Московский государственный университет
имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

На правах рукописи

Чокаев Бекхан Вахаевич

Мультипликативная сложность умножения в алгебрах

01.01.09 — дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2012

Работа выполнена на кафедре математической кибернетики факультета вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова.

Научный руководитель:	доктор физико-математических наук, профессор Алексеев Валерий Борисович.
Официальные оппоненты:	доктор физико-математических наук, профессор Гашков Сергей Борисович;
	кандидат физико-математических наук, Поспелов Алексей Дмитриевич.
Ведущая организация:	Вычислительный центр РАН имени А. А. Дородницына.

Защита диссертации состоится 16 ноября 2012 г. в 11 часов на заседании диссертационного совета Д 501.001.44 при Московском государственном университете имени М.В. Ломоносова по адресу: 119991, Москва, ГСП-1, Ленинские горы, 2-й учебный корпус, факультет ВМК, аудитория 685. Желающие присутствовать на заседании диссертационного совета должны сообщить об этом за два дня по тел. 939-30-10 (для оформления заявки на пропуск).

С диссертацией можно ознакомиться в фундаментальной библиотеке МГУ имени М. В. Ломоносова. С текстом автореферата можно ознакомиться на официальном сайте факультета ВМК МГУ http://cs.msu.ru/.

Автореферат разослан ___ октября 2012 г.

Ученый секретарь
диссертационного совета
профессор Н.П. Трифонов

Общая характеристика работы

Актуальность темы. Одной из центральных областей алгебраической теории сложности является сложность умножения в алгебрах. Алгеброй называется линейное пространство над некоторым полем, наделенное операцией умножения: отображением, которое двум произвольным элементам пространства ставит в соответствие определенный элемент этого пространства, причем это отображение является линейным по обоим аргументам. Задача сложности умножения в алгебре заключается в том, чтобы построить алгоритм, который для любых двух элементов этой алгебры вычислял бы их произведение, и имел бы наименьшую сложность. При этом под сложностью алгоритма могут подразумеваться различные понятия. Например, можно учитывать все арифметические операции над полем, которые требуются алгоритму для вычисления произведения в алгебре. Возникающая сложность называется *арифметической (тотальной) сложностью.* Другой способ определения сложности алгоритма — учитывать только так называемые существенные умножения, то есть такие операции умножения, оба операнда в которых зависят от входных переменных. В этом случае возникают понятия *ранга и мультипликативной сложности* умножения в алгебре[1].

Одной из наиболее важных и интересных задач в данной области является задача сложности умножения в алгебре матриц. В 1969 году Ф. Штрассен опубликовал алгоритм умножения квадратных матриц порядка n арифметической сложности $O(n^{\log_2 7})$, тем самым впервые доказав, что традиционный алгоритм умножения матриц "строка на столбец" не является оптимальным[2]. После выхода статьи Штрассена эта задача привлекла большое внимание со стороны математиков из разных стран. Несколько групп ученых из разных университетов мира, предлагая новые подходы и конструкции, понижали верхнюю оценку сложности умножения матриц. На сегодняшний день лучшей известной верхней оценкой для умножения двух квадратных матриц порядка n является $O(n^{2,373})$[3,4]. Существует гипотеза о том, что сложность умножения матриц порядка n равна $o(n^{2+\varepsilon})$

[1] P. Bürgisser, M. Clausen, M. Shokrollahi. *Algebraic Complexity Theory.* Springer, 1997.

[2] V. Strassen. *Gaussian elimination is not optimal.* Numer. Math. 13, 354–356 (1969).

[3] V. Vassilevska Williams. *Multiplying matrices faster than Coppersmith-Winograd.* Proceedings of the 44th ACM Symposium on Theory of Computing, 19–22 May 2012, New York, NY, Association for Computing Machinery, pp. 887–898.

[4] A. Stothers. *On the complexity of matrix multiplication.* Ph.D. dissertation, University of Edinburgh, 2010.

для любого ε, однако до сих пор это утверждение не доказано и не опровергнуто[5].

В 2003 году Генри Коэн и Кристофер Уманс предложили новый подход для получения верхних оценок сложности умножения матриц, основанный на вложениях в групповые алгебры[6]. Групповой называется алгебра, в которой существует базис такой, что множество элементов, входящих в этот базис, образуют группу относительно умножения в алгебре. Было показано, что, если сложность умножения в групповых алгебрах — почти линейна относительно размерности алгебры, то сложность умножения квадратных матриц порядка n — почти квадратична относительно n. В 2005 году этим методом были получены алгоритмы умножения матриц минимальной сложности среди всех известных алгоритмов[7]. Эти результаты стимулировали рост интереса к групповым алгебрам. В кандидатской диссертации А. Д. Поспелова были исследованы коммутативные групповые алгебры над алгебраически замкнутыми полями и полем вещественных чисел[8]. Им были установлены точные значения сложности умножения в таких групповых алгебрах.

Целью данной диссертации является исследование сложности умножения в коммутативных групповых алгебрах над произвольными полями. Для решения этой задачи предложен метод нахождения структуры групповых алгебр, который позволяет использовать теорему Алдера-Штрассена для получения нижних оценок и теорему Блезера, описывающую все алгебры минимального ранга, для получения верхних оценок.

