Московский государственный университет имени М. В. Ломоносова
Факультет вычислительной математики и кибернетики

На правах рукописи

Лысиков Владимир Владимирович

Некоторые вопросы теории сложности билинейных отображений

Специальность 01.01.09 – дискретная математика
и математическая кибернетика

Диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
д. ф.-м. н., профессор
Алексеев Валерий Борисович

Москва – 2013

Содержание

Введение

Теория сложности вычислений является одной из важнейших областей математической кибернетики. После появления компьютеров измерение эффективности используемых алгоритмов и исследование возможностей их улучшения стали важными практическими вопросами, изучение которых привело, в том числе, к появлению математической теории, в рамках которой исследуется различные характеристики эффективности алгоритмов в различных математических моделях вычислений. Наиболее важные из таких характеристик — это время работы алгоритма, т. е. количество элементарных шагов в рассматриваемой модели, и используемая память. Появление теории сложности вычислений можно отнести к пятидесятым годам XX века: Б. А. Трахтенброт в [30] утверждает, что исследования временной сложности алгоритмов в СССР начались в 1956 г., а М. Сипсер в [25] упоминает письмо К. Гёделя к Дж. фон Нейману, датируемое 1953 г. В настоящее время теория сложности вычислений является очень широкой областью исследований, включающей множество направлений и связанной практически со всеми областями математики.

Одним из направлений в теории сложности вычислений является алгебраическая теория сложности. Естественно, что алгоритмы, вычисляющие функции, связанные с какой-либо алгебраической струк-

турой на входных данных, например, алгоритмы умножения матриц или вычисления каких-либо полиномов, часто излагаются в терминах этой алгебраической структуры, независимо от того, как конкретно представляются входные данные. В связи с этим сложность вычисления таких функций удобно рассматривать в так называемых алгебраических моделях вычислений, в которых операции рассматриваемой алгебраической структуры считаются элементарными, несмотря на то, что на реальном компьютере они могут представляться не одной командой.

Одной из основных проблем алгебраической теории сложности является задача определения сложности умножения матриц. В 1969 г. был опубликован алгоритм Ф. Штрассена [27] для умножения квадратных матриц размера $n \times n$, имеющий сложность $O(n^{\log_2 7})$ арифметических операций вместо $O(n^3)$ для тривиального алгоритма, что положило начало исследованиям асимптотически быстрых алгоритмов умножения матриц. Штрассен также заметил связь алгоритмов умножения матриц с алгебраическим понятием тензорного ранга, что позволило применять для изучения сложности этих алгоритмов конструкции мультилинейной алгебры. После нескольких лет исследований в этой области Д. Копперсмитом и Ш. Виноградом [12] был получен алгоритм с асимптотической сложностью $O(n^{2.376})$. Недавние исследования с использованием компьютерных средств [26, 31, 36]

позволили улучшить эту оценку до $O(n^{2.373})$. Наилучшая известная на текущее время нижняя оценка сложности умножения квадратных матриц $3n^2 - o(n^2)$ была получена М. Лэндсбергом [18]. В случае, если в алгоритме разрешается использовать только ограниченные по модулю некоторой фиксированной константой коэффициенты, известна оценка вида $\Omega(n^2 \log n)$ [22]. Подробные обзоры истории верхних оценок сложности матричного умножения и применяемых для их получения методов содержатся в [32] и [5].

Понятие ранга тензора и связанная с ним техника могут быть применены не только к алгоритмам умножения матриц, но и к вычислению отображений из более широкого класса — билинейных отображений над полем или кольцом. В этом случае ранг тензора, соответствующего отображению, будет равен оптимальному количеству операций умножения в алгоритме, не учитывающем коммутативность координат аргументов. Эта мера сложности называется билинейной сложностью или рангом отображения. При рассмотрении алгоритмов, использующих коммутативность, получается другая мера сложности, называемая мультипликативной сложностью.

Важным классом билинейных отображений, включающим в себя умножение квадратных матриц, является класс ассоциативных алгебр, то есть билинейных отображений вида $A \times A \to A$, обладающих свойством ассоциативности. Этот класс отображений удобен тем, что

позволяет использовать классические результаты о структуре алгебр. Помимо того, что общие результаты о сложности ассоциативных алгебр включают в качестве частного случая результаты для сложности матричного умножения, результаты об ассоциативных алгебрах могут использоваться вместе с другими приемами для получения верхних или нижних оценок. Например, базовая конструкция в алгоритме Копперсмита-Винограда может быть интерпретирована как приближенный алгоритм для умножения в алгебре определенного вида. В связи с этим интересен вопрос о структуре алгебр с малой сложностью умножения.

В 1981 г. А. Алдером и Ф. Штрассеном [1] была получена нижняя оценка сложности умножения в алгебрах в терминах их структуры. Эта оценка оказалась неулучшаемой, в связи с чем возник вопрос об описании всех алгебр, на которых она достигается — алгебр минимального ранга и минимальной мультипликативной сложности. Эта задача решалась несколько десятков лет многими исследователями, окончательное описание было получено М. Блезером [3] для ранга и М. Блезером и Б. В. Чокаевым [6] для мультипликативной сложности. После этого в [7] М. Блезером и А. М. де Вольтером было начато изучение алгебр почти минимального ранга, т. е. алгебр, для которых билинейная сложность на 1 больше оценки Алдера-Штрассена. Одной из целей данной диссертации является продолжение этих исследо-

ваний. В диссертации обобщается результат Блезера и де Вольтера о полупростых алгебрах почти минимального ранга на случай произвольного основного поля, характеристика которого отлична от 2. Также получен критерий почти минимальности для класса локальных алгебр в терминах существования базисов определенного вида.

Для классификации полупростых алгебр почти минимального ранга были получены результаты, которые могут представлять самостоятельную ценность. Так, было получено точное значение сложности умножения обобщенных кватернионов. Оптимальный алгоритм умножения кватернионов над полем действительных чисел был получен в 70х годах [10, 13, 16], однако он не обобщается непосредственным образом на алгебры обобщенных кватернионов над произвольным полем. Задача об определении сложности умножения обобщенных кватернионов была отмечена в [7] как один из ключевых вопросов на пути к описанию алгебр почти минимального ранга.

Также была улучшена на единицу нижняя оценка Блезера для сложности умножения в матричных алгебрах [4]. Несмотря на то, что методы, использованные М. Лэндсбергом в [18] позволяют получить оценку, более сильную асимптотически, наш результат дает лучшую оценку для алгебр малой размерности.

Другой целью диссертации является исследование связи между алгоритмами вычисления билинейного отображения с целыми ко-

эффициентами (например, умножения матриц или полиномов) над полями различных характеристик. Мы докажем равенство рангов билинейного отображения с целочисленными коэффициентами над алгебраическими замкнутыми полями нулевой и простой характеристики, за исключением конечного числа простых характеристик. Ранее результаты, касающиеся связи сложности одного и того же билинейного отображения над различными кольцами и полями, были получены в [15] и [24]. Т. Д. Хауэлл первым отметил, что билинейная сложность отображения не возрастает при расширении кольца, над которым рассматриваются алгоритмы, а также доказал, что в некоторых условиях такое расширение не влияет на сложность, в частности, что минимальная сложность достигается при использовании в качестве основного кольца алгебраически замкнутого поля. А. Шёнхаге рассматривал сложность матричного умножения над различными полями одной характеристики. Он доказал, что асимптотика сложности матричного умножения над полями одной характеристики одинакова с точностью до постоянного множителя. Штрассен в [29] показал, что этот множитель не превосходит 4 при выполнении гипотезы Штрассена о прямой сумме.

Краткое содержание диссертации

В главе 1 приводятся основные определения и известные факты, касающиеся билинейных отображений, алгебр и билинейной сложности.

В главе 2 рассматриваются билинейные отображения малого ранга и алгоритмы умножения кватернионов.

В разделе 2.1 вводится понятие алгебры обобщенных кватернионов.

В разделе 2.2 рассматриваются алгоритмы для билинейных отображений, ранг которых равен сумме двух размерностей. Описывается структура алгоритмов для таких отображений в случае, если любой базис одного из пространств аргументов содержит регулярный элемент. Доказывается критерий почти минимальности ранга для локальных алгебр.

В разделе 2.3 описывается билинейный алгоритм умножения обобщенных кватернионов, имеющий сложность 8.

В разделе 2.4 рассматривается сложность умножения пар обобщенных кватернионов. Доказывается нижняя оценка 16 для этой сложности.

Глава 3 посвящена классификации полупростых алгебр пояти минимального ранга над бесконечным полем характеристики, отличной

от 2.

В разделе 3.1 рассматриваются простые алгебры, вопрос о почти минимальности которых разрешается с использованием уже известных нижних оценок.

В разделе 3.2 доказывается новая нижняя оценка билинейной сложности матричных алгебр над расширением основного поля и завершается классификация полупростых алгебр пояти минимального ранга.

В главе 4 рассматривается связь значений ранга $\mathbb{Z}$-билинейного отображения над полями различных характеристик.

В разделе 4.1 приводятся условия, при которых тензорное произведение двух модулей не явялется тривиальным.

В разделах 4.2 и 4.3 приводятся два разных доказательства основного результата главы, использующие различные методы. Доказано, что ранг $\mathbb{Z}$-билинейного отображения над алгебраически замкнутым полем характеристики 0, равен рангу этого отображения над всеми алгебраически замкнутыми полями простых характеристик, за исключением конечного числа.

Основные результаты диссертации

1. Описана структура оптимальных алгоритмов для класса билинейных отображений, ранг которых равен сумме размерностей аргументов.
2. Получен критерий почти минимальности ранга для локальных алгебр.
3. Описана конструкция билинейных алгоритмов ранга 8 для умножения в алгебрах обобщенных кватернионов над полем характеристики, отличной от 2.
4. Доказана нижняя оценка сложности умножения в матричных алгебрах над расширением основного поля, улучшающая известную оценку Блезера.
5. Полностью описана структура полупростых алгебр почти минимального ранга над бесконечным полем характеристики, отличной от 2.
6. Установлено, что значения ранга $\mathbb{Z}$-билинейного отображения над алгебраически замкнутыми полями различных характеристик совпадают за исключением конечного числа простых характеристик.

Глава 1

Основные понятия

1.1. Билинейные отображения и алгебры

Обычно в литературе по алгебраической теории сложности рассматриваются билинейные отображения векторных пространств над полем, но нам потребуется более общее определение, работающее над коммутативным кольцом, рассмотриваемое, например, в [15]. Аналогом понятия векторного пространства в этом случае является понятие модуля над кольцом (см. напр. [19, 34]).

Термин «кольцо» всюду в диссертации будет обозначать коммутативное кольцо с единицей.

Определение 1.1. Пусть S — кольцо. *Модулем* над S называется абелева группа $\langle M, + \rangle$ с операцией умножения на элементы кольца S, удовлетворяющей соотношениям

$$a(x + y) = ax + ay,$$

$$(a + b)x = ax + bx,$$

$$a(bx) = (ab)x,$$

$$1 \cdot x = x$$

для любых $a, b \in S$, $x, y \in M$.

Кольцо S называют *кольцом скаляров* модуля M, а его элементы — *скалярами*.

Обычным образом вводятся понятия гомоморфизма, изоморфизма, подмодуля и прямой суммы модулей.

Определение 1.2. Пусть S — кольцо, M и N — модули над S. Отображение $\varphi\colon M \to N$ называется *гомоморфизмом модулей*, если оно сохраняет операции сложения и умножения на скаляры из S, т. е.

$$\varphi(x+y) = \varphi(x) + \varphi(y),$$
$$\varphi(ax) = a\varphi(x)$$

для любых $a \in S$, $x, y \in M$.

Гомоморфизм, являющийся взаимно-однозначным отображением, называется *изоморфизмом*.

