(v)) \textit{ выполняется}$$
$$T_i \notin \langle U'_1, \ldots, U'_j, T_{j+1}, \ldots, T_{i-1} \rangle.$$

Доказательство. Из условия получается, что

$$T_i + \sum_{r=j+1}^{i-1} \alpha_r T_r \in \langle U_1, \ldots, U_j \rangle$$

для каких-то $\alpha_r \in \mathbb{F}$. Предположим, что эти коэффициенты не однозначны. Тогда при вычитании двух разных линейных комбинаций, какие-то коэффициенты останутся ненулевыми. Пусть $s = \max\{i : \alpha_i = \alpha'_i \neq 0\}$ (α'_i - другой вариант коэффициентов). Тогда получается, что $T_s \in \langle U_1, \ldots, U_j, T_{j+1}, T_{s-1} \rangle \subset \langle U_1, \ldots, U_{s-1} \rangle$, а это противоречит предположению индукции. Получается, что α_i определены однозначно.

Из второго условия получается, что

$$T_i + \sum_{r=j+1}^{i-1} \alpha_r T_r \notin \langle U_1, \ldots, U_{j-1}, T_j \rangle.$$

Тогда по китайской теореме об остатках:

$$\exists v \in nod_{\langle U_1,\ldots,U_{j-1}\rangle}(T_j) : T_i + \sum_{r=j+1}^{i-1} \alpha_r T_r \notin \langle U_1, \ldots, U_{j-1}, v\rangle.$$

Обновим $U' \leftarrow (U + radsp(v))$. Предположим, что все еще выполняется условие:

$$T_i \in \langle U'_1, \ldots, U'_j, T_{j+1}, \ldots, T_{i-1}\rangle,$$

тогда

$$T_i + \sum_{r=j+1}^{i-1} \beta_r T_r \in \langle U'_1, \ldots, U'_j\rangle \subset \langle U_1, \ldots, U_j\rangle.$$

Так как мы доказали единственность коэффициентов, то $\alpha_r = \beta_r$. Отсюда получается противоречие с написанным раннее. ■

Далее индуктивно применяем утверждение начиная с круга 1. Переход выполняется прямо из условий утверждения, поэтому осталось проверить базу.

На первом круге мы должны что-то сделать только в случае, если $T_i \in \langle U_1, T_2, \ldots, T_{i-1}\rangle$. Но из линейной независимости следует, что утверждение все равно верно при $j = 1$, а новую линейную форму v мы должны брать по нулевому идеалу. На последнем круге выполняется инвариант по фазе: $T_i \notin \langle U_1, \ldots, U_{i-1}\rangle \mathcal{I}_i$.

Итак, индуктивное предположение выполнено, на каждом круге $rk(U)$ увеличивается не более, чем на 1. Отсюда получаем оценку на $rk(U)$. ■

Из доказательства теоремы следует, что оценка ранга U очень не строгая. Во-первых, неточность появляется уже на первой фазе. Поэтому более точной оценкой является

$$rk(U) \leq (k-1)(k-2) + \frac{(k-1)(k-2)}{2} = \frac{3(k-1)(k-2)}{2}.$$

Следует заметить, что теорема помимо оценки на ранг ядра также дает и аналитический способ его построения, причем он состоит из двух важных пунктов: построение ядерного соответствия и последующая достройка до ядра. Поэтому если получится, что ядерное соответствие окажется ядром, то второго слагаемого вообще не будет. Далее в работе будет показано, что при $k = 3$ выполняется именно такой случай.

6.4 Теорема Сильвестра-Галлаи

Из предыдущего подраздела видно, что достаточно много линейных форм в тождестве оказались «подобными» по модулю не очень большого идеала. Всего линейных форм, которые при этом находятся в $radsp(K)$, не более, чем $\frac{3(k-1)(k-2)}{2}$. Соответственно, осталось понять, как соотносятся друг с другом оставшиеся линейные формы. Итоговый результат сформулирован в следующей теореме:

Теорема 8. *Итоговая оценка Пусть $|\mathbb{F}| > d$. Тогда ранг простого, минимальноого $\Sigma\Pi\Sigma(k, d)$ тождества, в котором наибольшее число независимых слагаемых равно k', не более, чем $\frac{3(k-1)(k-2)}{2} + (k - k') \cdot SG_{k'}(\mathbb{F}, d)$.*

Первое слагаемое получается из размера ядра. Соответственно, осталось показать, откуда получается второе слагаемое. Для этого необходимо доказать следующее:

Теорема 9. *Пусть $|\mathbb{F}| > d$. Тогда ранг для неядерной части простого и строго минимальноого (то есть $k' = k+1$) $\Sigma\Pi\Sigma(k,d)$ тождества над $\mathbb{F}$ не более, чем $SG_{k-1}(\mathbb{F},d)$.*

Сначала покажем, что этого достаточно.