Другой целью диссертации является установление алгебраической структуры алгебр минимальной мультипликативной сложности. В 1981 году Алдер и Штрассен доказали свою фундаментальную нижнюю оценку для мультипликативной сложности умножения в произвольной ассоциативной алгебре с единицей[9]. Так как мультипликативная сложность является обобщением понятия ранга, то оценка Алдера-Штрассена выполняется также для ранга умножения в алгебре. Практически сразу возникла задача описания алгебр минимального ранга с точки зрения их алгебраической

[5]Алексеев В. Б. *Сложность умножения матриц. Обзор.* Киберн. сб. (1988) **25**, 189–236.

[6]H. Cohn, C. Umans. A Group-Theoretic Approach to Fast Matrix Multiplication.//Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, 2003, p. 438–449.

[7]H. Cohn, R. D. Kleinberg, B. Szegedy, C. Umans. Group-theoretic Algorithms for Matrix Multiplication.// Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, 2005, p. 379–388.

[8]Поспелов А. Д. *Сложность умножения в ассоциативных алгебрах.* Диссертация. Московский государственный университет им. М. В. Ломоносова, 2008.

[9]A. Alder, V. Strassen. On the algorithmic complexity of associative algebras. Theoret. Comput. Sci., 15:201–211, 1981.

структуры, то есть таких алгебр, для которых оценка Алдера-Штрассена выполняется как равенство для ранга. В течение почти 20 лет эта задача решалась многими математиками для различных классов алгебр над различными полями. Однако до 2002 года эта проблема оставалась открытой, пока Маркус Блезер не получил полное описание всех алгебр минимального ранга над произвольными полями[10]. Так как доказывать нижние оценки для мультипликативной сложности обычно сложнее, чем для ранга, то в отличие от алгебр минимального ранга для алгебр минимальной мультипликативной сложности результатов было получено немного. Фейг получил описание специального класса алгебр — алгебр с делением минимальной мультипликативной сложности[11]. Однако алгебраическая структура произвольных алгебр минимальной мультипликативной сложности была неизвестна. В частности, оставался открытым вопрос о существовании алгебры минимальной мультипликативной сложности, которая не является алгеброй минимального ранга. В данной диссертации доказано, что произвольная алгебра является алгеброй минимальной мультипликативной сложности тогда и только тогда, когда она является алгеброй минимального ранга, тем самым получено описание всех алгебр минимальной мультипликативной сложности с точки зрения их алгебраической структуры. Этот результат обобщает результат Блезера на случай мультипликативной сложности и результат Фейга на случай произвольных алгебр. Для решения этой задачи предложен новый метод доказательства нижних оценок для мультипликативной сложности умножения в алгебрах с ненулевым радикалом.

Целью диссертационной работы является исследование мультипликативной сложности умножения в коммутативных групповых алгебрах над произвольными полями, а также решение задачи определения алгебраической структуры алгебр минимальной мультипликативной сложности над произвольными полями.

Методы исследования. При выполнении диссертационного исследования использовались методы алгебры, алгебраической теории сложности, теории вероятности.

Научная новизна. В работе доказано, что любая групповая алгебра абелевой группы над произвольным полем характеристики нуль является алгеброй минимального ранга. Описаны структура и мультипликативная

[10]Markus Bläser. *A Complete Characterization of the Algebras of Minimal Bilinear Complexity.* SIAM J. Comput., 34(2):277-298, 2004.

[11]Ephraim Feig. *On systems of bilinear forms whose minimal division-free algorithms are all bilinear.* J. Algorithms 2(3): 261–281, 1981.

сложность таких групповых алгебр. Над полями простой характеристики найдено необходимое и достаточное условие того, что коммутативная групповая алгебра является алгеброй минимального ранга. Доказаны верхние и нижние оценки на мультипликативную сложность умножения в таких алгебрах. Решена задача описания алгебраической структуры алгебр минимальной мультипликативной сложности над произвольными полями.

Достоверность полученных в диссертации результатов обусловлена строгостью математических доказательств, использованием апробированных научных методов и средств.

Теоретическая и практическая значимость работы. Результаты диссертационной работы имеют теоретический характер. Вместе с тем, как упомянуто выше, рассматриваемые в диссертации задачи могут потенциально помочь для нахождения сложности умножения матриц. Операция умножения матриц лежит в основе многих важных прикладных задач линейной алгебры, таких как, обращение матрицы, решение системы линейных уравнений, вычисление определителя. Также некоторые алгоритмы на графах, которые используются на практике, имеют такую же сложность, как умножение матриц. Таким образом, несмотря на свой теоретический характер, результаты диссертационной работы потенциально могут быть применимы в развитии различных областей прикладной математики.

Соответствие диссертации паспорту научной специальности. В диссертации проведено исследование в области сложности алгоритмов и вычислений, а именно, изучены задачи алгебраической теории сложности и разработаны методы для их решения, что соответствует паспорту специальности 01.01.09.

Апробация результатов. Результаты, полученные в диссертации, докладывались и обсуждались на международных конференциях: VIII международной конференции «Дискретные модели в теории управляющих систем» (Москва, 2009), X международном семинаре «Дискретная математика и её приложения» (Москва, 2010), XVI международной конференции «Проблемы теоретической кибернетики» (Нижний Новгород, 2011), XVIII международной научной конференции студентов, аспирантов и молодых ученых «Ломоносов – 2011» (Москва, 2011), XI международном семинаре «Дискретная математика и её приложения» (Москва, 2012), XXVII международной конференции «IEEE Computational Complexity Conference» (Порту, Португалия, 2012).