В случае, когда S — поле, гомоморфизмы модулей суть линейные операторы, а изоморфизмы — обратимые линейные операторы.

Определение 1.3. Подмножество N модуля M называется подмодулем, если оно замкнуто относительно операций сложения и умножения на скаляры, т.е. для любых $n_1, n_2 \in N$ и $a \in S$ сумма $n_1 + n_2$ и произведение an_1 также принадлежат N.

Определение 1.4. Пусть S — кольцо, M и N — модули над S. *Прямой суммой* модулей M и N называется модуль $M \oplus N$, состоящий

из пар вида (x, y), где $x \in M$, $y \in N$, с покоординатным сложением и умножением.

Из определения видно, что любое кольцо S может рассматриваться как модуль над собой. С помощью прямых сумм можно определить модуль $S^n = \underbrace{S \oplus S \oplus \cdots \oplus S}_{n \text{ раз}}$, элементами которого являются наборы длины n, составленные из элементов S. Под S^0 удобно понимать тривиальный модуль $\mathbf{0}$, состоящий из единственного элемента — нуля. Модули вида S^n наиболее близки по свойствам конечномерным векторным пространствам над полем, например, в них можно корректно ввести обобщения понятий базиса и линейной зависимости.

Определение 1.5. Пусть S — кольцо. Модуль M над S будем называть *конечномерным свободным модулем*, если $M \cong S^n$ для некоторого $n \geqslant 0$. Число n будем называть *размерностью*[†] *свободного модуля* M.

Определение 1.6. Пусть S — кольцо, M — модуль над S. Гомоморфизмы $f\colon M \to S$ будем называть *линейными функционалами* на M. Множество M^* всех линейных функционалов можно рассматривать

[†] Обычно в алгебре эту величину называют рангом свободного модуля, но мы используем термин «ранг» в другом смысле.

как модуль над S, если определить операции следующим образом:

$$(f+g)(x) = f(x) + g(x),$$
$$(af)(x) = a \cdot f(x)$$

для любых $f, g \in M^*$, $x \in M$, $a \in S$. Модуль M^* называется *сопряженным к M.*

Перечислим простейшие свойства конечномерных свободных модулей, которые обобщают аналогичные свойства конечномерных линейных пространств.

Утверждение 1.1 ([19, §III.6])**.** *Пусть S — кольцо, M — конечномерный свободный модуль над S. Справедливы следующие утверждения:*

1. *В M существует базис, то есть набор элементов $e_1, \ldots, e_n$ такой, что любой элемент $x \in M$ представляется в виде*

$$x = \sum_{i=1}^{n} x_i e_i, \quad x_i \in S$$

единственным образом. Количество элементов в базисе равно размерности M.

2. *Сопряженный модуль M^* также является конечномерным свободным модулем, его размерность совпадает с размерностью M.*

3. *Если* $e_1, \ldots, e_n$ *— базис* M*, то существуют линейные функционалы* $\varepsilon_1, \ldots, \varepsilon_n \in M^*$*, удовлетворяющие соотношению*

$$\varepsilon_i(e_j) = \delta_{ij}.$$

Эти функционалы образуют базис M^**, называемый сопряженным к базису* $e_1, \ldots e_n$*.*

4. *Любой линейный функционал* $f \in M^*$ *имеет вид*

$$f(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} x_i f_i,$$

где $f_i = f(e_i)$*.*

Определим теперь основные объекты, сложность которых мы будем изучать — билинейные отображения и алгебры.

Определение 1.7. Пусть S — кольцо, U, V, W — модули над S. Отображение $\varphi\colon U \times V \to W$ называется *билинейным*, если выполняются соотношения

$$\varphi(a_1x_1 + a_2x_2, y) = a_1\varphi(x_1, y) + a_2\varphi(x_2, y),$$
$$\varphi(x, a_1y_1 + a_2y_2) = a_1\varphi(x, y_1) + a_2\varphi(x, y_2)$$

для любых $a_1, a_2 \in S$, $x, x_1, x_2 \in U$, $y, y_1, y_2 \in V$.

В случае, если из контекста не ясно, какое кольцо S рассматривается, мы будем использовать термин «S-билинейное отображение».

Если U, V, W — конечномерные свободные модули, то для того, чтобы однозначно задать билинейное отображение φ, достаточно определить его значения на парах базисных элементов U и V. Действительно, пусть в U, V и W фиксированы базисы $(u_1, \ldots, u_n)$, $(v_1, \ldots v_m)$ и $(w_1, \ldots, w_l)$ соответственно. Если заданы значения

$$\varphi(u_i, v_j) = \sum_{k=1}^{l} t_{ijk} w_k, \tag{1.1}$$

то для произвольных $x = \sum\limits_{i=1}^{n} x_i u_i$ и $y = \sum\limits_{j=1}^{m} y_i v_i$ значение $\varphi(x, y)$ можно вычислить, исходя из билинейности:

$$\begin{aligned}\varphi(x, y) &= \varphi(\sum_{i=1}^{n} x_i u_i, \sum_{j=1}^{m} y_i v_i) = \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} x_i y_j \varphi(u_i, v_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{l} t_{ijk} x_i y_j w_k.\end{aligned}$$

Таким образом, для полного задания билинейного отображения достаточно задать nml коэффициентов $t_{ijk} \in S$.

Определение 1.8. Пусть S — кольцо. *Алгеброй* над S называется модуль A с заданной на нем билинейной операцией умножения. Алгебра называется *ассоциативной*, если умножение ассоциативно, т. е.

$$x(yz) = (xy)z \quad \text{для всех } x, y, z \in A,$$

и *коммутативной*, если

$$xy = yx \quad \text{для всех } x, y \in A.$$

Элемент $1 \in A$ называется *единицей*, если для любого $x \in A$ выполняется

$$1 \cdot x = x \cdot 1 = x.$$

В алгебре A с единицей элемент $a \in A$ называется *обратимым*, если существует $a^{-1} \in A$ такой, что

$$aa^{-1} = a^{-1}a = 1.$$

Обычным образом определяются гомоморфизмы и изоморфизмы алгебр как гомоморфизмы и изоморфизмы модулей, сохраняющие произведение, и подалгебры как подмодули, замкнутые относительно умножения.

Заметим, что любое кольцо S может рассматриваться как алгебра над $\mathbb{Z}$, если операцию умножения целого числа на элемент кольца определить обычным образом:

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n \text{ раз}}, \quad n > 0$$

$$(-n) \cdot a = -(n \cdot a), \quad n > 0$$

$$0 \cdot a = 0$$

1.2. Ассоциативные алгебры над полем

В главах 2 и 3 мы будем рассматривать сложность умножения в конечномерных ассоциативных алгебрах с единицей над полем. Тео-

рия таких алгебр является классическим разделом алгебры, результаты которого изложены во многих монографиях и учебных пособиях, напр. [21, 33, 35]. В этом разделе приведены основные определения и результаты этой теории, которыми мы будем пользоваться.

Термин «алгебра» будет обозначать конечномерную ассоциативную алгебру с единицей над некоторым полем F. Поле F можно рассматривать как подмножество алгебры A, если отождествить скаляры $\alpha \in F$ с элементами $\alpha \cdot 1 \in A$.

Определение 1.9. Подмодуль L алгебры A называется *левым идеалом*, если он замкнут относительно умножения на любой элемент алгебры слева, т. е. для любых $x \in A$, $l \in L$ произведение xl принадлежит L. Аналогично опредляются *правые идеалы*. Подмодуль, являющийся одновременно левым и правым идеалом, называется *двусторонним идеалом* или просто *идеалом*. Левый (правый, двусторонний) идеал называется *максимальным*, если он не содержится ни в каком левом (правом, двустороннем) идеале, кроме всей алгебры A.

Определение 1.10. Идеал называется *нильпотентным*, если для некоторого натурального n произведение любых n элементов идеала равно 0.

Алгебра называется *полупростой*, если она не имеет нильпотентных идеалов кроме тривиального идеала $\mathbf{0}$. Алгебра называется

простой, если она не имеет идеалов кроме $\mathbf{0}$ и всей алгебры. Алгебра называется *локальной*, если она имеет единственный максимальный левый идеал. Алгебра называется *алгеброй с делением*, если любой ее ненулевой элемент обратим.

Определение 1.11. Квадратные матрицы размера $n \times n$ с элементами из алгебры A с обычным образом определенным умножением образуют алгебру, которая обозначается $A^{n\times n}$ и называется *алгеброй матриц над* A.

Прямым произведением алгебр A и B называется алгебра $A \times B$, состоящая из пар вида (a, b), где $a \in A, b \in B$, с покоординатным умножением.

Теорема 1.1 (Дж. Веддербёрн, Э. Артин)**.** *Алгебра полупроста тогда и только тогда, когда она изоморфна прямому произведению конечного числа простых алгебр. Алгебра проста тогда и только тогда, когда она изоморфна алгебре матриц над некоторой алгеброй с делением.*

Определение 1.12. Коммутативная алгебра с делением над полем F сама является полем и называется *алгебраическим расширением поля* F.

Определение 1.13. Если D — алгебра с делением, то для любого элемента a множество элементов, представимых в виде линейной ком-

бинации степеней a, является расширением основного поля F, которое называется *расширением, порожденным элементом* a. Расширение, порожденное каким-либо своим элементом, называется *простым*.

1.3. Модель вычислений

Мы будем рассматривать сложность вычисления билинейных отображений конечномерных свободных модулей. В этом случае элементы модулей можно представлять в виде наборов координат в некотором фиксированном базисе, и можно рассматривать алгоритмы, которые по наборам координат аргументов вычисляют значение билинейного отображения. Элементарными операциями в таком алгоритме естественно считать операции над элементами кольца, над которым рассматривается отображение.

В процессе исследования задачи о сложности умножения матриц был выделен класс алгоритмов, обладающих определенной структурой: вначале над каждым из аргументов производятся линейные операции (умножение на константы и сложение), затем полученные таким образом промежуточные результаты перемножаются, и затем с помощью только линейных операций из произведений получаются координаты результата. Мерой сложности алгоритма при этом считается количество умножений на втором этапе, линейные операции

считаются «бесплатными». Дадим формальное определение.

Определение 1.14. Пусть S — кольцо, U, V, W — конечномерные свободные модули над S и $\varphi\colon U \times V \to W$ — билинейное отображение. *Билинейным алгоритмом* для φ называется последовательность троек $(f_1, g_1, z_1; f_2, g_2, z_2; \ldots; f_r, g_r, z_r)$, где $f_s \in U^*$, $g_s \in V^*$, $z_s \in W$, такая, что для любых $x \in U$, $y \in V$ выполняется

$$\varphi(x, y) = \sum_{s=1}^{r} f_s(x) g_s(y) z_s. \tag{1.2}$$

Количество троек r называется *сложностью билинейного алгоритма. Билинейной сложностью* или *рангом* отображения φ называется минимально возможная сложность билинейного алгоритма для этого отображения. Ранг отображения φ обозначается $R(\varphi)$.

Если алгебра A является конечномерным свободным модулем, то ее *билинейной сложностью* или *рангом* называется ранг умножения в ней. Ранг алгебры обозначается $R(A)$.