Доказательство.(Теорема 8)

Без ограничения общности можно считать, что $T_1,\dots,T_{k'}$ линейно независимы. Тогда $\forall i \in [k'+1,k]$ существуют такие $\alpha_{i,j}$ что

$$D_i := \sum_{j\in[k']} \alpha_{i,j}T_j + T_i = 0.$$

Пусть $N_i = \{j : \alpha_{i,j} \neq 0\}$. Тогда

$$\forall i \in [k'+1,k] :\ D_i = \sum_{j\in N_i} \alpha_{i,j}T_j + T_i = 0.$$

Очевидно, что если есть ядро для схемы $\mathcal{C}$, то оно является также содержит для схемы $\hat{D}_i$, полученной из D_i делением на наибольший общий делитель всех слагаемых (очевидно, что свойство линейной независимости при этом сохраняется). Таким образом, схема $\hat{D}_i$ является строго минимальным, простым тождеством, а значит, ранг неядерной части равен $SG_{k'}(\mathbb{F},d)$.

В случае, когда $\bigcap_{i\in[k'+1,k]} N_i = [k']$, очевидно, что любая линейная форма схемы описывается некоторым полученным «базисом». Отсюда и следует искомая оценка.

Предположим, что это не так. Пусть $S := \bigcap_{i\in[k'+1,k]} N_i \neq [k']$. Из определения схем D_i получается, что $\sum\limits_{i\in[k'+1,k]} T_i = \sum_{s\in S}\beta_s T_s$ для некоторых β_s из $\mathbb{F}$. Тогда

$$\mathcal{C} = \mathcal{C}_{[k']} + \mathcal{C}_{[k'+1,k]} = \sum_{i\in[k']} T_i + \sum_{s\in S}\beta_s T_s = 0.$$

Так как S — собственное подмножество $[k']$, то данное условие противоречит линейной независимости T_i для $i \in [k']$, противоречие. ■

Доказательство теоремы 9 можно найти в [14].

6.5 Нижние и верхние оценки на ранг тождеств

Теперь оценки на ранги будем рассматривать асимптотически. Выше было показано, что верхние оценки для рангов в любом поле $\mathbb{F}$ являются величинами порядка $O(k^2\log d)$. Тем не менее, известные нижние оценки — $\Omega(k\log d)$. Они достигаются для полей вычетов: $\mathbb{F}_p$, где p - простое число.

Сначала рассмотрим тождество над полем $\mathbb{F}_2$ при $k = 3$:

$$\mathcal{C}(x_1,\dots,x_r) := \prod_{\substack{b_1,\dots,b_{r-1}\in\mathbb{F}_2\\ b_1+\dots+b_{r-1}\equiv 1}} (b_1x_1+\dots+b_{r-1}x_{r-1})+$$
$$+ \prod_{\substack{b_1,\dots,b_{r-1}\in\mathbb{F}_2\\ b_1+\dots+b_{r-1}\equiv 0}} (x_r+b_1x_1+\dots+b_{r-1}x_{r-1})+$$
$$+ \prod_{\substack{b_1,\dots,b_{r-1}\in\mathbb{F}_2\\ b_1+\dots+b_{r-1}\equiv 1}} (x_r+b_1x_1+\dots+b_{r-1}x_{r-1})$$

В этом случае $r \geq 2$. Тогда $d = 2^{r-2}$, а $rk(\mathcal{C}) = r = \log_2 d + 2$, то есть нижняя оценка выполняется. Следующая лемма показывает, что можно построить тождество для любого k.

Лемма 6.1. *Пусть $D := \sum_{j=1}^{k} T_j$ — простая, минимальная и нулевая $\Sigma\Pi\Sigma$ схема над $\mathbb{F}_2$, определенная на переменных $y_1,\dots,y_s$. Пусть степень D равна g, верхний слой k, ранг s. $\mathcal{C}$ определена выше, причем $\mathcal{C} = S_1 + S_2 + S_3$. Тогда схема, определяемая*

$$D' := \sum_{j=1}^{k-1} T_j \cdot S_1 - T_k \cdot S_2 - T_k \cdot S_3,$$

является минимальной, простой и нулевой со степенью $d' = d+g$, верхним слоем, равным $k' = k+1$, и рангом $r' = s+r$.