Кроме того, результаты обсуждались на научных семинарах: «Дискретная математика и математическая кибернетика» и «Дискретный ана-

лиз» кафедры математической кибернетики факультета ВМК МГУ, Колмогоровском семинаре по сложности вычислений и сложности определений кафедры математической логики и теории алгоритмов механико-математического факультета МГУ, семинаре «Computational Complexity» факультета «Computer Science» университета Саарланда (Германия).

Публикации. Результаты автора по теме диссертации опубликованы в 7 работах, список которых приводится в конце автореферата.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав и библиографии, включающей 57 наименований. Общий объем диссертации составляет 80 страниц.

Краткое содержание работы

Во введении содержится история вопроса, обосновывается актуальность темы исследования. В нём сформулирована цель диссертации, описана структура диссертации и перечислены основные результаты.

Первая глава посвящена описанию методов алгебры и алгебраической теории сложности, используемых при доказательстве результатов диссертации. В ней даются основные определения, вводятся модель вычисления и постановка задачи, приводятся известные методы получения нижних оценок для мультипликативной сложности умножения в алгебрах.

Определение 1. Пусть U, V, W — конечномерные линейные пространства над полем k, и $\psi : U \times V \to W$ — билинейное отображение. Билинейным вычислением (билинейным алгоритмом) для ψ называется такая последовательность $(f_1, g_1, w_1, \ldots, f_r, g_r, w_r)$, где $f_\rho \in U^*, g_\rho \in V^*$[12], $w_\rho \in W$, $1 \leq \rho \leq r$, что для любых $u \in U, v \in V$

$$\psi(u, v) = \sum_{\rho=1}^{r} f_\rho(u) g_\rho(v) w_\rho.$$

Число r называется длиной билинейного вычисления. Рангом или билинейной сложностью ψ называется длина кратчайшего билинейного вычисления для ψ. Ранг ψ обозначается $R(\psi)$.

Ранг умножения в алгебре A (являющегося билинейным отображением $A \times A \to A$) называется *рангом алгебры* A и обозначается $R(A)$.

[12]Через U^*, V^* обозначены двойственные пространства к пространствам U, V соответственно.

Обобщением билинейного вычисления и ранга является квадратичное вычисление и мультипликативная сложность.

Определение 2. Квадратичным вычислением (квадратичным алгоритмом) для ψ называется такая последовательность $(f_1, g_1, w_1, \ldots, f_l, g_l, w_l)$, где $f_\lambda, g_\lambda \in (U \times V)^*$, $w_\lambda \in W$, $1 \leq \lambda \leq l$, что для любых $u \in U, v \in V$

$$\psi(u, v) = \sum_{\lambda=1}^{l} f_\lambda(u, v) g_\lambda(u, v) w_\lambda.$$

Число l называется длиной квадратичного вычисления. Мультипликативной сложностью ψ называется длина кратчайшего квадратичного вычисления для ψ. Мультипликативная сложность ψ обозначается $C(\psi)$.

Мультипликативная сложность умножения в алгебре A называется *мультипликативной сложностью алгебры* A и обозначается $C(A)$.

Очевидно, для любого ψ справедливо $C(\psi) \leq R(\psi)$.

Теорема 1 (А. Алдер, Ф. Штрассен[13])**.** *Для произвольной ассоциативной алгебры* A *выполняется*

$$C(A) \geq 2 \dim A - t(A), \tag{1}$$

где $t(A)$ *— число максимальных двусторонних идеалов* A*.*

Алгебра, для которой оценка (1) совпадает с верхней оценкой, называется *алгеброй минимальной мультипликативной сложности*. Если оценка (1) выполняется как равенство для ранга, то есть $R(A) = 2 \dim A - t(A)$, то алгебра называется *алгеброй минимального ранга*. Очевидно, что произвольная алгебра минимального ранга является алгеброй минимальной мультипликативной сложности.

Определение 3. Пусть A — алгебра над полем k размерности n, и пусть $a_1, \ldots, a_n$ — некоторый базис A. Если множество $\{a_1, \ldots, a_n\}$ образует группу относительно умножения в A, то такой базис называется *групповым базисом*, а алгебра соответственно *групповой алгеброй*. Обратно, пусть $G = \{g_1, \ldots, g_n\}$ — группа порядка n, и k — поле. Тогда множество формальных сумм

$$B = \{\alpha_1 g_1 + \cdots + \alpha_n g_n | \alpha_\nu \in k,\ 1 \leq \nu \leq n\}$$

[13] A. Alder, V. Strassen. On the algorithmic complexity of associative algebras. Theoret. Comput. Sci., 15:201–211, 1981.

с умножением, определяемым по правилу

$$\left(\sum_{\nu=1}^{n}\alpha_\nu g_\nu\right)\left(\sum_{\mu=1}^{n}\beta_\mu g_\mu\right)=\sum_{\kappa=1}^{n}\left(\sum_{\nu,\mu:g_\nu g_\mu=g_\kappa}\alpha_\nu\beta_\mu\right)g_\kappa,$$

образует групповую алгебру. Будем обозначать групповую алгебру группы G над полем k через $k[G]$. Очевидно, что $k[G]$ коммутативна тогда и только тогда, когда G — абелева.