Определение билинейного алгоритма (1.2) можно записать также в координатной форме. Если отображение φ задано в некоторых базисах $(u_1, \ldots, u_n)$, $(v_1, \ldots, v_m)$, $(w_1, \ldots, w_l)$ соотношением вида (1.1) с коэффициентами t_{ijk}, а составляющие билинейного алгоритма f_s, g_s и z_s имеют в этих базисах координаты $f_i^{(s)}$, $g_j^{(s)}$ и $z_k^{(s)}$, т.е.

$$f_s(u_i) = f_i^{(s)}, \quad g_s(v_j) = g_j^{(s)}, \quad z_s = \sum_{k=1}^{l} z_k^{(s)} w_k,$$

то определение билинейного алгоритма переписывается в виде

$$t_{ijk} = \sum_{s=1}^{r} f_i^{(s)} g_j^{(s)} z_k^{(s)}. \tag{1.3}$$

Одним из основных методов получения нижних оценок в алгебраической теории сложности является метод подстановки, при котором оценки сложности функций от большого числа переменных сводятся к оценкам для функций с меньшим числом переменных путем подстановки линейных комбинаций новых переменных вместо старых. Приведем основные леммы, позволяющие использовать этот метод в модели билинейных алгоритмов.

Определение 1.15. *Левым ядром* $\operatorname{lker}\varphi$ билинейного отображения $\varphi\colon U \times V \to W$ называется множество всех $u \in U$ таких, что для любого $v \in V$ имеет место $\varphi(u, v) = 0$. Аналогично определяется *правое ядро* $\operatorname{rker}\varphi$.

Лемма 1.1. *Пусть* $\varphi\colon U \times V \to W$ *— билинейное отображение. Если* $\operatorname{lker}\varphi = \mathbf{0}$*, то в любом билинейном алгоритме* $(f_1, g_1, z_1; \ldots; f_r, g_r; z_r)$ *для* φ *функционалы* f_k *порождают в линейной оболочке все пространство* U^*

Доказательство. Допустим, что линейная оболочка набора функционалов $\{f_1, \ldots, f_r\}$ не совпадает с пространством U^*. В этом случае существует ненулевой элемент $u \in U$ такой, что $f_1(u) = \cdots = f_r(u) = 0$.

Из определения билинейного алгоритма следует, что $\varphi(u, v) = 0$ для любого $v \in V$, т.е. $u \in \operatorname{lker} \varphi$. $\square$

Заметим, что условие доказанной леммы верно, если φ — умножение в некоторой алгебре с единицей.

Лемма 1.2. *Пусть $\varphi\colon U \times V \to W$ — билинейное отображение, $(f_1, g_1, z_1; \ldots; f_r, g_r, z_r)$ — билинейный алгоритм для φ, а U' — подпространство U. Тогда*

$$r \geqslant q + R(\varphi|_{U' \times V}),$$

где q — количество функционалов f_k, равных тождественно нулю на U'

Доказательство. Ограничив все функционалы f_k на подпространство U', мы получим алгоритм $(f_1|_{U'}, g_1, z_1; \ldots; f_r|_{U'}, g_r, z_r)$ для отображения $\varphi|_{U' \times V}$. В нем тройки, для которых $f_k|_{U'} = 0$ можно опустить, после чего получится алгоритм для $\varphi|_{U' \times V}$ сложности $r - q$, существование которого означает, что $R(\varphi|_{U' \times V}) \leqslant r - q$. $\square$

А. Алдером и Ф. Штрассеном в [1] была получена нижняя оценка сложности умножения в ассоциативных алгебрах над полем.

Теорема 1.2 (А. Алдер, Ф. Штрассен)**.** *Пусть F — поле, A — конечномерная ассоциативная алгебра с единицей над F. Для ранга*

алгебры A справедлива оценка

$$R(A) \geqslant 2 \dim A - t(A),$$

где $t(A)$ — количество максимальных двусторонних идеалов алгебры A.

В случае, если эта оценка достигается, алгебра A называется *алгеброй минимального ранга*, а если ранг алгебры на единицу больше оценки Алдера-Штрассена — *алгеброй почти минимального ранга.*

Для алгебр с делением справедлива следующая более сильная оценка.

Теорема 1.3 (У. Баур, см. [11, теорема 17.27])**.** *Если D — алгебра с делением, то существует элемент $a \in D$ такой, что справедлива нижняя оценка*

$$R(D) \geqslant 2 \dim D - 2 + \frac{\dim D}{\dim F(a)}.$$

Для оценки сложности отображений с малой размерностью одного из пространств аргументов можно использовать следующую нижнюю оценку:

Теорема 1.4 (Ф. Штрассен, см. [28])**.** *Пусть F — поле, $\varphi\colon F^3 \times U \to U$ — билинейное отображение, и операторы A_i определяются соотношением $A_i x = \varphi(e_i, x)$, причем A_1 невырожден. Тогда*

$$R(\varphi) \geqslant \dim U + \frac{1}{2} \operatorname{rk}[A_1^{-1}A_2, A_1^{-1}A_3].$$

Де Гроотом в [14] была построена теория эквивалентных преобразований билинейных алгоритмов.

Определение 1.16. Пусть S — кольцо, U, V, W — конечномерные свободные модули над S, и $\varphi\colon U \times V \to W$ — билинейное отображение. Множество троек (F, G, H), элементы которых являются автоморфизмами модулей U, V и W соответственно, удовлетворяющих условию

$$H\varphi(Fx, Gy) = \varphi(x, y)$$

для любых $x \in U, y \in V$, образует группу относительно покомпонентной композиции. Эта группа называется *группой изотропии* отображения φ и обозначается $\Gamma^{\circ}(\varphi)$.

Отображения из группы изотропии позволяют получать из билинейных алгоритмов для φ новые билинейные алгоритмы.

Утверждение 1.2. *Пусть S — кольцо, U, V, W — конечномерные свободные модули над S, и $\varphi\colon U \times V \to W$ — билинейное отображение. Если $(f_1, g_1, z_1; \ldots; f_r, g_r, z_r)$ — билинейный алгоритм для φ, то $(\hat{f}_1, \hat{g}_1, \hat{z}_1; \ldots; \hat{f}_r, \hat{g}_r, \hat{z}_r)$, где $\hat{f}_s = f_s \circ F$, $\hat{g}_s = g_s \circ G$, $\hat{z}_s = Hz_s$, также будет билинейным алгоритмом для φ.*

Доказательство. Непосредственно следует из определений:

$$\sum_{s=1}^{r} \hat{f}_s(x)\hat{g}_s(y)\hat{z}_s = \sum_{s=1}^{r} f_s(Fx)g_s(Gy)Hz_s =$$

$$= H(\sum_{s=1}^{r} f_s(Fx)g_s(Gy)z_s) = H\varphi(Fx, Gy) = \varphi(x, y). \qquad \square$$

Определение 1.17. Билинейные алгоритмы $(f_1, g_1, z_1; \ldots; f_r, g_r, z_r)$ и $(\hat{f}_1, \hat{g}_1, \hat{z}_1; \ldots; \hat{f}_r, \hat{g}_r, \hat{z}_r)$ для φ называются *эквивалентными*, если они получаются друг из друга преобразованием, описанным в предыдущем утверждении, т. е.

$$\hat{f}_s = f_s \circ F, \quad \hat{g}_s = g_s \circ G, \quad \hat{z}_s = Hz_s$$

для некоторой тройки $(F, G, H) \in \Gamma^{\circ}(\varphi)$.

Если A — ассоциативная алгебра над S и a, b, c — некоторые ее обратимые элементы, то тройка

$$F\colon x \mapsto axb^{-1}, \quad G\colon y \mapsto byc^{-1}, \quad H\colon z \mapsto azc^{-1}$$

является элементом группы изотропии умножения в A. Соответствующее эквивалентное преобразование часто применяется при изучении сложности умножения в алгебрах для приведения некоторых слагаемых алгоритма к какому-либо каноническому виду.

1.4. Тензорные произведения и расширение кольца скаляров

В данном разделе термин «алгебра» будет обозначать коммутативную ассоциативную алгебру с единицей над кольцом, так что любая алгебра над кольцом также является кольцом.

Введем конструкцию тензорного произведения модулей. Это основная конструкция мультилинейной алгебры, которая широко используется при изучении колец и их модулей (см. напр. [9, 19]).

Определение 1.18. Пусть S — кольцо, M и N — модули над S. *Тензорным произведением* модулей M и N будем называть модуль $M \otimes_S N$, состоящий из формальных сумм вида $\sum_{i=1}^{t} m_i \otimes n_i$, где $m_i \in M, n_i \in N$. Два элемента в $M \otimes N$ равны тогда и только тогда, когда они приводятся друг к другу с помощью следующих эквивалентных преобразований:

$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \tag{1.4a}$$

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \tag{1.4b}$$

$$a(m \otimes n) = (am) \otimes n = m \otimes (an) \tag{1.4c}$$

для любых $a \in S$, $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$.

Элементы тензорного произведения называются *тензорами*. Тензоры вида $m \otimes n$ называются *разложимыми*.

Утверждение 1.3 ([17, §X.5]). *Имеют место следующие изоморфизмы*

$$M \otimes_S N \cong N \otimes_S M$$

$$M \otimes_S (N \otimes_T L) \cong (M \otimes_S N) \otimes_T L$$

$$S \otimes_S M \cong M \otimes_S S \cong M$$

$$M \otimes_S (N_1 \oplus N_2) \cong (M \otimes_S N_1) \oplus (M \otimes_S N_2)$$

В случае, если один или оба модуля в тензорном произведении являются алгебрами, на тензорном произведении также можно ввести дополнительную структуру.

Определение 1.19. Пусть S — кольцо, A и B — алгебры над S. На тензорном произведении $A \otimes_S B$ можно ввести структуру алгебры над S, если определить операцию умножения на разложимых тензорах как

$$(a \otimes b)(c \otimes d) = (ac) \otimes (bd),$$

и распространить на все $A \otimes_S B$ по билинейности. Эта алгебра называется *тензорным произведением алгебр* A и B.

Определение 1.20. Пусть S — кольцо, A — алгебра над S, а M — модуль над S. На тензорном произведении $A \otimes_S M$ можно ввести структуру модуля над A, определив умножение следующим образом:

$$a(\sum_{i=1}^{t} a_i \otimes m_i) = \sum_{i=1}^{t} (aa_i) \otimes m_i$$

для любых $a, a_i \in A$, $m_i \in M$. Будем говорить, что этот модуль получен из M *расширением кольца скаляров до* A.

Эти определения корректны, т. е. определенные операции согласованы с равенством тензоров (1.4) (см. напр. [19, §§XVI.4-6]).

Так как любое кольцо является алгеброй над $\mathbb{Z}$, можно рассматривать тензорные произведения колец. На таком произведении можно ввести структуру кольца в соответствии с определением 1.19 и алгебры над каждым из сомножителей в соответствии с определением 1.20.

Из утверждения 1.3 видно, что расширение кольца скаляров с S до A переводит конечномерный свободный модуль S^n в конечномерный свободный модуль той же размерности A^n. Более того, если $e_1, \ldots, e_n$ — базис S^n, то любой элемент $A \otimes_S S^n$ может быть представлен в виде $\sum_{i=1}^{n} a_i \otimes e_i$ для некоторых $a_i \in A$, то есть если элементы исходного модуля представлять наборами координат в некотором базисе, то элементы расширенного представляются аналогичными наборами, но их координаты принимают значения из A, а не из S. Такой подход позволяет рассмотреть алгоритмы вычисления S-билинейных отображений, которые используют в качестве промежуточных результатов элементы некоторой алгебры над S. В некоторых случаях такие алгоритмы будут иметь меньший ранг, чем алгоритмы, использующие только элементы основного кольца.

Определение 1.21. Пусть S — кольцо, A — алгебра над S, а U, V и W — конечномерные свободные модули над S. Для любого S-билинейного отображения $\varphi\colon U \times V \to W$ определим A-билинейное отображение $\varphi^A\colon (A \otimes U) \times (A \otimes V) \to (A \otimes W)$ на элементах вида $1 \otimes x$ как

$$\varphi^A(1 \otimes x, 1 \otimes y) = 1 \otimes \varphi(x, y),$$

а на произвольных тензорах исходя из свойства A-билинейности, т. е.

$$\varphi^A(\sum_{i=1}^{n} a_i \otimes x_i, \sum_{j=1}^{m} b_j \otimes y_j) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j \otimes \varphi(x_i, y_j).$$

Будем говорить, что отображение φ^A получено из φ *расширением кольца скаляров до* A. Любой билинейный алгоритм для φ^A будем называть *билинейным алгоритмом для* φ *над* A. Ранг отображения φ^A будем называть *рангом* φ *над* A и обозначать $R_A(\varphi)$.