Доказательство этой леммы следует из определений, используя, что $S_2+S_3 = -S_1$.
Для поля характеристики $p > 0$:

$$\mathcal{C}(x_1,\dots,x_r) := \prod_{\substack{b_1,\dots,b_{r-1}\in\mathbb{F}_p\\ b_1+\dots+b_{r-1}\equiv 1}} (b_1x_1+\dots+b_{r-1}x_{r-1})+$$
$$+ \prod_{\substack{b_1,\dots,b_{r-1}\in\mathbb{F}_p\\ b_1+\dots+b_{r-1}\equiv 0}} (x_r+b_1x_1+\dots+b_{r-1}x_{r-1})+$$
$$+ \prod_{\substack{b_1,\dots,b_{r-1}\in\mathbb{F}_p\\ b_1+\dots+b_{r-1}\equiv 1}} (x_r+b_1x_1+\dots+b_{r-1}x_{r-1})$$

также подходит.
Особый случай возникает для поля характеристики 0. Рассмотрим его подробнее.
На данный момент известно лишь тождество ранга 4 для таких полей:

$$x_4(x_4+x_1+x_2)(x_4+x_2+x_3)(x_4+x_3+x_1)-(x_4+x_1)(x_4+x_2)(x_4+x_3)(x_4+x_1+x_2+x_3)+$$
$$+x_1x_2x_3(2x_4+x_1+x_2+x_3).$$

Однако, можно доказать, что в данном случае решение оптимально и нельзя построить тождество более высокого ранга (простое и минимальное).

Заметим, что из теории Сильвестра-Галлаи получается, что ранг тождеств должен оцениваться как составляющая, соответствующая оценке на ранги ядер, и добавка от $SG_k(\mathbb{F}, m)$. Во-первых, в случае $\mathbb{F} = \mathbb{R}$ можно показать, что $SG_2(\mathbb{R}, d) \leq 2$.

Оценка на ранг тождества получается равной $\frac{3}{2}(k-1)(k-2) + (k-k') \cdot SG_{k'}(\mathbb{F}, d)$, где k' - максимальное число линейно независимых мультипликативных членов. В случае $k = 3$ это число может быть равно только двум, поэтому от второго слагаемого получается 2.

Осталось вспомнить, откуда берется первое слагаемое. Величину $(k-1)(k-2)$ мы получили из поиска K-соответствия для мультипликативных членов схемы. Далее, уже для поиска ядра, за основу бралось именно множество K. Нужно показать, что уже его в случае $k = 3$ достаточно, чтобы получить ядро.

Рассмотрим схему $\mathcal{C} = T_1 + T_2 + T_3$. Пусть есть множество K ранга 2, такое, что существует K-соответствие между T_1 и T_2, а также между T_1 и T_3. По построению множества K сначала рассматривалась некоторая линейная форма l из T_1 и добавлялась в K. Очевидно, что T_2 и T_3 не содержат линейных форм, похожих на l, иначе они оба содержат такие формы и это противоречило бы простоте схемы. При этом, также из простоты схемы, T_1 и T_2 линейно независимы. Тогда получится, что $M(L_K(T_1))$ и $M(L_K(T_2))$ линейно независимы. Действительно, в первом случае обязательно имеется элемент в списке, который пропорционален l. Во втором случае такого нет из описанного выше. Следовательно, линейная независимость сохранилась. Получается, что от ядра в оценку ранга дает вклад только слагаемое $(k-1)(k-2)$, что в случае $k = 3$ равно 2.

Таким образом, при $k = 3$ и $\mathbb{F} = \mathbb{R}$ оценка на ранг действительно равна 4, и не зависит от степени схемы. Этот результат показывает, что хотя бы в этом случае результат сильно завышен и, возможно, получится сделать более точные оценки.

7 Вспомогательные леммы

Лемма 7.1. *Схема $\mathcal{C}$ глубины 3 с верхним слоем k и степенью $d > 0$ может быть полиномиальным алгоритом к схеме $\mathcal{C}' = \Sigma\Pi\Sigma(k, d)$ такой, что $\mathcal{C} \equiv 0 \Leftrightarrow \mathcal{C}' \equiv 0$. Такая схема называется соответствующей $\mathcal{C}$.*

Доказательство.