Вторая глава посвящена исследованию мультипликативной сложности умножения в коммутативных групповых алгебрах над полями характеристики нуль.

В разделе 2.1 приводится постановка задачи и ее решение для групповой алгебры циклической группы над полем рациональных чисел. Доказывается, что сложность умножения в такой алгебре есть две размерности алгебры минус число натуральных делителей размерности алгебры.

Обозначим через $\mathbb{Q}$ поле рациональных чисел. Пусть $\mathbb{Q}[\mathbb{Z}_n]$ — групповая алгебра циклической группы над полем рациональных чисел. Циклическая группа $\mathbb{Z}_n$ определяется законом умножения:

$$g_i\cdot g_j=\begin{cases} g_{i+j}, & i+j<n,\\ g_{i+j-n}, & i+j\geq n.\end{cases}$$

Прежде чем формулировать теорему о групповой алгебре $\mathbb{Q}[\mathbb{Z}_n]$ введем понятие *кругового многочлена*. Круговым многочленом называется многочлен вида

$$\Phi_n(X)=\prod_k(x-\xi_n^k),$$

где произведение берётся по всем натуральным числам k, меньшим n и взаимно простым с n, а $\xi_n=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ — комплексный корень степени n из единицы. Обозначим через $\mathbb{Q}[X]/(\Phi_d(X))$ — фактор-алгебру алгебры многочленов от переменной X над полем рациональных чисел по модулю многочлена $\Phi_d(X)$.

Теорема 2. *Пусть $\mathbb{Q}[\mathbb{Z}_n]$ — групповая алгебра циклической группы порядка n над полем рациональных чисел, и σ равно количеству делителей числа n. Тогда алгебра $\mathbb{Q}[\mathbb{Z}_n]$ является алгеброй минимального ранга, $R(\mathbb{Q}[\mathbb{Z}_n])=2n-\sigma$, и*

$$\mathbb{Q}[\mathbb{Z}_n]\cong\underset{d|n}{\times}\mathbb{Q}[X]/(\Phi_d(X)). \tag{2}$$

В разделе 2.2 доказывается теорема 3, которая является обобщением теоремы 2 на случай групповой алгебры произвольной абелевой группы над полем рациональных чисел. Устанавливается структура и мультипликативная сложность умножения в такой групповой алгебре.

Пусть G_n — произвольная абелева группа порядка $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, где $p_1, p_2, \dots, p_s$ — попарно различные простые числа. Так как произвольная абелева группа изоморфна прямому произведению примарных циклических групп, то будем считать, что G_n определяется следующим образом:

$$G_n \cong G_{p_1^{k_1}} \times G_{p_2^{k_2}} \times \ldots \times G_{p_s^{k_s}}. \tag{3}$$

$$G_{p_i^{k_i}} \cong \mathbb{Z}_{p_i^{k_{i1}}} \times \mathbb{Z}_{p_i^{k_{i2}}} \times \ldots \times \mathbb{Z}_{p_i^{k_{is_i}}}, \tag{4}$$

$$0 = k_{i0} < k_{i1} \le k_{i2} \le \ldots \le k_{is_i} = l_i, \ \sum_{j=1}^{s_i} k_{ij} = k_i, \qquad i = 1, \dots, s. \tag{5}$$

Пусть $m = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$. Тогда m делит n, и $m = n \Leftrightarrow G_n \cong \mathbb{Z}_n$. Далее, пусть числа u и v таковы, что $1 \le u \le l_i,\ k_{iv} < u \le k_{i,v+1}$, т. е. v однозначно определяется по u. Тогда

$$\sigma_1 = 1,\ \sigma_{p_i^u} = p_i^{t_{iu}} \cdot \frac{p_i^{u(s_i-v)} - p_i^{(u-1)(s_i-v)}}{p_i^u - p_i^{u-1}},\ \text{где } t_{iu} = \sum_{j=1}^{v} k_{ij}\ . \tag{6}$$

Определим теперь числа σ_d, где d — произвольный делитель числа m, а также число σ, зависящее от структуры группы G_n:

$$d = p_1^{u_1} p_2^{u_2} \dots p_s^{u_s},\ 0 \le u_i \le l_i, \Rightarrow \sigma_d = \sigma_{p_1^{u_1}} \cdot \sigma_{p_2^{u_2}} \cdot \ldots \cdot \sigma_{p_s^{u_s}}, \tag{7}$$

$$\sigma = \sum_{d|m} \sigma_d = \prod_{i=1}^{s} \sum_{u=0}^{l_i} \sigma_{p_i^u}. \tag{8}$$

Теорема 3. *Пусть $\mathbb{Q}[G_n]$ — произвольная коммутативная групповая алгебра размерности n над полем рациональных чисел. Тогда алгебра $\mathbb{Q}[G_n]$ является алгеброй минимального ранга, $R(\mathbb{Q}[G_n]) = 2n - \sigma$, и*

$$\mathbb{Q}[G_n] \cong \underset{d|m}{\times} (\mathbb{Q}[X]/\Phi_d)^{\sigma_d}. \tag{9}$$

В разделе 2.3 доказывается, что любая коммутативная групповая алгебра над произвольным полем характеристики нуль является алгеброй минимальной мультипликативной сложности.