Многие важные билинейные отображения, например, умножение матриц или полиномов, являются $\mathbb{Z}$-билинейными, что значит, что можно рассматривать их сложность над произвольным кольцом. Интересен вопрос о том, как связаны значения ранга $\mathbb{Z}$-билинейного отображения φ над различными кольцами. Ясно, что если A — алгебра над S, то каждому билинейному алгоритму $(f_1, g_1, z_1; \ldots; f_r, g_r, z_r)$ над S соответствует билинейный алгоритм $(\hat{f}_1, \hat{g}_1, \hat{z}_1; \ldots; \hat{f}_r, \hat{g}_r, \hat{z}_r)$ над A, где $\hat{f}_s(a \otimes x) = a f_s(x)$, $\hat{g}_s(a \otimes y) = a g_s(y)$, $\hat{z}_s = 1 \otimes z_s$, то есть

$R_S(\varphi) \geqslant R_A(\varphi)$. Этот факт впервые был замечен Т. Д. Хауэллом в работе [15], где также были рассмотрены некоторые случаи, в которых это неравенство обращается в равенство, то есть переход к алгебре не дает преимуществ при вычислении φ.

Теорема 1.5 (Т. Д. Хауэлл)**.** *Пусть S — кольцо, A — алгебра над S. Для любого S-билинейного отображения φ имеет место неравенство $R_S(\varphi) \geqslant R_A(\varphi)$.*

Для любого кольца S и любого S-билинейного отображения φ справедливо равенство $R_S(\varphi) = R_{S[x]}(\varphi)$.

Если F — алгебраически замкнутое поле, то для любой алгебры A над F, $A \neq \mathbf{0}$, и для любого F-билинейного отображения φ справедливо равенство $R_F(\varphi) = R_A(\varphi)$.

Позже Шёнхаге [24] исследовал вопрос о связи ранга над полями одной характеристики и показал, что при переходе от поля к его расширению ранг уменьшается не более, чем в константное количество раз. В последней главе данной диссертации мы рассмотрим связь рангов над полями различных характеристик.

Глава 2

Алгоритмы умножения обобщенных кватернионов

В данной главе доказывается критерий почти минимальности ранга локальной алгебры в терминах существования базисов определенного вида. С помощью этого критерия построен билинейный алгоритм ранга 8 для умножения обобщенных кватернионов над полем характеристики, отличной от 2. Результаты этой главы опубликованы в [37, 38].

2.1. Алгебры обобщенных кватернионов

Для классификации алгебр почти минимального ранга нам потребуется рассмотреть сложность умножения в алгебрах обобщенных кватернионов. Это некоммутативные ассоциативные алгебры, обобщающие на случай произвольного основного поля F конструкцию алгебры кватернионов, открытую У. Р. Гамильтоном в XIX в.

Определение 2.1. *Центром* алгебры A называется подалгебра, состоящая из элементов, коммутирующих с любым элементом алгебры:

$$C(A) = \{x | xa = ax \ \forall a \in A\}.$$

Алгебра над F называется *центральной*, если ее центр совпадает с F.

Определение 2.2. Алгеброй обобщенных кватернионов над F называется простая центральная алгебра размерности 4.

Структура алгебр обобщенных кватернионов определяется следующими утверждениями:

Теорема 2.1 (см. [8]). *Если* $\operatorname{char} F \neq 2$, *то любая алгебра обобщенных кватернионов порождается двумя элементами* i *и* j, *удовлетворяющими условиям*

$$i^2 = p, \quad j^2 = q, \quad ij = -ji,$$

где $p, q \in F$, $p, q \neq 0$. *Элементы* 1, i, j, $k = ij$ *образуют базис алгебры. Такую алгебру будем обозначать* $\left(\frac{F}{p,q}\right)$.

Теорема 2.2 (см. [8]). *Если* $\operatorname{char} F = 2$, *то любая алгебра обобщенных кватернионов порождается двумя элементами* i *и* j, *удовлетворяющими условиям*

$$i(i+1) = p, \quad j^2 = q, \quad ij = j(i+1),$$

где $p, q \in F$, $q \neq 0$. *Элементы* 1, i, j, $k = ij$ *образуют базис алгебры.*

Теорема 2.3 (см. [8]). *Любая алгебра обобщенных кватернионов либо изоморфна алгебре матриц* $F^{2\times 2}$, *либо является некоммутативной алгеброй с делением. Любая некоммутативная алгебра с делением размерности* 4 *является алгеброй обобщенных кватернионов.*

2.2. Билинейные отображения малого ранга

Прежде чем обратиться к сложности умножения кватернионов, мы докажем некоторые общие утверждения о билинейных алгоритмах, ранг которых равен сумме размерностей пространств аргументов.

Определение 2.3. Пусть F — поле, U, V, W — векторные пространства над F, и $\varphi\colon U \times V \to W$ — билинейное отобоажение. Назовем элемент $u_0 \in U$ *(левым) φ-регулярным*, если линейный оператор $\varphi(u_0, \cdot)$ инъективен, т.е. $\varphi(u_0, v) = 0$ тогда и только тогда, когда $v = 0$.

Определение 2.4. Билинейный алгоритм $(f_1, g_1, z_1; \ldots; f_r, g_r, z_r)$ будем называть *двухкомпонентным*, если множество индексов $\{1,\ldots, r\}$ можно разбить на непересекающиеся множества I и J такие, что $\{f_i | i \in I\}$ и $\{g_j | j \in J\}$ являются базисами пространств U^* и V^* соответственно.

Лемма 2.1. *Пусть F — поле, U, V, W — векторные пространства над F, и $\varphi\colon U \times V \to W$ — билинейное отобоажение. Если $R(\varphi) = \dim U + \dim V$, $\operatorname{lker} \varphi = \mathbf{0}$, и в любом базисе пространства U найдется φ-регулярный элемент, то любой оптимальный билинейный алгоритм для φ является двухкомпонентным.*

Доказательство. Пусть $\dim U = m$, $\dim V = n$. Рассмотрим опти-

мальный билинейный алгоритм $(f_1, g_1, z_1; \ldots; f_{m+n}, g_{m+n}, z_{m+n})$ для φ. Так как $\operatorname{lker}\varphi = \mathbf{0}$, функционалы $f_1, \ldots, f_{m+n}$ порождают все пространство U^*. Пусть, без ограничения общности, $f_1, \ldots, f_m$ — базис U^*, а элемент u_1 двойственного базиса $u_1, \ldots, u_m$ является φ-регулярным. Из φ-регулярности u_1 следует, что функционалы $g_1, g_{m+1}, \ldots, g_{m+n}$ порождают все пространство V^*, так как иначе существует ненулевой элемент v такой, что $g_1(v) = g_{m+1}(v) = \cdots = g_{m+n}(v) = 0$, и из определения билинейного алгоритма следует, что $\varphi(u_1, v) = 0$.

Обозначим через G линейную оболочку множества функционалов $\{g_{m+1}, \ldots, g_{m+n}\}$. Если G есть все пространство V^*, то множества индексов $I = \{1, \ldots, m\}$ и $J = \{m+1, \ldots, m+n\}$ образуют разбиение, требуемое в определении двухкомпонентного алгоритма. В противном случае $\dim G = n - 1$ и существует единственная с точностью до умножения на константу линейная зависимость между $g_{m+1}, \ldots, g_{m+n}$. Пусть, без ограничения общности, $g_{m+1}, \ldots, g_{m+s}$ входят в уравнение линейной зависимости с ненулевыми коэффициентами, а остальные функционалы — с нулевыми.

Если найдется f_p с $m + 1 \leqslant p \leqslant m + s$ такой, что в разложении его по базису $f_1, \ldots, f_m$ элемент f_1 присутствует с ненулевым коэффициентом, то множества индексов $I = \{2, \ldots, m, p\}$ и $J = \{1, m+1, \ldots, m+n\} \setminus \{p\}$ образуют требуемое разбиение. Иначе рассмотрим функционалы $g_1, g_{m+s+1}, \ldots, g_{m+n}$. Эти функционалы не

могут порождать все V^*, так как их количество меньше размерности $\dim V = n$. Взяв ненулевой элемент $v_0 \in V$ такой, что

$$g_1(v_0) = g_{m+s+1}(v_0) = \cdots = g_{m+n}(v_0) = 0,$$

получим, что $\varphi(u_1, v_0) = 0$, поскольку $f_k(u_1) = 0$ при $2 \leqslant k \leqslant m$ по определению u_1 и при $m+1 \leqslant k \leqslant m+s$, так как все f_k с индексами из этого промежутка не содержат f_1 в разложении по базису $(f_1, \ldots, f_m)$. Получаем противоречие с φ-регулярностью элемента u_1. □

Теорема 2.4. *Пусть F — поле, U, V, W — векторные пространтсва над F, и $\varphi\colon U \times V \to W$ — билинейное отображение. Двухкомпонентный билинейный алгоритм для φ существует тогда и только тогда, когда существуют базисы $u_1, \ldots, u_m$ и $v_1, \ldots, v_n$ пространств U и V соответственно, и наборы $z'_1, \ldots, z'_m$ и $z''_1, \ldots, z''_n$ элементов W такие, что*

$$\varphi(u_i, v_j) = \lambda_{ij} z'_i + \mu_{ij} z''_j \tag{2.1}$$

для некоторых коэффициентов $\lambda_{ij}, \mu_{ij} \in F$.

Доказательство. Пусть существует двухкомпонентный билинейный алгоритм для φ. Без ограничения общности, он имеет вид

$$(f_1, G_1, z'_1; \ldots; f_m, G_m, z'_m;\ F_1, g_1, z''_1; \ldots; F_n, g_n, z''_n),$$

где $f_1, \ldots, f_m$ и $g_1, \ldots, g_n$ — базисы соответствующих пространств.

Пусть $u_1, \ldots, u_m$ и $v_1, \ldots, v_n$ — двойственные им базисы. Тогда

$$\varphi(u_i, v_j) = G_i(v_j)z'_i + F_j(u_i)z''_j.$$

Обратно, если существуют базисы $u_1, \ldots, u_m$ и $v_1, \ldots, v_n$ и наборы $z'_1, \ldots, z'_m, z''_1, \ldots, z''_n$ такие, что $\varphi(u_i, v_j) = \lambda_{ij}z'_i + \mu_{ij}z''_j$, а $f_1, \ldots, f_m$ и $g_1, \ldots, g_n$ — базисы, двойственные к (u_i) и (v_j) соответственно, то билинейный алгоритм

$$(f_1, \sum_{j=1}^{n} \lambda_{1j}g_j, z'_1; \ldots; f_m, \sum_{j=1}^{n} \lambda_{mj}g_j, z'_m; \sum_{i=1}^{m} \mu_{i1}f_i, g_1, z''_1; \ldots; \sum_{i=1}^{m} \mu_{in}f_i, g_n, z''_n)$$

вычисляет φ. Для того, чтобы проверить это, заметим, что в силу билинейности определение билинейного алгоритма (1.2) достаточно проверить на парах (u_i, v_j) элементов базисов, а на этих парах оно обращается в равенство (2.1). □

Этот результат позволяет получить критерий почти минимальности для локальных алгебр и, в частности, для алгебр с делением. Если φ — умножение в алгебре, φ-регулярные элементы суть обратимые элементы алгебры. Справедливо следующее утверждение об обратимости элементов в локальной алгебре:

Теорема 2.5 ([35, теорема III.2.2]). *Элемент локальной алгебры обратим тогда и только тогда, когда он не содержится в максимальном*

левом идеале.