Пусть линейная форма

$$l_{ij} = l_{ij}^0 + \sum_{t=1}^{n} l_{ij}^t x_t$$

принадлежит схеме $\mathcal{C}$. Тогда введем новую переменную y и построим

$$l'_{ij} = l_{ij}^0 y + \sum_{t=1}^{n} l_{ij}^t x_t.$$

Теперь

$$C'(x,y) = \sum_{i=1}^{k} c_i y^{d-d_i} \prod_{j=1}^{d_i} l'_{ij}.$$

Представим

$$C(x) = \sum_{i=1}^{d} P_i(x),$$

где $P_i(x)$ - состовляющая степени i в C. Тогда очевидно, что

$$C(x) = \sum_{i=1}^{d} P_i(x) y^{d-i},$$

откуда и следует, что $C \equiv 0 \Leftrightarrow C' \equiv 0$.

■

Лемма 7.2. *(***Китайская теорема об остатках***)* *Пусть $h \in R$, f является мультипликативным членом, и идеал I порожден несколькими мультипликативными членами. Тогда $h \notin \langle I, f\rangle \Leftrightarrow \exists g \in nod_I(f) : h \notin \langle I, g\rangle$.*

8 Выводы

Как было сказано выше, даже схемы глубины 3 — достаточно сложная структура. Тем не менее, оценки на ранги тождеств дают надежду на то, что такие схемы имеют простой вид, что позволяет использовать идеи, аналогичные алгоритму, разобранному в этой работе. Соответственно, проверку для более простых структур придумать намного проще и она будет более эффективной. Более того, из случая $\mathbb{F} = \mathbb{R}$ можно сделать вывод, что оценка $O(k^2 \log d)$ на ранг является сильно завышеной хотя бы для случая такого поля.

Список литературы

[1] *Agrawal M., Biswas S.* Primality and Identity Testing via Chinese Remaindering. // FOCS, 1999.

[2] *Agrawal M., Saptharishi R.* Classifying Polynomial and Identity Testing. // 2009.

[3] *Agrawal M., Vinay V.* Arithmetic circuits: A chasm at depth four. // FOCS, 2008.

[4] *Grigoriev D., Karpinski M.* An exponential lower bound for depth 3 arithmetic circuits. // STOC, 1999.

[5] *Zhi-Zhong Chen, Ming-Yang Kao* Reducing Randomness via Irrational Numbers. // STOC, 1997.

[6] *Kayal N., Saraf S.* Blackbox polynomial identity testing for depth 3 circuits. // ECCC, 2009.

[7] *Kayal N., Saxena N.* Polynomial Identity Testing for Depth 3 Circuits. // ECCC, 2005.

[8] *Klivans A., Spielman D. A.* Randomness efficient identity testing of multivariate polynomials. // STOC, 2001.

[9] *Lewin D., Vadhan S. P.* Checking Polynomial Identities over any Field: Towards a Derandomization? // STOC, 1998.

[10] *Nisan N., Wigderson A.* Lower bounds on arithmetic circuits via partial derivatives. // FOCS, 1995.

[11] *Raz R., Yehudayoff A.* Multilinear formulas, maximal-partition discrepancy and mixed-sources extractors. // FOCS, 2008.

[12] *Shpilka A., Wigderson A.* Depth-3 arithmetic formulae over fields of characteristic zero. // COCO, 1999.

[13] *Dvir Z., Shpilka A., Yehudayoff A.* Hardness-randomness tradeoffs for bounded depth arithmetic circuits. // STOC, 2008.

[14] *Saxena N., Seshadri C.* Improved black-box identity test for depth-3 circuits. // STOC, 2010.

[15] *Arvind V., Mukhopadhyay P.* The monomial ideal mempership problem an polynomial identity testing. // ISAAC, 2007.

[16] *Gupta A., Kamath P., Kayal N., Saptarishi R.* Arithmetic circuits: A chasm at depth three. // 2013.

[17] *Arora S., Barak B.* Computational Complexity: A Modern Approach. // 2009.

[18] *Saxena N.* Diagonal circuit identity testing and lower bounds. // ICALP, 2008.

[19] *Shpilka A., Volkovich I.* Improved polunomial identity testing for read-one formulas. // RANDOM, 2009.