Обозначим через $\mathbb{F}$ произвольное поле характеристики 0. Рассмотрим групповую алгебру $\mathbb{F}[G_n]$ абелевой группы G_n. Будем считать, что G_n определяется согласно формулам (3) — (5).

Как известно, произвольное поле характеристики 0 содержит подполе, изоморфное полю рациональных чисел. Поэтому будем считать, что поле $\mathbb{F}$ является расширением поля $\mathbb{Q}$.

Для любого натурального d многочлен $\Phi_d(X)$ имеет целые коэффициенты, следовательно, он является многочленом над полем $\mathbb{F}$. Обозначим через r_d число неприводимых над полем $\mathbb{F}$ многочленов, произведение которых равно многочлену $\Phi_d(X)$. Тогда можно записать

$$\Phi_d(X) = f_{d1}(X) \cdot f_{d2}(X) \cdot \ldots \cdot f_{dr_d}(X), \tag{10}$$

где многочлены $f_{dj}(X),\ j = 1, \ldots, r_d$, неприводимы над полем $\mathbb{F}$. Пусть числа m, σ, σ_d, определяются, в зависимости от группы G_n, по формулам (6) — (8). Определим константу $\sigma_{\mathbb{F}}$, зависящую от поля $\mathbb{F}$ и группы G_n, таким образом

$$\sigma_{\mathbb{F}} = \sum_{d|m} r_d \cdot \sigma_d$$

Справедлива следующая теорема, которая является обобщением теоремы 3.

Теорема 4. *Пусть $\mathbb{F}[G_n]$ — произвольная коммутативная групповая алгебра размерности n над полем характеристики 0. Тогда алгебра $\mathbb{F}[G_n]$ является алгеброй минимального ранга, $R(\mathbb{F}[G_n]) = 2n - \sigma_{\mathbb{F}} \leq 2n - \sigma$, и*

$$\mathbb{F}[G_n] \cong \underset{d|m}{\times} (\mathbb{F}[X]/\Phi_d)^{\sigma_d} \cong \underset{d|m}{\times} \overset{r_d}{\underset{j=1}{\times}} (\mathbb{F}[X]/f_{dj})^{\sigma_d}. \tag{11}$$

Третья глава посвящена коммутативным групповым алгебрам над полями простой характеристики. Переход к рассмотрению полей простой характеристики значительно меняет ситуацию. Структура групповых алгебр над такими полями оказывается более разнообразной, чем над полями характеристики нуль, и как следствие, существуют коммутативные групповые алгебры, не являющиеся алгебрами минимального ранга.

В разделе 3.1 доказывается необходимое и достаточное условие того, что коммутативная групповая алгебра над произвольным полем простой характеристики является алгеброй минимального ранга.

Все поля, рассматриваемые в третьей главе, имеют характеристику p, где p произвольное простое число. Разобьём множество $\mathcal{G}$ — всех абелевых групп, на последовательность вложенных подмножеств. Пусть G_N — произвольная абелева группа порядка N. Тогда группу G_N можно однозначно представить в виде прямого произведения примарных циклических групп:

$G_N \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \ldots \times \mathbb{Z}_{p_r^{k_r}}$, где $p_1, p_2, \ldots, p_r$ — простые числа. Будем говорить, что $G_N \in \mathcal{G}_i$, если не более чем i из этих простых чисел совпадают с p. Очевидно, что $\mathcal{G}_i \subset \mathcal{G}_{i+1}$, и $\mathcal{G} = \mathcal{G}_0 \cup \mathcal{G}_1 \cup \ldots \cup \mathcal{G}_l \cup \ldots$.

Пусть $\mathbb{F}$ — произвольное поле характеристики p (если $\mathbb{F}$ — конечное, то обозначим число его элементов через q). Пусть $G_N \in \mathcal{G}_1$ — произвольная абелева группа порядка N, принадлежащая множеству $\mathcal{G}_1$, и пусть $N = p^k n = p^k p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, где $p \nmid n,\ p_1, p_2, \ldots, p_r$ — попарно различные простые числа. Тогда

$$G_N \cong \mathbb{Z}_{p^k} \times G_n, \tag{12}$$

где G_n — произвольная абелева группа порядка n. Пусть G_n определяется согласно формулам (3)–(5). Пусть $m = p_1^{l_1} p_2^{l_2} \ldots p_r^{l_r}$. Обозначим

$$t = \begin{cases} 2p^k s_m - 2, & \text{если } s_m > 1, \\ 2p^k - 4, & \text{если } s_m = 1, \end{cases} \tag{13}$$

где s_m — мультипликативная степень числа q по модулю m, то есть такое минимальное натуральное число, что $q^{s_m} - 1$ делится на m.

Теорема 5. *Пусть $\mathbb{F}[G_N]$ — групповая алгебра абелевой группы порядка N над произвольным полем простой характеристики. Алгебра $\mathbb{F}[G_N]$ является алгеброй минимального ранга тогда и только тогда, когда выполняются два условия:*
1) группа G_N принадлежит множеству групп $\mathcal{G}_1$,
2) если $\mathbb{F}$ — конечное поле, то число его элементов $q \geq t$.