Поскольку в локальной алгебре обратимы те и только те элементы, которые не лежат в единственном максимальном идеале (в частности, в алгебре с делением обратимы все элементы), любой базис локальной алгебры содержит обратимый элемент. Используя этот факт мы можем связать существование алгоритмов ранга $2 \dim A$ с существованием базисов, обладающих определенными свойствами.

Теорема 2.6. *Пусть F — поле, A — локальная алгебра над F, $\dim A = n$. Если A не является алгеброй минимального ранга, то есть $R(A) \geqslant 2n$, то A имеет почти минимальный ранг тогда и только тогда, когда в A существует пара базисов $u_1 = 1, u_2, \ldots, u_n$ и $v_1 = 1, v_2, \ldots, v_n$ и пара наборов элементов $z'_1, \ldots, z'_n$ и $z''_1, \ldots, z''_n$ такие, что*

$$u_i v_j = \lambda_{ij} z'_i + \mu_{ij} z''_j \tag{2.2}$$

для некоторых $\lambda_{ij}, \mu_{ij} \in F$.

Доказательство. Так как в каждом базисе локальной алгебры существует обратимый элемент, любой алгоритм ранга $2n$ является двухкомпонентным, а двухкомпонентный алгоритм обеспечивает существование базисов и наборов, удовлетворяющих соотношению (2.2). При этом элементы u_1 и v_1 можно взять равными 1, так как эквива-

лентное преобразование $u \mapsto u_1^{-1}u$, $v \mapsto vv_1^{-1}$, $z \mapsto u_1^{-1}zv_1^{-1}$ не влияет на выполнение соотношения (2.2). $\square$

2.3. Сложность умножения обобщенных кватернионов

Докажем, что алгебры обобщенных кватернионов над полем характеристики, отличной от 2, являются алгебрами почти минимального ранга.

Теорема 2.7. *Пусть F — поле,* $\operatorname{char} F \neq 2$, *$H$ — алгебра обобщенных кватернионов с делением над F. Тогда $R(H) = 8$.*

Доказательство. Так как любое подполе алгебры обощенных кватернионов имеет размерность 1 или 2, по теореме 1.3 имеет место нижняя оценка $R(H) \geqslant 8$. В силу результатов предыдущего раздела, для доказательства того, что $R(H) = 8$, достаточно привести пример пары базисов $u_1, \ldots, u_4$ и $v_1, \ldots, v_4$ и пары наборов $z_1', \ldots, z_4'$ и $z_1'', \ldots, z_4''$, удовлетворяющих условию (2.2).

Напомним, что по теореме 2.1 в H существует базис $1, i, j, k$ такой, что $i^2 = p \in F$, $j^2 = q \in F$, $ij = -ji = k$. Возьмем в качестве u_i и v_j этот стандартный кватернионный базис:

$$(u_1, u_2, u_3, u_4) = (v_1, v_2, v_3, v_4) = (1, i, j, k),$$

а наборы z'_i и z''_j определим следующим образом:

$$\begin{aligned}(z'_1, z'_2, z'_3, z'_4) = (&1 + \alpha i + \beta j + \gamma k, 1 + \alpha i - \beta j - \gamma k,\\ &1 - \alpha i + \beta j - \gamma k, 1 - \alpha i - \beta j + \gamma k),\\ (z''_1, z''_2, z''_3, z''_4) = (&1 - \alpha i - \beta j - \gamma k, 1 - \alpha i + \beta j + \gamma k,\\ &1 + \alpha i - \beta j + \gamma k, 1 + \alpha i + \beta j - \gamma k),\end{aligned}$$

где α, β, γ — некоторые ненулевые константы из F. Непосредственно проверяется, что условие (2.2) для указанных кватернионов выполняется с коэффициентами, указанными в табл. 2.1.

Учитывая нижнюю оценку $R(H) \geqslant 8$, получаем, что 8 является точным значением ранга H. □

2.4. Ранг произведения алгебр обобщенных кватернионов

Теорема 2.8. *Пусть F — поле. Если H_1 и H_2 — алгебры обобщенных кватернионов с делением над F, а $A = H_1 \times H_2$, то $R(A) = 16$.*

Доказательство. Верхняя оценка $R(A) \leqslant 16$ следует из теоремы 2.7. Докажем нижнюю оценку. В тексте доказательства будем отождествлять H_1 и H_2 с их образами в A.

Пусть $(f_1, g_1, z_1; \ldots; f_r, g_r, z_r)$ — билинейный алгоритм для умножения в A. Так как A — алгебра с единицей, функционалы f_k порождают все пространство A^*.

Если каждый из функционалов f_k равен нулю либо на H_1, либо на H_2, то, рассмотрев по отдельности тройки алгоритма, соответствующие тем и другим, мы получим билинейные алгоритмы для H_2 и для H_2 соответственно, и поскольку ранг каждого из них меньше 8, ранг исходного алгоритма не меньше 16.

В противном случае найдется функционал, не равный нулю ни на H_1, ни на H_2. Для базиса, содержащего такой функционал, в двойственном базисе будет присутствовать обратимый элемент A, то есть элемент вида $a = (a', a'')$ с ненулевыми a' и a''. При применении эквивалентного преобразования $x \mapsto a^{-1}x, z \mapsto a^{-1}z$ этот элемент переходит в 1. Таким образом, без ограничения общности можно считать, что $f_1, \ldots, f_8$ — базис, $u_1 = 1, u_2, \ldots, u_8$ — двойственный базис. В базисе $u_1, \ldots, u_8$ найдется такой элемент $u_i = (u_i', u_i'')$, что $u_i' \notin F$. Пусть, без ограничения общности, этот элемент — u_2.

Убрав из алгоритма слагаемые с индексами $3 \leqslant k \leqslant 8$ и ограничив все f_k на линейную оболочку U пары элементов $\{1, u_2\}$, мы получим алгоритм $(f_1|_U, g_1, z_1; f_2|_U, g_2, z_2; f_9|_U, g_9, z_9; \ldots; f_r|_U, g_r, z_r)$ для отображения, полученного ограничением умножения на $U \times A$, причем $f_1|_U, f_2|_U$ — двойственный базис к базису $1, u_2$ подпространства U.

Докажем, что сложность этого алгоритма не меньше 10. Допустим, она равна 9, т. е. $r = 15$. Функционалы g_k при $k = 1, 9, \ldots, 15$ образуют базис A^*, так как в противном случае, взяв ненулевой элемент v, на котором они все равны нулю, получим $1 \cdot v = 0$. Пусть $v_1, v_9 \ldots, v_{15}$ — двойственный к $g_1, g_9, \ldots, g_{15}$ базис. Тогда

$$v_j = 1 \cdot v_j = f_j(1)z_j, \quad u_2 v_j = f_j(u_2)z_j + g_2(v_j)z_2.$$

Так как $v_j \neq 0$, из первого равенства следует, что $f_j(1) \neq 0$. Вычитая из второго равенства первое с коэффициентом $\frac{f_j(u_2)}{f_j(1)}$, получаем

$$(u_2 - \frac{f_j(u_2)}{f_j(1)})v_j = g_2(v_j)z_2. \tag{2.3}$$

Аналогичное равенство должно выполняться для первых компонент соответствующих элементов. Так как v_j — базис, можно выбрать четыре элемента $v_{j_1} = (v'_1, v''_1), \ldots, v_{j_4} = (v'_4, v''_4)$ такие, что их первые компоненты $v'_1, \ldots, v'_4$ образуют базис H_1. Пусть также $z_2 = (z'_2, z''_2)$. Таким образом, равенство (2.3) для первых компонент имеет вид

$$(u'_2 - \frac{f_j(u_2)}{f_j(1)})v'_k = g_2(v_{j_k})z'_2.$$

Так как u_2 было выбрано так, что $u'_2 \notin F$, имеем $z'_2 \neq 0$. Получаем, что для элементов базиса $v'_1(z'_2)^{-1}, \ldots, v'_4(z'_2)^{-1}$ выполнено

$$v'_k(z'_2)^{-1} = (u'_2 - \frac{f_j(u_2)}{f_j(1)})^{-1} \in F(u'_2),$$

то есть $H_1 = F(u_2')$, что противоречит некоммутативности алгебры H_1.

□

Таким образом, алгебра $A = H_1 \times H_2$ не является алгеброй почти минимального ранга, так как она имеет два максимальных идеала (а именно, H_1 и H_2) и ранг $16 > 2 \dim A - 2 + 1$.

	v_1	v_2	v_3	v_4
u_1	$\frac{1}{2}z_1' + \frac{1}{2}z_1''$	$\frac{1}{2\alpha}z_1' - \frac{1}{2\alpha}z_2''$	$\frac{1}{2\beta}z_1' - \frac{1}{2\beta}z_3''$	$\frac{1}{2\gamma}z_1' - \frac{1}{2\gamma}z_4''$
u_2	$\frac{1}{2\alpha}z_2' - \frac{1}{2\alpha}z_1''$	$\frac{p}{2}z_2' + \frac{p}{2}z_2''$	$-\frac{1}{2\gamma}z_2' + \frac{1}{2\gamma}z_3''$	$-\frac{p}{2\beta}z_2' + \frac{p}{2\beta}z_4''$
u_3	$\frac{1}{2\beta}z_3' - \frac{1}{2\beta}z_1''$	$\frac{1}{2\gamma}z_3' - \frac{1}{2\gamma}z_2''$	$\frac{q}{2}z_3' + \frac{q}{2}z_3''$	$\frac{q}{2\alpha}z_3' - \frac{q}{2\alpha}z_4''$
u_4	$\frac{1}{2\gamma}z_4' - \frac{1}{2\gamma}z_1''$	$\frac{p}{2\beta}z_4' - \frac{p}{2\beta}z_2''$	$-\frac{q}{2\alpha}z_4' + \frac{q}{2\alpha}z_3''$	$-\frac{pq}{2}z_4' - \frac{pq}{2}z_4''$

Таблица 2.1. Коэффициенты соотношения (2.2) для обобщенных кватернионов.

Глава 3

Полупростые алгебры почти минимального ранга

В данной главе получена классификация полупростых алгебр почти минимального ранга над бесконечным полем характеристики, отличной от 2. Для этого доказана нижняя оценка, улучшающая оценку М. Блезера. Результаты главы опубликованы в [38].

3.1. Следствия известных оценок

Рассмотрим вопрос о почти минимальности полупростой алгебры A над полем F, разложение Веддерберна-Артина которой состоит из t сомножителей: $A \cong A_1 \times \cdots \times A_t$. В этом случае оценка Алдера-Штрассена имеет вид

$$R(A) \geqslant 2 \dim A - t,$$

так как пересечение любого идеала A с сомножителем A_i должно быть идеалом A_i, то есть либо $\mathbf{0}$, либо A_i и, следовательно, максимальными идеалами A являются подалгебры $\prod\limits_{i \neq i_0} A_i$.

При анализе структуры полупростых алгебр почти минимального ранга мы будем применять следующую лемму, которая использу-

ется в доказательстве теоремы Алдера-Штрассена.

Лемма 3.1 (А. Алдер, Ф. Штрассен, см. [1]). *Если A — простая алгебра, B — произвольная алгебра, то справедлива оценка*

$$R(A \times B) \geqslant 2 \dim A - 1 + R(B).$$

Обозначим символом $\Delta(A)$ разность между рангом алгебры $R(A)$ и оценкой Алдера-Штрассена $2 \dim A - t(A)$. Из леммы 3.1 следует, что для полупростых A и B справедливо соотношение

$$\Delta(A \times B) \geqslant \Delta(B).$$

Это значит, что полупростая алгебра минимального ранга ($\Delta = 0$) является произведением простых алгебр минимального ранга, а полупростая алгебра почти минимального ранга ($\Delta = 1$) — произведением простых алгебр минимального и почти минимального ранга.