В разделе 3.2 доказываются верхняя и нижняя оценки для мультипликативной сложности умножения в коммутативных групповых алгебрах над полями простой характеристики.

Из теоремы 5 следует, что по данной групповой алгебре $F_q[G_N]$ над конечным полем F_q мощности q, вычислив t по формуле (13), можно определить, является ли эта алгебра алгеброй минимального ранга. Если является, то можно вычислить σ_{F_q} и найти точное значение для $R(F_q[G_N])$. Если она не является алгеброй минимального ранга, то нижняя оценка $2N - \sigma_{F_q}$ остается справедливой, тогда как о верхней оценке уже ничего сказать нельзя. Однако, удается доказать, что билинейная сложность умножения в алгебре $F_q[G_N]$ растет линейно относительно её размерности.

Теорема 6. *Пусть $\mathbb{F}[G_N]$ — групповая алгебра абелевой группы порядка N над произвольным полем характеристики p, $G_N \in \mathcal{G}_l$. Тогда существует константа C_l, зависящая только от множества $\mathcal{G}_l$, такая, что*

$$R(\mathbb{F}[G_N]) \leq C_l N. \tag{14}$$

Пусть $G_1, G_2, \ldots, G_n, \ldots$ — последовательность групп такая, что $G_n \in \mathcal{G}_{l_n} \setminus \mathcal{G}_{l_n-1}$, $|G_n| \to \infty$ при $n \to \infty$, и $\sup l_n = l < \infty$. Из теоремы 6 следует, что над произвольным полем $\mathbb{F}$ характеристики p верно, что $R(\mathbb{F}[G_n]) \leq C \cdot \dim\mathbb{F}[G_n]$, где константа C не зависит от n. При этом, остается открытым вопрос о том, как растет билинейная сложность $R(\mathbb{F}[G_n])$ при $n \to \infty$, если $\sup l_n = \infty$. Для доказательства некоторой нетривиальной нижней оценки для такой последовательности групповых алгебр над произвольным полем простой характеристики в диссертационной работе используется следующая теорема[14]:

Теорема 7. *Пусть A — ассоциативная алгебра. Для всех $m, n > 0$,*

$$C(A) \geq \dim A + \dim(\mathrm{rad}A)^m + \dim(\mathrm{rad}A)^n - \dim(\mathrm{rad}A)^{n+m-1}.$$

При помощи этой теоремы Блезер построил последовательность явно заданных алгебр A_n с наилучшей среди известных нижней оценкой мультипликативной сложности, а именно, с оценкой $(3-o(1))\dim A_n$. Оказывается, что последовательность алгебр с такой нижней оценкой можно выбрать и среди коммутативных групповых алгебр.

Теорема 8. *Пусть $\mathbb{F}[G_n]$ — последовательность групповых алгебр над полем $\mathbb{F}$ характеристики p такая, что $G_n \in \mathcal{G}_n \setminus \mathcal{G}_{n-1}$, и $\dim\mathbb{F}[G_n] = p^{k_n}$. Тогда*

$$C(\mathbb{F}[G_n]) \geq (3 - o(1))\dim\mathbb{F}[G_n], \text{ при } n \to \infty.$$

Четвертая глава посвящена задаче описания алгебр минимальной мультипликативной сложности над произвольными полями с точки зрения их алгебраической структуры.

В разделе 4.1 приводятся постановка и актуальность задачи, формулируется основная теорема главы (теорема 11).

Много работ в алгебраической теории сложности посвящено описанию алгебр минимального ранга с точки зрения их алгебраической структуры. Одной из мотиваций этих работ являлось найти сложность умножения матриц малого порядка. Давно известно, что алгебра $k^{2\times 2}$ — алгебра матриц размерности 2×2, является алгеброй минимального ранга. Долгое время открытой проблемой было определить, является ли алгебра $k^{3\times 3}$ алгеброй минимального ранга[15]. Один способ решения этой задачи — описать все

[14] Markus Bläser. *Improvements of the Alder-Strassen Bound: Algebras with Nonzero Radical.* Institut für Theoretische Informatik, Germany.

[15] P. Bürgisser, M. Clausen, M. Shokrollahi. *Algebraic Complexity Theory.* Springer, 1997.

алгебры минимального ранга с точки зрения их алгебраических свойств и проверить выполнение этих свойств для $k^{3\times 3}$.

Де Грут был первым, кто нашел описание всех алгебр с делением D минимального ранга[16]. Над бесконечным полем все такие алгебры являются простыми расширениями поля k. Если k конечное, то D имеет минимальный ранг, если вдобавок $\#k \geqslant 2\dim D - 2$, что следует из описания всех алгоритмов умножения многочленов по модулю некоторого неприводимого многочлена[17]. Де Грут и Хейнц[18] исследовали коммутативные алгебры минимального ранга над бесконечным полем. Далее Бучи и Клаузен[19] описали все локальные алгебры минимального ранга над бесконечным полем. Затем Хейнц и Моргенштерн[20] описали все основные алгебры над алгебраически замкнутыми полями. Наконец, все полупростые алгебры над произвольными полями и все алгебры над алгебраически замкнутыми полями были найдены Блезером[21]. Важным побочным эффектом этого результата стало то, что алгебра $k^{3\times 3}$ не является алгеброй минимального ранга. Полное и окончательное описание всех алгебр минимального ранга было получено Блезером в 2002 году[22].

Теорема 9 (М. Блезер)**.** *Алгебра A над полем k является алгеброй минимального ранга тогда и только тогда, когда*

$$A \cong C_1 \times \cdots \times C_s \times \underbrace{k^{2\times 2} \times \cdots \times k^{2\times 2}}_{u \text{ раз}} \times B, \tag{15}$$

где $C_1, \ldots, C_s$ — локальные алгебры минимального ранга, для которых $\dim(C_\sigma/\mathrm{rad}C_\sigma) \geq 2$, то есть $C_\sigma \cong k[X]/(p_\sigma(X)^{d_\sigma})$ для некоторого неприводимого над k полинома p_σ, $\deg p_\sigma \geq 2, d_\sigma \geq 1$ и $\#k \geq 2\dim C_\sigma - 2$, $\sigma = 1, \ldots, s$, а B — сверхосновная алгебра минимального ранга над k. Сверхосновная алгебра B является алгеброй минимального ранга тогда и только тогда, когда найдутся такие $w_1, \ldots, w_m \in \mathrm{rad}B, w_i^2 \neq 0$, $w_i w_j = 0$, $i \neq j$,

[16]Hans F. de Groote. *Characterization of division algebras of minimal rank and the structure of their algorithm varieties.* SIAM J. Comput., 12:101–117, 1983.

[17]S. Winograd. *On multiplication in algebraic extension fields.* Theoret. Comput. Sci., 8:359–377, 1979.

[18]Hans F. de Groote and Joos Heintz. *Commutative algebras of minimal rank.* Lin. Alg. Appl., 55:37–68, 1983.

[19]Werner Büchi and Michael Clausen. *On a class of primary algebras of minimal rank.* Lin. Alg. Appl., 69:246–268, 1985.

[20]Joos Heintz and Jacques Morgenstern. *On associative algebras of minimal rank.* In Proc. 2nd Applied Algebra and Error Correcting Codes Conf. (AAECC), Lecture Notes in Comput. Sci. 228, pages 1–24. Springer, 1986.

[21]Markus Bläser. *Lower bounds for the bilinear complexity of associative algebras.* Comput. Complexity, 9:73-112, 2000.

[22]Markus Bläser. *A Complete Characterization of the Algebras of Minimal Bilinear Complexity.* SIAM J. Comput., 34(2):277-298, 2004.

что

$$\mathrm{rad}B = L_B + Bw_1B + \cdots + Bw_mB = R_B + Bw_1B + \cdots + Bw_mB$$

и $\#k \geq 2N(B) - 2$*, где* L_B *и* R_B *суть правый и левый аннигиляторы* $\mathrm{rad}B$ *(то есть множество всех таких* $x \in \mathrm{rad}B$*, что* $x(\mathrm{rad}B) = \{0\}$*, соответственно* $(\mathrm{rad}B)x = \{0\}$*), а* $N(B)$ *— наибольшее целое* j*, для которого* $(\mathrm{rad}B)^j \neq \{0\}$*. Любое из чисел* s, u *может равняться нулю, а множитель* B *является необязательным.*

Так как доказывать нижние оценки для мультипликативной сложности обычно сложнее, чем для ранга, то в отличие от алгебр минимального ранга для алгебр минимальной мультипликативной сложности результатов было получено немного. Один известный результат принадлежит Фейгу[23], который дополняет описание алгебр с делением минимального ранга Де Грута:

Теорема 10 (Фейг)**.**

1. Алгебра с делением D *имеет минимальную мультипликативную сложность тогда и только тогда, когда она имеет минимальный ранг.*

2. Более того, каждый оптимальный квадратичный алгоритм для такой алгебры является билинейным, то есть после перестановки некоторых f_λ *с* g_λ*, имеем*

$f_\lambda(x, y) = f_\lambda(x, 0)$ *и* $g_\lambda(x, y) = g_\lambda(0, y)$ *для всех* $x, y \in D$*.*

Справедлива следующая теорема, которая является обобщением теоремы Фейга на случай произвольных алгебр или, что то же самое, обобщением теоремы Блезера на случай мультипликативной сложности.

Теорема 11. *Алгебра* A *над произвольным полем является алгеброй минимальной мультипликативной сложности тогда и только тогда, когда она является алгеброй минимального ранга.*

В разделе 4.2 рассматривается случай сверхосновных алгебр минимальной мультипликативной сложности, доказывается теорема 12, устанавливающая структуру таких алгебр.

Теорема 12. *Сверхосновная алгебра* A *над произвольным полем* k *имеет минимальную мультипликативную сложность тогда и только тогда, когда она имеет минимальный ранг.*

[23]Ephraim Feig. *On systems of bilinear forms whose minimal division-free algorithms are all bilinear.* J. Algorithms 2(3): 261–281, 1981.

В разделе 4.3 рассматривается случай локальных алгебр минимальной мультипликативной сложности, доказывается теорема 13, устанавливающая структуру таких алгебр.