Алгебры минимального ранга были описаны в [3]. Из этого описания следует, что простыми алгебрами минимального ранга являются алгебра матриц $F^{2\times 2}$ и простые алгебраические расширения поля F, причем в случае конечного поля F размерность расширения не должна превышать $\frac{|F|}{2} + 1$.

Мы будем рассматривать только бесконечные поля F. Пусть простая алгебра изоморфна $D^{n\times n}$. В случае $n = 1$ возможны 3 случая для D: простое расширение F, расширение F, не являющееся простым, и некоммутативная алгебра с делением. Простые расширения

являются алгебрами минимального ранга. Для оценки сложности расширений, не являющихся простыми, нам потребуются некоторые факты из теории несепарабельных расширений.

Определение 3.1. Неприводимый многочлен называется *сепарабельным*, если все его корни (принадлежащие алгебраическому замыканию F) различны. *Минимальным многочленом* элемента a алгебры A называется многочлен $f \in F[x]$ такой, что $f(a) = 0$, имеющий минимально возможную степень и единичный старший коэффициент. Элемент a алгебраического расширения K называется *сепарабельным*, если его минимальный многочлен сепарабелен. Расширение называется *сепарабельным*, если все его элементы сепарабельны.

Лемма 3.2 (см. [33, §44,§46], [19, упр. V.25])**.** *Любое алгебраическое расширение поля характеристики* 0 *сепарабельно и просто.*

Над полем характеристики p размерность любого алгебраического расширения K имеет вид np^e, где n — размерность максимального сепарабельного подрасширения E. Расширение является простым тогда и только тогда, когда найдется элемент $x \in K$ такой, что $x^{p^e} \in E$ и $x^{p^{e-1}} \notin E$.

Таким образом, расширения, не являющиеся простыми, являются несепарабельными. для разбора этого случая мы применим оценку Баура (теорема 1.3) с учетом приведенной леммы о размерно-

сти несепарабельных расширений. Из этой леммы следует, что если расширение K имеет размерность np^e и не является простым, то любое его простое подрасширение $F(a)$ имеет размерность $n'p^{e'}$, где $n' \leqslant n$ — размерность его максимального сепарабельного подполя, и $e' < e$, так как иначе найдется несепарабельный элемент x, для которого x^{p^e} сепарабелен, а $x^{p^{e-1}}$ несепарабелен, из чего следует простота исходного расширения K. Следовательно, по теореме Баура

$$R(K) \geqslant 2\dim K - 2 + \frac{\dim K}{\dim F(a)} \geqslant 2\dim K - 2 + p,$$

что при $p \neq 2$ означает, что расширение K не является алгеброй почти минимального ранга.

Для некоммутативных алгебр с делением можно применить следующие оценки, полученные М.Блезером [4].

Теорема 3.1 (М. Блезер)**.** *Для некоммутативной алгебры с делением D справедлива оценка*

$$R(D) \geqslant \frac{5}{2}\dim D - 3.$$

Теорема 3.2 (М. Блезер)**.** *Пусть D — алгебра с делением, $n \geqslant 2$, $A \cong D^{n\times n}$ — простая алгебра. Тогда*

$$R(A) \geqslant \frac{5}{2}\dim A - 3n.$$

При $d > 6$ оценка теоремы 3.1 дает неравенство

$$R(D) \geqslant \frac{5}{2} \dim D - 3 > 2 \dim D,$$

которое означает, что D не является алгеброй почти минимального ранга. Так как размерность алегбры D над ее центром должна быть квадратом (см. [35, следствие IV.5.2]), некоммутативных алгебр с делением размерностей $2, 3, 5$ и 6 не существует. Некоммутативные алгебры с делением размерности 4 — это алгебры обобщенных кватернионов, рассмотренные ранее. Из результатов предыдущей главы следует, что они являются простыми алгебрами почти минимального ранга, причем полупростая алгебра почти минимального ранга не может содержать более одного простого сомножителя такого вида.

При $n > 1$ можно применить оценку теоремы 3.2. Эта оценка позволяет доказать, что простые алгебры с $n \geqslant 4$, а также с $n = 3$, $\dim D \geqslant 3$ и $n = 2$, $\dim D \geqslant 4$, не являются алгебрами почти минимального ранга.

Рассмотрим оставшиеся случаи. Случай $n = 2$, $\dim D = 1$ соответствует алгебре матриц $F^{2\times 2}$, которая является алгеброй минимального ранга. Случай $n = 3$, $\dim D = 1$ — это алгебра $F^{3\times 3}$, рассмотренная в [2], где доказана оценка, свидетельствующая о том, что эта алгебра не является алгеброй почти минимального ранга.

Теорема 3.3 (М. Блезер)**.** $R(F^{3\times 3}) \geqslant 19$.

Случай $n = 2$, $\dim D = 2$ рассмотрен в [7] для поля $F = \mathbb{R}$ и также не является алгеброй почти минимального ранга. Доказательство не использует специфики поля $\mathbb{R}$ и может быть дословно переписано для любого поля характеристики, отличной от 2.

Теорема 3.4 (М. Блезер, А. М. де Вольтер)**.** *Если K — алгебраическое расширение поля F, $\dim K = 2$, то $R(K^{2\times 2}) \geqslant 17$.*

Оставшиеся два случая ($n = 2$, $\dim D = 3$ и $n = 3$, $\dim D = 2$) мы рассмотрим далее. Для доказательства того, что эти алгебры не являются алгебрами почти минимального ранга, мы улучшим оценку теоремы 3.2 в случае, когда алгебра D является расширением поля F.

3.2. Сложность умножения в алгебрах матриц

Лемма 3.3. *Пусть $P(x_1, \ldots, x_n)$ — ненулевой многочлен степени k над бесконечным полем F. Тогда существует набор $\alpha_1, \ldots, \alpha_n$, в котором не более k ненулевых значений, на котором этот многочлен не равен 0. Если P существенно зависит от переменной x_i, то одним из ненулевых значений можно взять α_i.*

Доказательство. Если многочлен P не равен тождественно 0, то существует моном, входящий в него с ненулевым коэффициентом. В случае, если P существенно зависит от x_i, то существует моном с нену-

левым коэффициентом, содержащий x_i. Так как степень многочлена равна k, этот моном содержит не более k переменных.

Подставим нули вместо всех переменных, кроме тех, которые входят в этот моном. Получим многочлен $P'(x_{i_1}, \ldots, x_{i_t})$, $t \leqslant k$. Он содержит рассматриваемый моном, а потому не равен тождественно нулю, т.е. найдутся значения $\alpha_{i_1}, \ldots, \alpha_{i_t}$, при подстановке которых полином имеет ненулевое значение. Если при этом рассматриваемый моном содержит переменную x_i, то P' можно записать в виде $\sum_{j=0}^{p} P''_j(\tilde{x}) x_i^j$, где P''_j не зависят от x_i и не все P''_j при $j \geqslant 1$ тождественно равны нулю. Подставив вместо всех переменных, кроме x_i, значения так, что хотя бы один из P''_j при $j \geqslant 1$ не обращается в 0, получим, что P' существенно зависит от x_i и можно подставить ненулевое значение вместо x_i так, что получившееся значение многочлена P' будет ненулевым. □

Лемма 3.4. *Пусть K — расширение бесконечного поля F, $\dim_F K = d$, $r\colon K \to F$ — ненулевой линейный функционал, а $u_1, \ldots u_{n^2 d}$ — некоторый базис F-алгебры $K^{n\times n}$. Многочлен*

$$Q(\tilde{x}, \tilde{y}) = r(\det[\sum_{i=1}^{n^2 d} x_i u_i, \sum_{i=1}^{n^2 d} y_i u_i]) \in F[\tilde{x}, \tilde{y}]$$

существенно зависит от всех переменных, кроме тех, которые соответствуют скалярным матрицам $u_i = \gamma I$, $\gamma \in K$, если такие элементы содержатся в рассматриваемом базисе.

Доказательство. Пусть $u_1 \neq \gamma I$. Докажем, что многочлен Q существенно зависит от y_1. Зависимость от остальных переменных доказывается аналогично. Так как u_1 — нескалярная матрица, найдется вектор $z_1 \in K^n$ такой, что $u_1 z_1 = z_2$ не пропорционален z_1. Дополним пару z_1, z_2 до K-базиса пространства K^n и будем рассматривать матрицы из $K^{n\times n}$ как операторы в этом базисе. В этом базисе u_1 имеет вид

$$\begin{pmatrix} 0 & * & \dots & * \\ 1 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{pmatrix},$$

где на местах, отмеченных звездочками, могут стоять произвольные значения из K. Выберем x_i так, что $X = \sum_{i=1}^{n^2 d} x_i u_i$ в том же базисе имеет вид $\operatorname{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$, где все λ_i различны. При этом оператор $\operatorname{ad} X \colon Y \mapsto [X, Y]$ переводит матрицу $Y = (y_{ij})$ в матрицу $[X, Y] = ((\lambda_i - \lambda_j) y_{ij})$. Возьмем $\mu \in K$ такой, что $r(\mu) \neq 0$ и выберем матрицу $Y = \sum_{i=1}^{n^2 d} y_i u_i$ такую, что $Y z_1 = 0$, т.е.

$$Y = \begin{pmatrix} 0 & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{pmatrix},$$

и $Y + u_1$ имеет вид

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & \frac{\mu}{(\lambda_1-\lambda_n)(\lambda_2-\lambda_1)} \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \frac{1}{\lambda_3-\lambda_2} & 0 & \dots & 0 & 0 \\ 0 & 0 & \frac{1}{\lambda_4-\lambda_3} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \frac{1}{\lambda_n-\lambda_{n-1}} & 0 \end{pmatrix}.$$

Тогда $\det[X, Y] = 0$, так как первый столбец $[X, Y]$ будет нулевым, и $\det[X, Y + u_1] = \mu$. Получаем, что можно выбрать набор $(\tilde{x}, \tilde{y})$ так, что

$$Q(x_1, \dots, x_{n^2d}, y_1, y_2, \dots, y_{n^2d}) = 0,$$
$$Q(x_1, \dots, x_{n^2d}, y_1 + 1, y_2, \dots, y_{n^2d}) \neq 0,$$

что означает, что переменная y_1 является существенной. □

Лемма 3.5. *Пусть K — расширение бесконечного поля F, а $n \geqslant 2$. Из любого базиса F-алгебры $K^{n\times n}$ можно выбрать не более $3n - 1$ элементов, в линейной оболочке которых найдутся 3 элемента a_1, a_2, a_3 такие, что a_1 и $[a_1^{-1}a_2, a_1^{-1}a_3]$ обратимы.*

Доказательство. Пусть $u_1, \dots, u_{n^2d}$ — рассматриваемый базис. Если в нем есть обратимая матрица u_i, то возьмем $a_1 = u_i$. Иначе пусть $r\colon K \to F$ — некоторый ненулевой линейный функционал и $\mu \in K$ таков, что $r(\mu) \neq 0$. Рассмотрим вначале многочлен

$P(\tilde{x}) = r(\det \sum_{i=1}^{n^2 d} x_i u_i)$. Он ненулевой, так как существует матрица с определителем μ, и является однородным многочленом степени n (легко проверить, что $P(\lambda\tilde{x}) = \lambda^n P(\tilde{x})$). По лемме 3.3 можно выбрать значения x_i, на которых P не равен 0, и среди которых $s \leqslant n$ ненулевых, то есть в линейной оболочке s элементов базиса найдется невырожденная матрица a_1.

Далее, рассмотрим базис, составленный из элементов $u'_i = a_1^{-1} u_i$ и многочлен

$$Q(\tilde{x}, \tilde{y}) = r(\det[\sum_{i=1}^{n^2 d} x_i u'_i, \sum_{i=1}^{n^2 d} y_i u'_i]),$$

исследованный в предыдущей лемме. Это однородный многочлен степени $2n$. Снова применяя лемму 3.3, получаем, что найдется $q \leqslant 2n$ элементов нового базиса, содержащих матрицы $a'_2 = a_1^{-1} a_2$ и $a'_3 = a_1^{-1} a_3$ такие, что $[a'_2, a'_3]$ обратима, причем один из элементов базиса может быть задан заранее, если он не является скалярной матрицей. Тогда в линейной оболочке соответствующих элементов исходного базиса содержатся матрицы a_2 и a_3.

В случае, когда в исходном базисе есть обратимая матрица $a_1 = u_i$, мы получаем $2n + 1 \leqslant 3n - 1$ элементов, удовлетворяющих необходимым требованиям. В случае, когда все элементы базиса необратимы, мы в качестве одного из q элементов, выбираемых на втором шаге, можем взять один из s элементов, выбранных на первом,

так как вырожденные матрицы не являются скалярными. В итоге получаем $s + q - 1 \leqslant 3n - 1$ элементов, удовлетворяющих требуемым условиям. $\square$

Теорема 3.5. *Пусть K — расширение бесконечного поля F, $n \geqslant 2$, $A \cong K^{n\times n}$. Тогда*

$$R_F(A) \geqslant \frac{5}{2}\dim_F A - 3n + 1. \tag{3.1}$$

Доказательство. Пусть $(f_1, g_1, z_1; \ldots; f_r, g_r, z_r)$ — билинейный алгоритм умножения в A. По лемме 1.1 из набора f_k можно выбрать базис пространства A^*. По лемме 3.5 из двойственного базиса пространства A можно выбрать не более $3n - 1$ элемента, в линейной оболочке которых найдутся элементы a_1, a_2, a_3 такие, что a_1 и $[a_1^{-1}a_2, a_1^{-1}a_3]$ обратимы. Обозначим линейную оболочку этих трех элементов через U.

Рассмотрим ограничение умножения на линейную оболочку $U \times A$. По теореме 1.4 ранг этого билинейного отображения не меньше $\frac{3}{2}\dim A$. По лемме 1.2 ранг исходного алгоритма не меньше $(\dim A - 3n + 1) + \frac{3}{2}\dim A$, так как все f_k, кроме соответствующих выбранным $t \leqslant 3n - 1$ элементам, обращаются в 0 на U. $\square$

Из полученного результата следует, что алгебры вида $K^{n\times n}$ при $\dim K = 2, n = 3$ или $\dim K = 3, n = 2$ не являются алгебрами почти минимального ранга.

Учитывая результаты предыдущего раздела, окончательно получаем полное описание полупростых алгебр почти минимального ранга.

Теорема 3.6. *Любая полупростая алгебра почти минимального ранга над бесконечным полем F, $\operatorname{char} F \neq 2$, имеет вид H или $H \times B$, где H — алгебра обобщенных кватернионов с делением, B — полупростая алгебра минимального ранга.*

Глава 4

Целочисленные билинейные отображения над полями различных характеристик

В главе рассматривается связь рангов $\mathbb{Z}$-билинейного отображения над полями различной характеристики. Результаты опубликованы в [39–41]

4.1. Ненулевые тензорные произведения

При работе с тензорными произведениями следует учитывать тот факт, что произведение ненулевых модулей может быть равно $\mathbf{0}$. Так, например, $\mathbb{Q} \otimes_{\mathbb{Z}} F_p = \mathbf{0}$ для любого поля F_p простой характеристики p, потому что для любого разложимого тензора $q \otimes x$ справедливо $q \otimes x = \frac{q}{p} \otimes (px) = \frac{q}{p} \otimes 0 = 0$. В этом разделе мы приведем некоторые случаи, в которых тензорное произведение не является нулевым. Эти результаты в алгебре хорошо известны и являются простейшими частными случаями общих теорем (см. напр. [9, 19])

Лемма 4.1. *Пусть S — кольцо, M — конечномерный свободный модуль над S, N — произвольный ненулевой модуль над S. Тогда тензорное произведение $M \otimes_S N$ не является нулевым модулем.*

Доказательство. Следует из простейших свойств тензорного произведения (утверждение 1.3):

$$M \otimes_S N \cong S^m \otimes_S N \cong (S \oplus \cdots \oplus S) \otimes_S N \cong N \oplus \cdots \oplus N \neq \mathbf{0}. \quad \square$$

Лемма 4.2. *Тензорное произведение ненулевых линейных пространств над полем F не является нулевым.*

Доказательство. Ненулевое линейное пространство M над полем F можно представить в виде прямой суммы одномерного пространства и какого-то его дополнения: $M \cong F \oplus M'$. Значит и тензорное произведение также содержит некоторое одномерное подпространство, т. к.

$$M \otimes_F N \cong (F \oplus M') \otimes_F (F \oplus N') \cong F \oplus M' \oplus N' \oplus M' \otimes_F N'. \quad \square$$

Лемма 4.3 (см. [9, §III.3])**.** *Пусть S — кольцо без делителей нуля, Q — его поле частных, M — модуль над S, содержащий свободный элемент m, т. е. элемент, для которого $am \neq 0$ для любого $a \in S$. Тогда $Q \otimes_S M$ не является нулевым модулем.*

Лемма 4.4. *Пусть S — кольцо без делителей нуля, Q — его поле частных, K — поле, содержащее Q, и M — модуль над S, содержащий свободный элемент. Тогда $K \otimes_S M$ не является нулевым модулем.*

Доказательство. Следует из двух предыдущих лемм:

$$K \otimes_S M \cong (K \otimes_Q Q) \otimes_S M \cong K \otimes_Q (Q \otimes_S M) = K \otimes_Q M' \neq 0,$$

так как K и $M' = Q \otimes_S M$ — линейные пространства над Q, причем M' ненулевое по предыдущей лемме. □

4.2. Связь между билинейными алгоритмами

Мы будем рассматривать $\mathbb{Z}$-билинейное отображение φ и алгоритмы для него над различными кольцами и полями, определенные в разделе 1.3 (определение 1.21). Под «алгеброй» будет пониматься коммутативная ассоциативная алгебра с единицей над кольцом.

Основным инструментом является простое наблюдение, основанное на теореме Хауэлла о том, что ранг отображений над алгебраически замкнутым полем минимален (теорема 1.5).

Лемма 4.5. *Если S — кольцо, F — алгебраически замкнутое поле, φ — $\mathbb{Z}$-билинейное отображение, и $S \otimes_{\mathbb{Z}} F \neq \mathbf{0}$, то $R_S(\varphi) \geqslant R_F(\varphi)$.*

Доказательство. Так как $S \otimes_{\mathbb{Z}} F$ есть алгебра над S, то $R_S(\varphi) \geqslant R_{S \otimes_{\mathbb{Z}} F}(\varphi)$. Так как $S \otimes_{\mathbb{Z}} F$ также есть алгебра над F и F алгебраически замкнуто, то по теореме 1.5 имеем $R_{S \otimes_{\mathbb{Z}} F}(\varphi) = R_F(\varphi)$. □

Докажем теперь еще несколько лемм, которые позволят переносить алгоритмы между полями различных характеристик.

Лемма 4.6. *Пусть Z — коммутативное кольцо без делителей нуля, Q — его поле частных и φ — Z-билинейное отображение. Тогда верно равенство*

$$R_Q(\varphi) = \min_{k \in Z \setminus \{0\}} R_Z(k\varphi).$$

Доказательство. Если $(f_1, g_1, z_1; \ldots; f_r, g_r, z_r)$ — билинейный алгоритм над Z для $k\varphi$, то $(f_1, g_1, \frac{1}{k} z_1; \ldots; f_r, g_r, \frac{1}{k} z_r)$ — алгоритм над Q для φ.

Обратно, пусть $(f_1, g_1, z_1; \ldots; f_r, g_r, z_r)$ — билинейный алгоритм над Q для φ. Определим k_f как произведение знаменателей всех коэффициентов всех функционалов f_s в некотором базисе. Аналогично определим k_g и k_z. Тогда последовательность троек $(k_f f_1, k_g g_1, k_z z_1; \ldots; k_f f_r, k_g g_r, k_z z_r)$ образует билинейный алгоритм над Z для билинейного отображения $k_f k_g k_w \varphi$.

Получаем, что $R_Q(\varphi) \leqslant R_Z(k\varphi)$ для любого $k \in Z \setminus \{0\}$, и при этом существует $k \in Z \setminus \{0\}$ такой, что $R_Q(\varphi) \geqslant R_Z(k\varphi)$, откуда следует утверждение леммы. □

Лемма 4.7. *Пусть S — коммутативное кольцо, φ — S-билинейное отображение, $\{A_p | p \in I\}$ — семейство алгебр над S и $A = \prod_{p \in I} A_p$. Тогда справедливо равенство*

$$R_A(\varphi) = \max_{p \in I} R_{A_p}(\varphi).$$

Доказательство. Пусть $(f_{p,1}, g_{p,1}, z_{p,1}; \ldots; f_{p,r}, g_{p,r}, z_{p,r})$ — оптимальные билинейные алгоритмы над A_p для φ. Добавив при необходимости нулевые тройки, можно считать что ранг каждого из этих алгоритмов равен $r = \max\limits_{p \in I} R_{A_p}(\varphi)$. Рассмотрим эти алгоритмы в координатном виде; пусть коэффициенты функционалов $f_{p,q}$, $g_{p,q}$ и элементов $z_{p,q}$ в стандартных базисах равны $f_{p,i}^{(q)}$, $g_{p,j}^{(q)}$ и $z_{p,k}^{(q)}$ соответственно. Рассмотрим билинейный алгоритм над A, коэффициенты $f_i^{(q)}$,$g_j^{(q)}$,$z_k^{(q)}$ элементов которого задаются последовательностями $(f_{p,i}^{(q)} | p \in I)$, $(g_{p,j}^{(q)} | p \in I)$, $(z_{p,k}^{(q)} | p \in I)$ соответственно. Так как соотношение (1.3) выполняется покоординатно, то полученный билинейный алгоритм (f_q, g_q, z_q) будет алгоритмом для φ над прямым произведением A. Таким образом, $R_A(\varphi) \leqslant r$. И наоборот, взяв p-ю координату из каждого коэффициента каждого элемента билинейного алгоритма над A, мы получим билинейный алгоритм над соответствующей компонентой A_p. $\square$

Теперь с помощью этих лемм и утверждений о ненулевых тензорных произведениях из предыдущего раздела можно доказать следующую теорему, связывающую ранги билинейного отображения φ над алгебраически замкнутыми полями различных характеристик. Символом $\bar{\mathbb{Q}}$ обозначается алгебраическое замыкание поля рациональных чисел, символом $\bar{\mathbb{F}}_p$ — алгебраическое замыкание поля из p элементов.

Теорема 4.1. *Для любого $\mathbb{Z}$-билинейного отображения φ справедливо соотношение*

$$R_{\bar{\mathbb{Q}}}(\varphi) = R_{\bar{\mathbb{F}}_p}(\varphi)$$

для всех простых p, кроме, быть может, конечного числа.

Доказательство. Рассмотрим оптимальный алгоритм над $\bar{\mathbb{Q}}$ для $\mathbb{Z}$-билинейного отображения φ. Так как в алгоритме участвует только конечное число коэффициентов $f_i^{(q)}$, $g_j^{(q)}$, $z_k^{(q)}$, то подполе F, порожденное этими коэффициентами, будет конечным алгебраическим расширением $\mathbb{Q}$, для которого $R_F(\varphi) = R_{\mathbb{Q}}(\varphi)$. Применяя лемму 4.6 для кольца O_F целых элементов F, получим, что $R_F(\varphi) = R_{O_F}(k\varphi)$ для некоторого k. Из доказательства леммы видно, что можно взять $k \in \mathbb{Z}$, так как любое алгебраическое число представляется в виде $\frac{n}{m}$, где n — целое алгебраическое и $m \in \mathbb{Z}$.