Теорема 13. *Локальная алгебра A над произвольным полем k имеет минимальную мультипликативную сложность тогда и только тогда, когда она имеет минимальный ранг.*

В разделе 4.4 рассматривается алгебра, для которой фактор-алгебра по радикалу изоморфна алгебре квадратных матриц порядка 2. Доказывается, что такая алгебра является алгеброй минимальной мультипликативной сложности тогда и только тогда, когда ее радикал нулевой.

Теорема 14. *Алгебра A над произвольным полем k такая, что $A/\operatorname{rad} A = k^{2\times 2}$, имеет минимальную мультипликативную сложность тогда и только тогда, когда она имеет минимальный ранг.*

В разделе 4.5 приводится доказательство основной теоремы 11 на основании результатов разделов 4.2, 4.3 и 4.4.

Раздел 4.6 посвящен обобщению второй части теоремы Фейга для локальных и сверхосновных алгебр. Вводится понятие почти билинейного алгоритма умножения в алгебре. Доказывается теорема 15 о том, что любой квадратичный алгоритм для умножения в локальной или сверхосновной алгебре является почти билинейным. Однако показывается, что существуют квадратичные алгоритмы для таких алгебр, не являющиеся билинейными.

Теорема 15. *Пусть A — локальная или сверхосновная алгебра минимальной мультипликативной сложности. Тогда любой оптимальный квадратичный алгоритм $\beta = (f_1, g_1, w_1, \ldots, f_\ell, g_\ell, w_\ell)$ для A является почти билинейным. В частности, если $w_\lambda \notin L_A \cap R_A$ для всех λ, то β является билинейным.*

Следующий пример показывает, что существуют квадратичные алгоритмы для умножения в локальных и сверхосновных алгебрах минимальной сложности, не являющиеся билинейными.

Пример 1. Пусть k — поле характеристики отличной от двух. Алгебра $k[X]/(X^2)$ является локальной и сверхосновной, но имеет квадратичный алгоритм, который не является билинейным (но естественно является почти билинейным): мы можем вычислить коэффициенты $(a+bX)(a'+b'X)$ как aa' и $ab'+ba' = \frac{1}{2}(b+b')(a+a') + \frac{1}{2}(b-b')(-a+a')$. Заметим, что $X \in L_{k[X]/(X^2)} = R_{k[X]/(X^2)}$.

Основные результаты, выносимые на защиту

1. Установлена структура и получены точные значения мультипликативной сложности коммутативных групповых алгебр над полем рациональных чисел. Доказано, что любая групповая алгебра абелевой группы над произвольным полем характеристики нуль является алгеброй минимального ранга. Описаны структура и мультипликативная сложность таких групповых алгебр, зависящие от разложения над данным полем многочлена $X^n - 1$ на неприводимые сомножители.

2. Найдено необходимое и достаточное условие того, что коммутативная групповая алгебра над произвольным полем простой характеристики является алгеброй минимального ранга. Доказаны линейные верхние оценки на билинейную сложность умножения в коммутативных групповых алгебрах над произвольным полем простой характеристики. Над произвольным полем простой характеристики построена последовательность групповых алгебр абелевых групп с высокой нижней оценкой на мультипликативную сложность.

3. Полностью решена задача описания алгебраической структуры алгебр минимальной мультипликативной сложности над произвольными полями. Доказано, что любой квадратичный алгоритм для умножения в сверхосновной или локальной алгебре минимальной мультипликативной сложности является почти билинейным.

Благодарности

Автор выражает благодарность своему научному руководителю, доктору физико-математических наук, профессору Алексееву Валерию Борисовичу за постановку задачи и постоянное внимание к работе.

Публикации автора по теме диссертации

[1] Чокаев Б. В. *Исследование сложности умножения в коммутативных групповых алгебрах.* // Сборник тезисов лучших дипломных работ 2009 года, с. 105–106. Изд-во факультета ВМиК МГУ, Москва, 2009.

[2] Чокаев Б. В. *О сложности умножения в коммутативных групповых алгебрах.* // Труды VIII Международной Конференции «Дискретные

модели в теории управляющих систем», с. 351–356. Изд-во Макс Пресс, Москва, 2009.

[3] Чокаев Б. В. *Исследование сложности умножения в коммутативных групповых алгебрах.* // Материалы X Международного семинара «Дискретная математика и её приложения», с. 150–153. Изд-во мех.-мат. факультета МГУ, Москва, 2010.

[4] Чокаев Б. В. *Сложность умножения в коммутативных групповых алгебрах над полями характеристики 0.* // Вестник МГУ, серия 15, № 4, стр. 30-40. Изд-во МГУ, Москва, 2010.

[5] Чокаев Б. В. *Сложность умножения в коммутативных групповых алгебрах над полями простой характеристики.* // Дискретная математика, т. 22, вып. 4, стр. 121-137. “Наука”, Москва, 2010.

[6] Блезер М., Чокаев Б. В. *О почти билинейных алгоритмах для локальных и сверхосновных алгебр.* // Материалы XI Международного семинара «Дискретная математика и её приложения», с. 95–98. Изд-во мех.-мат. факультета МГУ, Москва, 2012.

[7] Markus Bläser, Bekhan Chokaev. *Algebras of minimal multiplicative complexity.* // Proc. 27th Ann. IEEE Computational Complexity Conference (CCC), 224–234, 2012.