Кольцо O_F, рассматриваемое как модуль над $\mathbb{Z}$, является свободным модулем, поэтому тензорное произведение $O_F \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p$ не является нулевым. По лемме 2 получаем $R_{O_F}(k\varphi) \geqslant R_{\bar{\mathbb{F}}_p}(k\varphi) = R_{\bar{\mathbb{F}}_p}(\varphi)$, если $k \neq 0$. Равенство $k = 0$ в $\bar{\mathbb{F}}_p$ выполняется для не более чем конечного числа характеристик p (а именно, для простых делителей k), поэтому неравенство $R_{\bar{\mathbb{Q}}}(\varphi) \geqslant R_{\bar{\mathbb{F}}_p}(\varphi)$ выполнено для всех p, кроме, быть может, конечного числа.

Для перехода от билинейных алгоритмов для $\mathbb{Z}$-билинейного

отображения φ над полями простой характеристики к алгоритмам над полем характеристики 0 рассмотрим последовательность полей $\bar{\mathbb{F}}_p$. Пусть r — минимально возможное число, встречающееся в последовательности $R_{\bar{\mathbb{F}}_p}(\varphi)$ бесконечное число раз. Рассмотрим бесконечное прямое произведение

$$S = \prod_{p:R_{\bar{\mathbb{F}}_p}(\varphi)=r} \bar{\mathbb{F}}_p.$$

Любой кратный 1 элемент этого кольца не равен 0, так как он не равен 0 в компонентах произведения, соответствующих достаточно большим p. Как следствие, $S \otimes_{\mathbb{Z}} \bar{\mathbb{Q}}$ не является нулевым кольцом (по лемме 4.4). Таким образом $r = R_S(\varphi) \geqslant R_{\bar{\mathbb{Q}}}(\varphi)$ по лемме 4.7. Из выбора числа r следует, что неравенство $R_{\bar{\mathbb{F}}_p}(\varphi) < r$ может выполняться только для конечного числа простых p.

Таким образом, мы получили соотношения $R_{\bar{\mathbb{Q}}}(\varphi) \geqslant R_{\bar{\mathbb{F}}_p}$ и $R_{\bar{\mathbb{F}}_p}(\varphi) \geqslant R_{\bar{\mathbb{Q}}}(\varphi)$ для всех p, кроме, может быть, конечного числа. Объединяя эти два неравенства, получаем утверждение теоремы. $\square$

4.3. Метаматематическое доказательство

Интересно, что теорему 4.1 можно доказать также методами математической логики, не прибегая к чисто алгебраическим конструкциям. Для этого можно использовать полноту теорий ACF_c алгебраически замкнутых полей характеристики c. В дополнение к

обычным аксиомам поля в ACF_c используется схема аксиом алгебраической замкнутости: для всех натуральных $n \geqslant 1$

$$\forall a_0 \ldots \forall a_{n-1} \exists x (x^n + \sum_{i=0}^{n-1} a_i x^i = 0),$$

а также аксиомы, определяющие характеристику поля: в случае простой характеристики p аксиомой теории ACF_p будет формула $\Psi_p \equiv (0 = \underbrace{1 + \cdots + 1}_{p})$, а теория ACF_0 содержит схему аксиом $\neg\Psi_p$ для всех простых p.

Теорема 4.2 (А. Робинсон, см. [23])**.** *Для любой характеристики c теория ACF_c полна.*

Из этой теоремы следуют утверждения о связи выводимости формул первого порядка в теориях ACF_c.

Утверждение 4.1. *Если F — алгебраически замкнутое поле характеристики c, то любая формула Φ общезначима в F тогда и только тогда, когда она выводима в ACF_c.*

Утверждение 4.2 (см. [20])**.** *Формула Φ выводима в теории ACF_0 тогда и только тогда, когда она выводима в ACF_p для всех простых p, кроме, может быть, конечного числа.*

Приведем теперь второе доказательство теоремы 4.1.

Доказательство. Заметим, что для $\mathbb{Z}$-билинейного отображения φ утверждение $R(\varphi) \leqslant r$ можно записать в виде замкнутой формулы логики предикатов в сигнатуре теории колец $\langle =, +, \cdot, 0, 1\rangle$. Действительно, пусть φ задается в некоторой тройке базисов коффициентами t_{ijk} в соответствии с (1.1). Исходя из координатного представления билинейного алгоритма (1.3), утверждение $R(\varphi) \leqslant r$ выполняется тогда и только тогда, когда истинна формула

$$\exists f_1^{(1)} \dots \exists f_a^{(r)} \exists g_1^{(1)} \dots \exists g_b^{(r)} \exists z_1^{(1)} \dots \exists z_c^{(r)} \bigwedge_{\substack{1 \leqslant i \leqslant a \\ 1 \leqslant j \leqslant b \\ 1 \leqslant k \leqslant c}} (t_{ijk} = \sum_{s=1}^{r} f_i^{(s)} g_j^{(s)} z_k^{(s)}).$$

Так как t_{ijk} целые, то их можно записать в виде суммы единиц и при необходимости перенести в правую часть, чтобы избавиться от знака «минус». Полученная формула является замкнутой формулой теории колец, и утверждение $R_S(\varphi) \leqslant r$ верно тогда и только тогда, когда эта формула истинна в кольце S. Как следствие, в виде формулы теории колец можно записать и утверждение $R_S(\varphi) = r$.

Применяя эти следствия к формуле, выражающей утверждение $R_F(\varphi) = r$, получаем утверждение теоремы 4.1. □

Литература

1. Alder A., Strassen V. On the Algorithmic Complexity of Associative Algebras // Theor. Comput. Sci. — 1981. — Vol. 15. — P. 201–211.

2. Bläser M. On the complexity of the multiplication of matrices of small formats // J. Complexity. — 2003. — Vol. 19, no. 1. — P. 43–60.

3. Bläser M. A Complete Characterization of the Algebras of Minimal Bilinear Complexity // SIAM J. Comput. — 2004. — Vol. 34, no. 2. — P. 277–298.

4. Bläser M. Beyond the Alder-Strassen bound // Theor. Comput. Sci. — 2005. — Vol. 331, no. 1. — P. 3–21.

5. Bläser M. Fast matrix multiplication // Preprint. — 2013.

6. Bläser M., Chokaev B. Algebras of minimal multiplicative complexity // Proceedings of the 27th Annual IEEE Conference on Computational Complexity (CCC). — 2012. — P. 224–234.

7. Bläser M., de Voltaire A.M. Semisimple algebras of almost minimal rank over the reals // Theor. Comput. Sci. — 2009. — Vol. 410, no. 50. — P. 5202–5214.

8. The Book of Involutions / M.A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol. — AMS, 1998.

9. Bourbaki N. Algebra. Chapters 1–3. — Springer, 1998.

10. Brockett R. W., Dobkin D. On the optimal evaluation of a set of bilinear forms // Linear Algebra and Its Applications. — 1978. — Vol. 19, no. 3. — P. 207–235.

11. Bürgisser P., Clausen M., Shokrollahi M.A. Algebraic Complexity Theory. — Springer, 1997.

12. Coppersmith D., Winograd S. Matrix multiplication via arithmetic progressions // Journal of symbolic computation. — 1990. — Vol. 9, no. 3. — P. 251–280.

13. De Groote H. F. On the complexity of quaternion multiplication // Information Processing Letters. — 1975. — Vol. 3, no. 6. — P. 177–179.

14. De Groote H. F. On varieties of optimal algorithms for the computation of bilinear mappings I. the isotropy group of a bilinear mapping // Theor. Comput. Sci. — 1978. — Vol. 7, no. 1. — P. 1–24.

15. Howell T. D. Global properties of tensor rank // Linear Algebra and its Applications. — 1978. — Vol. 22. — P. 9–23.

16. Howell T. D, Lafon J.-C. The complexity of the quaternion product // Cornell University Tech. Rep. — 1975.

17. Knapp A. W. Basic algebra. — Springer, 2006.

18. Landsberg J. M. New lower bounds for the rank of matrix multiplication // Preprint, ArXiv:1206.1530. — 2012.

19. Lang S. Algebra. — Springer, 2002.

20. Marker D., Messmer M., Pillay A. Model theory of fields. — Springer, 1996.

21. Pierce R. S. The Associative Algebras. — Springer, 1982.

22. Raz R. On the Complexity of Matrix Product // SIAM J. Comput. — 2003. — Vol. 32, no. 5. — P. 1356–1369.

23. Robinson A. On the metamathematics of algebra. — North-Holland, 1951.

24. Schönhage A. Partial and total matrix multiplication // SIAM J. Comput. — 1981. — Vol. 10, no. 3. — P. 434–455.

25. Sipser M. The history and status of the P versus NP question // Proceedings of the XXIV annual ACM symposium on Theory of computing. — 1992. — P. 603–618.

26. Stothers A. J. On the complexity of matrix multiplication : Ph. D. thesis / A. J. Stothers ; University of Edinburgh. — 2010.

27. Strassen V. Gaussian elimination is not optimal // Numerische Mathematik. — 1969. — Vol. 13, no. 4. — P. 354–356.

28. Strassen V. Rank and optimal computation of generic tensors // Linear algebra and its applications. — 1983. — Vol. 52. — P. 645–685.

29. Strassen V. Relative bilinear complexity and matrix multiplication. // Journal für die reine und angewandte Mathematik. — 1987. — Vol. 375. — P. 406–443.

30. Trakhtenbrot B. A. A survey of Russian approaches to perebor (brute-force searches) algorithms // Annals of the History of Computing. — 1984. — Vol. 6, no. 4. — P. 384–400.

31. Vassilevska Williams V. Multiplying matrices faster than Coppersmith-Winograd // Proceedings of the 44th symposium on Theory of Computing / ACM. — 2012. — P. 887–898.

32. Алексеев В. Б. Сложность умножения матриц. Обзор // Кибернетич. сборн. — 1988. — № 25. — С. 189–236.

33. Ван дер Варден Б.Л. Алгебра. — М.: Наука, 1976.

34. Винберг Э. Б. Курс алгебры. — М.: Пиксел, 2011.

35. Дрозд Ю.А., Кириченко В.В. Конечномерные алгебры. — Киев: Вища школа, 1980.

36. Жданович Д. В. Экспонента сложности матричного умножения // Фундаментальная и прикладная математика. — 2012. — Т. 17, № 2. — С. 107–166.

37. Лысиков В. В. О билинейных алгоритмах умножения обобщенных кватернионов // Материалы XI международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения О. Б. Лупанова / М.: МГУ. — 2012. — С. 141–143.

38. Лысиков В. В. Об алгебрах почти минимального ранга // Дискретная математика. — 2012. — Т. 24, № 4. — С. 3–18.

39. Лысиков В. В. Сложность умножения матриц над полями различной характеристики // Международная конференция «Мальцевские чтения», 12-16 ноября 2012 г. Тезисы докладов / Новосибирск: Институт математики им. С. Л. Соболева, Новосибирский государственный университет. — 2012. — С. 41.

40. Лысиков В. В. О билинейных алгоритмах над полями различных характеристик // Вестник Московского Университета. Серия 15: Вычислительная математика и механика. — 2013. — Т. 4. — С. 33–38.

41. Лысиков В. В. О целочисленных билинейных отображениях // Материалы Международного молодежного научного форума «Ломоносов-2013» [Электронный ресурс] / М.: МАКС Пресс. — 2013.